Аппаратное и программное обеспечение ЭВМ и сетей

Раздел 7 Сетевые операционные системы

Тема № 50. Основные концепции Active Directory Sever Windows 2003

Понятие службы каталога и Active Directory

- Объединение компьютеров в единую информационную сеть позволяет пользователям совместно использовать общие ресурсы. Современные ОС, используют для организации ресурсов специальную сетевую службу, дающую пользователям возможность получения доступа к ресурсам сети без необходимости точного знания местоположения этих ресурсов. Речь идет о службе каталога (Directory Service).
- Каталог - глобальное унифицированное хранилище информации об элементах сетевой инфраструктуры. Вся информация о компонентах сети, а именно: пользователи, ресурсы, сетевые службы и т. п., размещается в каталоге. Внутри каталога объекты организуются либо в соответствии с физической, либо логической структурой сети.
- К задачам, которые служба каталога позволяет решить администратору, относятся:
  - **Управление сетевыми ресурсами**. Основная задача, ради чего компьютеры объединяются в сеть. Служба каталога облегчает пользователям поиск нужных ресурсов, скрывая от них подробности реализации механизма поиска. Пользователь формулирует запрос, а служба каталога локализует требуемый ресурс.

Понятие службы каталога и Active Directory

- **Управление пользователями**. Каждому пользователю поставлен в соответствие определенный набор характеристик, позволяющий персонализировать его деятельность в сети. Это дает возможность управлять доступом к сетевым ресурсам на уровне пользователей. При этом пользователи рассматривается в качестве обыкновенных объектов каталога, и являются элементами структуры сети (логической либо физической).
- **Управление приложениями**. В зависимости от задач, которые решают пользователи, на их компьютерах может быть развернуто различное ПО. В случае большой корпорации на передний план выходит задача по централизованному управлению программным обеспечением, включая развертывание новых приложений и выполнение обновления существующих.
- **Управление службами**. Большинство сетевых служб, например именование объектов сети, выделение IP-адресов, DNS служба и т.д., может быть интегрировано со службой каталога, что позволит более эффективно организовать функционирование этих служб.

Понятие службы каталога и Active Directory

- Практически все производители корпоративных операционных систем предлагают потребителям свои реализации службы каталога. Компания Microsoft предлагает свою версию службы каталога, названную Active Directory.
- Служба каталога Active Directory базируется на открытых стандартах:
- протокол LDAP;
- система доменных имен (Domain Name System, DNS);
- протокол аутентификации Kerberos v5.
- Эти стандарты (особенно LDAP) определили терминологию, используемую в архитектуре Active Directory, поэтому сначала мы кратко рассмотрим их особенности и взаимодействие со службой Active Directory.

Протокол LDAP

- Протокола LDAP был разработан на основе основные спецификации X.500. Данная спецификация была разработана Международными консультационными и стандартизирующими организациями комитетом по телефонии и телеграфии (Consultative Committee for International Telephone and Telegraph, CCITT) совместно с Международной организацией по стандартизации (International Standardization Organization, ISO). В рамках спецификации X.500 определяется ряд понятий:
  - ***системный агент каталога*** (Directory System Agent, DSA) представляет собой базу данных, в которой хранится информация каталога. База данных имеет иерархическую организацию и позволяет быстро и эффективно осуществлять поиск и извлечение необходимых данных;
  - ***агент пользователя каталога*** (Directory User Agent, DUA) обеспечивает функциональность доступа к каталогу, которая может быть реализована в различных пользовательских приложениях;
  - протокол доступа к каталогу (Directory Access Protocol, DAP) контролирует процесс взаимодействия между системным и пользовательским агентами каталога.

Протокол LDAP

- Протокола LDAP был разработан на основе основные спецификации X.500. Данная спецификация была разработана Международными консультационными и стандартизирующими организациями комитетом по телефонии и телеграфии (Consultative Committee for International Telephone and Telegraph, CCITT) совместно с Международной организацией по стандартизации (International Standardization Organization, ISO). В рамках спецификации X.500 определяется ряд понятий:
  - ***системный агент каталога*** (Directory System Agent, DSA) представляет собой базу данных, в которой хранится информация каталога. База данных имеет иерархическую организацию и позволяет быстро и эффективно осуществлять поиск и извлечение необходимых данных;
  - ***агент пользователя каталога*** (Directory User Agent, DUA) обеспечивает функциональность доступа к каталогу, которая может быть реализована в различных пользовательских приложениях;
  - протокол доступа к каталогу (Directory Access Protocol, DAP) контролирует процесс взаимодействия между системным и пользовательским агентами каталога.

Протокол LDAP

- Протокол LDAP (Lightweight Directory Access Protocol- Облегченный протокол доступа к каталогу) обеспечивает доступ к каталогу, разработанному в соответствии с рекомендациями стандарта X.500. Протокол представляет собой стандартное средство реализации доступа и обновления информации в каталоге для приложений.
- Протокол LDAP не полностью совместим со спецификацией X.500. Основное требование — служба каталога должна поддерживать систему именования X.500.
- Протокол LDAP является частью стека протоколов TCP/IP, что и послужило одной из причин его популярности. Разработчики компании Microsoft взяли за основу информационную модель X.500 и реализовали поддержку протокола LDAP. Доступ к содержимому каталога Active Directory по протоколу LDAP может осуществляться с помощью любого LDAP-клиента. При этом использование протокола LDAP не является единственно возможным способом доступа к каталогу Active Directory.
- *Примечание*
- *Служба каталога Active Directory поддерживает протокол LDAP версии 2 и 3.*

Протокол LDAP

- Спецификация протокола LDAP базируется на четырех моделях.
- ***Информационная модель*** (Information Model) описывает структуру каталога и содержащейся в ней информации.
- ***Модель именования (Naming Model)*** описывает схемы именования и идентификации объектов каталога.
- ***Функциональная модель (Functional Model)*** определяет действия, которые могут быть осуществлены над информацией, размещенной в каталоге.
- ***Модель безопасности (Security Model)*** описывает механизмы защиты информации, размещенной в каталоге.
- Понимание этих моделей необходимо как для эффективного использования служб Active Directory.

Информационная модель Active Directory

Объекты и дерево каталога

- Основным структурным компонентом каталога является элемент (entry), который в терминологии Active Directory называется объектом (object). Объекты являются фундаментальными единицами, которыми манипулирует служба каталога. При этом каждый объект характеризует некоторую отдельную сущность (например, принтер, компьютер, совместно используемую папку или пользователя). Выделяют объекты двух типов — контейнерного и не контейнерного типа. Объекты контейнерного типа способны выступать в качестве родительских объектов и могут быть использованы для размещения других объектов. Напрашивается аналогия с папками файловой системы, в которых могут быть размещены файлы и другие папки. Объекты контейнерного типа используются для организации объектов по какому-либо признаку. Например, все объекты, ассоциированные с пользователями, размещаются внутри объекта контейнерного типа. Объекты, ассоциированные с компьютерами, размешаются в другом объекте контейнерного типа. Такой подход позволяет упорядочить объекты и облегчить управление ими.

Протокол LDAP

- Множество объектов, расположенные во множестве контейнеров, организовано в иерархическую структуру, которая в терминологии X.500 называется информационным деревом каталога (Directory Information Tree, DIT). Объекты **не контейнерного** являются листьями этого дерева. В качестве узлов дерева **(node) выступают объекты контейнерного типа**. Каждую ветку дерева, вместе со всей совокупностью порожденных ею веток, можно рассматривать по отдельности как самостоятельное дерево. Такая совокупность называется прилегающим ***поддеревом (contiguous subtree).***
- Самый верхний элемент в иерархии объектов каталога в терминологии X.500 называют корнем дерева. Роль корня информационного дерева каталога в спецификации X.500 играет объект rootDSE.

Атрибуты

- Каждый объект каталога состоит из набора атрибутов (attributes), характеризующей объект. Так, например, в качестве атрибутов экземпляра класса "пользователь" могут выступать имя и фамилия пользователя, а также имя сопоставленной ему учетной записи.

Протокол LDAP

- В документации Microsoft часто называет атрибутами свойства (properties) объекта. Атрибуты могут быть обязательными (mandatory) или необязательными (optional). Значения обязательных атрибутов должны быть явно определены в процессе создания объекта.
- С каждым атрибутом в схеме связано понятие синтаксиса (syntax) - характеристикой атрибута. Синтаксис определяет тип значения атрибута (число, строка), порядок следования байтов и правила сравнения (matching rules), используемые для сравнения атрибутов данного типа. Служба каталога Active Directory допускает добавление описаний новых атрибутов и изменение существующих. Однако добавление новых синтаксисов, так же как и изменение существующих, запрещается. Определяя новый атрибут, администратор может только выбрать необходимый синтаксис из списка уже существующих.

Схема каталога

- Схема каталога (schema) - иерархическая структура, в которой хранятся правила, позволяющие управлять структурой каталога и его содержимым, а также определения всех классов объектов.
- Чтобы создать в каталоге объект нового типа, необходимо, прежде всего, добавить в схему определение нового класса объектов. При этом принято говорить о расширении (extending) схемы.

Протокол LDAP

- Возможность расширения схемы фактически означает расширяемость каталога путем его адаптации для хранения новых типов объектов. Информация схемы также хранится в виде объектов двух классов: ***схемы классов (Class schema) и схемы атрибутов (Attribute schema).*** Схема классов объединяет классы, определяющие типы объектов. В схеме атрибутов описываются атрибуты, которые могут быть определены для объектов каталога. Для каждого класса объектов в схеме определяются:
- перечень атрибутов, которые ***обязательно должны*** быть определены для экземпляров указанного класса;
- перечень атрибутов, которые ***могут быть определены*** для экземпляров данного класса;
- совокупность правил, определяющих ***возможных объектов-родителей и объектов-потомков.***

Модель именования LDAP

- Одним из условий успешного манипулирования объектами каталога является однозначная идентификация каждого объекта. Для именования и идентификации объектов в каталоге протокол LDAP использует механизм отличительных имен (Distinguished Name, DN).

Протокол LDAP

- Отличительное имя однозначно определяет положение объекта в информационном дереве каталога, представляя информацию обо всех узлах дерева, которые необходимо пройти, чтобы прийти от данного объекта к корню дерева. Можно провести аналогию с понятием полного пути, используемым для определения месторасположения файла в файловой системе. Например: отличительное имя, идентифицирующего объект Tasha, принадлежащий к подразделению ND домена khsu.ru: DC=by,DC=bru,DC=asu,OU=ND,CN=Users,CN=Tasha.
- Для формирования отличительного имени используются спецификаторы (specifier), определяющие тип объекта:
- DC (Domain Component) — спецификатор "составная часть доменного имени";
- OU (Organizational Unit) — спецификатор "организационная единица";
- CN (Common Name) — спецификатор "общее имя".
- Имя, идентифицирующее сам объект, согласно терминологии LDAP выступает в качестве относительного отличительного имени (Relative Distinguish Name, RDN). Относительное отличительное имя может повторяться в рамках всего каталога. Однако оно должно быть уникально в пределах родительского контейнера. Ниже приводится пример относительного отличительного имени объекта Tasha: CN=Tasha.
- Механизм отличительных имен LDAP является предпочтительной, но не единственной схемой именования объектов в Active Directory.

Схемы именования объектов в Active Directory

- Служба каталога Active Directory позволяет использовать целый ряд дополнительных схем именования, каждая из которых применяется в определенных ситуациях.

Основные имена субъектов безопасности

- Механизм основных имен (Security principal name, SPN) реализует способ именования объектов каталога, применяемой подсистемой безопасности Windows Server 2003. Основное имя субъекта системы безопасности определяется в качестве одного из атрибутов объекта каталога и имеет следующий формат: <имя_субъекта>@<суффикс_основного_имени>
- В качестве суффикса основного имени может выступать DNS-имя текущего или корневого домена или других доменов, lex@ayan.ru или kaizer@khsu.de Используемый для образования основного имени суффикс должен удовлетворять правилам построения доменных имен. Применительно к объектам, ассоциированным с пользователями, говорят об основном имени пользователя (User Principal Name, UPN): lex@ayan.ru. Основное имя позволяет упростить процесс регистрации пользователей в сети на компьютерах, принадлежащих к различным доменам. Основное имя уникально в пределах леса доменов, поэтому для регистрации от пользователя не требуется указания домена, к которому он принадлежит. Основное имя никоим образом не связано с его отличительным именем. Вследствие этого основное имя не меняется даже в случае перемещения объекта в рамках катало

Схемы именования объектов в Active Directory

Полные доменные имена

- Полное доменное имя (Fully Qualified Domain Name, FQDN) используется для однозначной идентификации объектов в пространстве доменных имен. Полное доменное имя образуется в соответствии с соглашениями о доменных именах. В рамках службы каталога механизм полных доменных имен используется для идентификации доменов и принадлежащих им компьютеров. Применительно к компьютеру полное доменное имя состоит из имени компьютера и имени домена: pc001.asu.bru.by

Глобально уникальные идентификаторы

- Отличительное имя однозначно определяет объект в каталоге. Однако перемещение объекта или его переименование (равно как и переименование любого из контейнеров, внутри которых данный объект содержится) приводит к изменению его отличительного имени. Это может привести к неправильной работе приложений, использующих отличительные имена для уникальной идентификации объектов. Задача уникальной и однозначной идентификации объекта может быть решена посредством введения специального атрибута, значение которого не менялось бы при переименовании или перемещении объекта.

Схемы именования объектов в Active Directory

- В службе каталога Active Directory обеспечение уникальности объектов достигается посредством глобально уникального идентификатора (Global Unique Identifier, GUID), представляющего собой 128-разрядное число. Глобально уникальный идентификатор генерируется непосредственно в момент создания объекта в каталоге и является одним из обязательных атрибутов, который не может быть изменен ни при каких обстоятельствах. В случае изменения отличительного имени глобально уникальный идентификатор остается неизменным, определяя конкретный объект каталога. Это свойство глобальных идентификаторов можно использовать при разработке приложений, работающих с объектами каталога.

Имена NetBIOS

- До появления службы каталога Active Directory в качестве основного способа именования объектов в операционных системах Windows применялись имена NetBIOS. В частности этот способ именования используется в операционных системах Windows 95/98/NT. Имена пользователей, компьютеров и доменов в среде Windows NT представляют собой имена NetBIOS.

Схемы именования объектов в Active Directory

- Большинство приложений, разработанных для этого семейства операционных систем, предполагают использование только этой схемы именования. Данная схема именования была реализована в Active Directory с целью сохранения обратной совместимости со старыми операционными системами и разработанными для них приложениями. Имя NetBIOS должно быть уникально в пределах домена и его длина не должна превышать 15 символов.

Унифицированный указатель ресурсов LDAP

- Протокол LDAP является одним из стандартных методов доступа к каталогу Active Directory. Любое LDAP-совместимое приложение может обратиться к объектам каталога посредством запроса, записанного в формате унифицированного указателя ресурсов LDAP (LDAP Uniform Resource Locator, LDAP URL). Унифицированный указатель ресурсов LDAP начинается с ключевого слова LDAP, затем следует имя сервера, содержащего копию каталога, и отличительное имя ресурса. Ниже приводится пример записи унифицированного указателя ресурсов:
- LDAP: //root.root.by/cn=tasha, cn=user,ou=nd, dc=bru,dc=by

Схемы именования объектов в Active Directory

Канонические имена

- Вместо отличительного имени для определения положения объекта в дереве каталога можно использовать так называемое каноническое имя (canonical name). Принцип построения канонического имени аналогичен принципу формирования отличительных имен, за исключением того, что при записи канонического имени опускаются спецификаторы, обозначающие тип объекта или контейнера. Для указания домена в каноническом имени используется соглашение о доменных именах. Ниже приводится пример канонического имени: bru.by/cit/nd/tasha

Служба DNS

- Протокол LDAP представляет собой механизм доступа пользователей к каталогу. Однако для того, чтобы клиент смог подключиться к серверу LDAP и отправить свой запрос, он должен точно знать его расположение в сети. Проблема осложняется тем фактом, что в сети может иметься несколько LDAP-серверов, с которыми клиента соединяют коммуникационные линии с различной пропускной способностью. Кроме того, интересующая клиента информация может располагаться не на всех LDAP-серверах. Компания Microsoft предложила задействовать Службу доменных имен (Domain Name Systems DNS) в качестве средства обнаружения (определения местонахождения) различных сетевых служб, например контроллеров доменов и Центров распределения ключей Kerberos. Доменная служба имен традиционно используется в TCP/IP-сетях для разрешения символических имен в IP-адреса. Для обнаружения сетевых служб (сервисов) DNS использует специальный тип ресурсных записей, это - SRV-записи. Нужно сразу отметить два важнейших момента:
- Active Directory требует обязательного использования службы DNS.

Служба DNS

- Active Directory может работать с любой службой DNS, которая поддерживает SRV-записи, разрешает использование в именах символа подчеркивания ("_") и, желательно (но не строго обязательно), обеспечивает динамическое обновление ресурсных записей.
- Доменное пространство имен Active Directory полностью отображается на пространство имен DNS. Другими словами, иерархия доменов корпоративной службы DNS аналогична иерархии доменов Active Directory.

SRV-записи

- Служба доменных имен использует SRV-записи для определения местонахождения серверов, предоставляющих услуги определенных служб. Каждая SRV-запись, используемая для работы с Active Directory, представляет собой DNS-псевдоним службы, записанный в формате: _Service._Protocol.DnsDomainName где:
  - service — название сетевой службы, которая доступна на данном сервере (например: ldap, kerberos, gc, kpasswd);
  - Protocol — протокол, который клиенты могут использовать для подключения к указанной службе (tcp, udp);
  - DnsDomainName — доменное имя домена, к которому принадлежит указанный сервер

Служба DNS

- Например, для LDAP-сервера, принадлежащего к домену bru.by, DNS-имя службы будет выглядеть следующим образом: _ldap._tcp.bru.by. SRV-записи регистрируются в базе данных DNS-сервера непосредственно контроллерами домена. По умолчанию каждый контроллер домена регистрирует в базе данных DNS пятнадцать различных SRV-записей. Если контроллер домена выполняет также функции сервера глобального каталога, в базе данных службы DNS регистрируется двадцать SRV-записей.
- *Примечание*
  Перечень ресурсных записей, которые каждый контроллер домена Windows Server 2003 регистрирует на сервере DNS в процессе своей загрузки, хранится в файле %SysfemRoot%\system32\config\netlogon.dns.

Протокол аутентификации Kerberos

- Протокол аутентификации Kerberos является основным механизмом аутентификации, используемым в среде доменов Active Directory на базе Windows 2000 Server и Windows Server 2003. Этот протокол был разработан в Массачусетском технологическом институте (Massachusetts Institute of Technology, MIT) в начале 1980-х. Проблема аутентификации пользователя заключается в необходимости проверки того факта, что он является тем, за кого себя выдает.

Служба DNS

- Известно множество различных способов проверки подлинности личности, которые упрощенно можно разделить на две группы:
- проверка личности на факт соответствия некоторым индивидуальным характеристикам человека (проверка отпечатков пальцев, снимков радужки глаза, код ДНК и т. д.). Для применения этой группы методов аутентификации необходимо задействовать специальное оборудование;
- проверка личности на факт знания некоторого секрета (пароли, цифровые комбинации и последовательности). В данном случае под секретом понимается некая символьная или цифровая последовательность, факт знания которой позволяет судить о подлинности пользователя. Указанные методы аутентификации наиболее просты в технологическом исполнении. Именно эти методы получили широкое распространение в современных операционных системах. Протокол аутентификации Kerberos также относится к этой группе методов.

Компоненты службы Active Directory

- Рассмотрим структуру службы каталога. Active Directory представляет собой совокупность служб, обслуживающих обращения пользователей к каталогу. Каталог рассматривается как распределенная база данных, в которой хранятся сведения об объектах сети. Подсистемы службы каталога образуют некую структуру, в которой выделяют пять уровней.
- 1. **Интерфейсы доступа к каталогу**. Это самый верхний уровень службы каталога, отвечающий за непосредственное взаимодействие с приложениями пользователей. На данном уровне описаны все возможные методы доступа к каталогу. Можно рассматривать данный уровень как набор прикладных интерфейсов программирования (Application Program Interfaces, API), для взаимодействия с агентом каталога.
- 2. **Системный агент каталога (Directory System Agent, DSA)**. Любой клиент, подключающийся к каталогу, взаимодействует с DSA (спецификация X.500). Все запросы, поступающие от пользователей, обрабатываются агентом, он же возвращает клиентам результаты запросов.

Компоненты службы Active Directory

- 3. **Уровень базы данных (Database Layer)**. Данный уровень службы каталога осуществляет преобразование запросов пользователей в формат, приемлемый для расширяемой оболочки хранилища, представляющей реляционную базу данных. Однако вышестоящие уровни представляют содержимое каталога в виде древовидной структуры.
- 4. **Расширяемая оболочка хранилища (Extensible Storage Engine, ESE)**.
- Расширяемая оболочка хранилища представляет собой механизм управления реляционным хранилищем данных. Компания Microsoft рассматривает ESE в качестве стандартного механизма управления реляционными хранилищами и широко применяет ее в различных своих продуктах. ESE берет на себя все обязанности по обслуживанию запросов, поступающих от пользователей (и преобразованных в соответствующий формат на вышестоящем уровне) на извлечение данных из каталога и манипуляции ими. Можно представить ESE как систему управления базой данных (СУБД). При этом в качестве базы данных выступает непосредственно хранилище данных.
- 5. **Файлы хранилища (Data Store files)**. Хранилище данных реализовано в виде набора файлов, которые используются непосредственно для организации хранения данных каталога

Компоненты службы Active Directory

- Поскольку информация, содержащаяся в этих файлах, критически важна для функционирования Active Directory, доступ к ним имеет только расширяемая оболочка хранилища. В данном случае можно говорить о самом низшем уровне операций в рамках службы каталога. Именно на этом уровне происходит манипуляция с данными, содержащимися в каталоге.

Доменная структура Active Directory

- Понятие домена является ключевым для Active Directory. Домены выступают в качестве основного средства формирования пространства имен каталога.
- ***Домены***
- Операционные системы Windows традиционно использовали понятие "домена" для логического объединения компьютеров, совместно использующих единую политику безопасности. Домен традиционно выступает в качестве основного способа создания областей административной ответственности. Как правило, каждым доменом управляет отдельная группа администраторов. В Active Directory понятие домена было расширено. Перечислим задачи, которые решены путем формирования 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). Построение доменной иерархии является отличным способом реализации децентрализованной модели управления сетью, когда каждый домен управляется независимо от других. Для этого каждую административную единицу необходимо выделить в отдельный домен.

Доменная структура Active Directory

- **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. Поскольку эти вопросы решаются организационно на уровне всего домена, данный комплекс мер принято называть политикой учетных записей. (Эти политики нельзя определять на уровне подразделений!)
- **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. С другой стороны, применение доверительных отношений (trust relationships) позволяет обеспечить пользователям одного домена доступ к ресурсам других доменов.
- **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.

Доменная структура Active Directory

- **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. Изменения, произведенные в доменном разделе, реплицируются исключительно в пределах домена. Соответственно, выделение удаленных филиалов в отдельные домены может позволить существенно сократить трафик, вызванный репликацией изменений содержимого каталога. Необходимо отметить, однако, что домены являются не единственным (и даже не основным) способом формирования физической структуры каталога. Того же самого результата администратор может добиться за счет использования механизма сайтов.
- **Ограничение размера копии каталога**. Каждый домен Active Directory может содержать до миллиона различных объектов. 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.

Доменная структура Active Directory

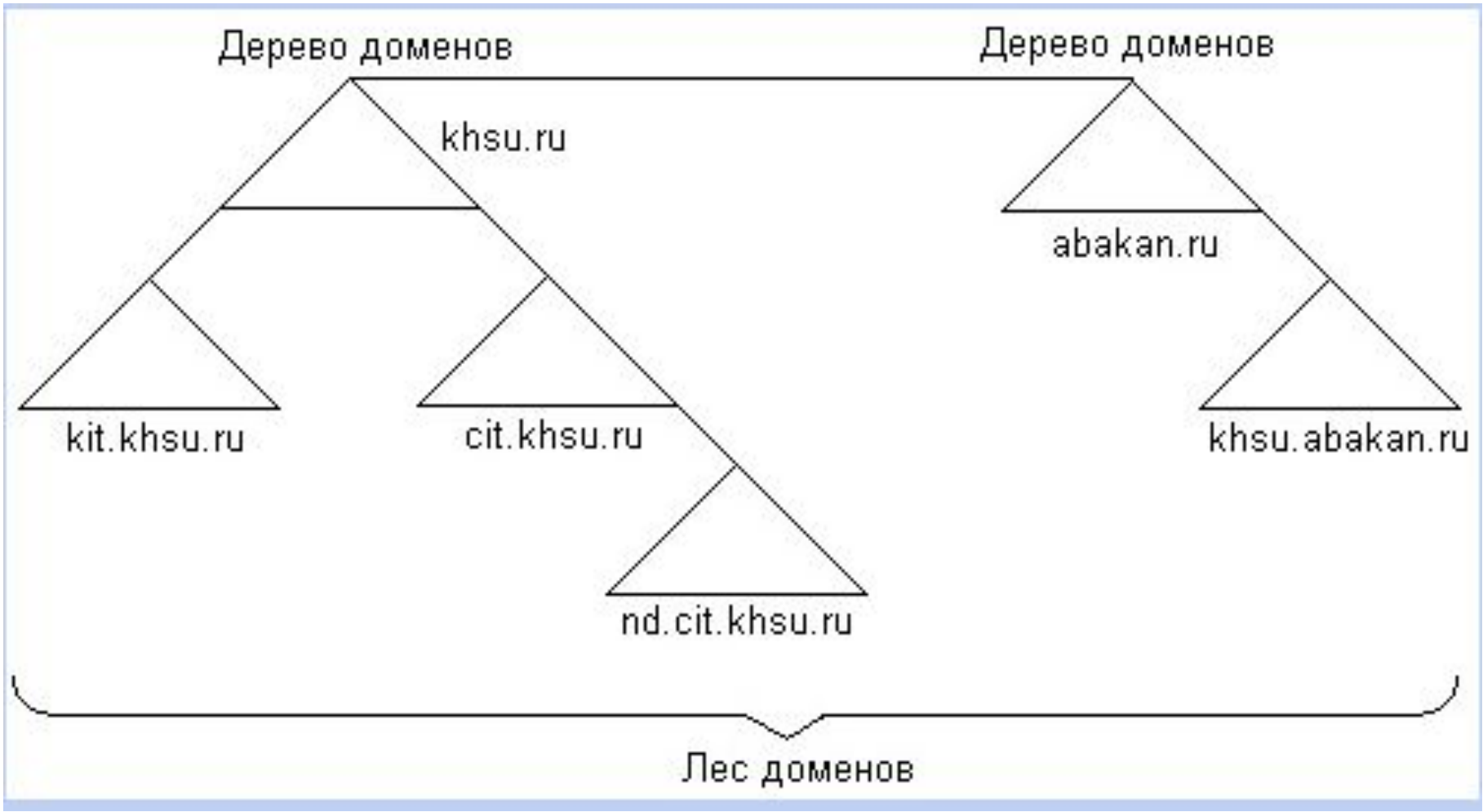
Иерархия доменов

- 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. Так, например, для домена kit, являющегося дочерним по отношению к домену bru.by, полное доменное имя будет записано в форме kit. bru.by. 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.
- *Примечание*
  Следует заметить, что каждому домену Active Directory помимо DNS имени сопоставлено уникальное NetBIOS-имя. Это имя используется для идентификации домена клиентами Windows 9x/NT.

Доменная структура Active Directory

- Совокупность доменов, использующих ***единую схему каталога***, ***называется лесом доменов (forest)***. Строго говоря, входящие в лес домены могут не образовывать "непрерывного" пространства смежных имен. Тем не менее, так же как и в случае пространства имен DNS, домены Active Directory могут образовывать непрерывное пространство имен. В этом случае они связываются между собой отношениями "родитель-потомок". При этом имя дочернего домена обязательно включает в себя имя родительского домена. Совокупность доменов, образующих непрерывное пространство смежных имен, называют деревом доменов (domain tree) (рис.7-50.1). Лес может состоять из произвольного количества деревьев домена.

Доменная структура Active Directory



- Рис. 7-50.1. **Дерево и лес доменов**
- ***Первое созданное в лесу доменов дерево является корневым деревом. Корневое дерево используется для ссылки на лес доменов.***

Доменная структура Active Directory

- ***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. Соответственно, первый домен, созданный в лесу доменов, называется корневым доменом леса (forest root domain).***
- 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. Особое внимание необходимо уделить вопросу именования доменов и, в частности, корневого домена. Для корневого домена лучше всего использовать доменное имя второго уровня. (bru.by). *Так как, именно домены второго уровня используются механизмом маршрутизации доменных суффиксов (в случае взаимодействия двух лесов доменов).*

Контроллеры домена

- ***Серверы Windows Server 2003, на которых функционирует экземпляр службы каталога Active Directory, называются контроллерами домена (domain controller, DC).***
- Контроллеры домена являются носителями полнофункциональных копий

Доменная структура Active Directory

- Контроллеры домена Windows Server 2003 выполняют ниже перечисленные 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 2003 может рассматриваться как Центр распределения ключей (KDC) Kerberos.
  - Администратор может осуществлять конфигурирование службы каталога и сети, подключившись к любому контроллеру домена Active Directory.

Специализированные роли контроллеров домена

- Служба каталога Active Directory использует модель репликации с множеством равноправных участников (multimaster replication). С точки зрения подсистемы репликации не имеет значения, какой из носителей осуществляет изменения в каталоге. Изменения могут быть произведены в любой из копий каталога. Однако существует определенный класс операций, которые должны выполняться только одним контроллером домена. Этот класс операций называется операциями с одним исполнителем (Flexible Single-Master Operations, FSMO). Если привлечь к выполнению подобных операций более одного контроллера домена, нельзя исключать возможность конфликтов. В определенных случаях подобные конфликты могут привести к нарушению целостности каталога.
- Рассмотрим пять существующих специализированных ролей.
  - **Владелец схемы** (Schema Master). Контроллер домена, осуществляющий изменения в схеме каталога. Существование только одного владельца (хозяина) схемы в пределах леса доменов исключает возможность конфликтов, связанных с ее изменением. Отказ владельца схемы приводит к тому, что выполнение операции расширения схемы станет невозможным.

Доменная структура Active Directory

- **Владелец доменных имен** (Domain Naming Master). Контроллер домена, отслеживающий изменения в структуре леса доменов. Любое изменение пространства имен доменов Active Directory (добавление, удаление, а также переименование доменов) осуществляется исполнителем данной роли. Тем самым гарантируется целостность пространства имен и уникальность его компонентов. Отказ исполнителя этой роли приводит к тому, что любое изменение пространства имен каталога станет невозможным
- **Владелец идентификаторов** (Relative ID Master). Контроллер домена, осуществляющий генерацию идентификаторов (глобальные идентификаторы, идентификаторы безопасности и т. п.). От идентификатора в первую очередь требуется уникальность. Самый простой способ гарантировать уникальность генерируемых идентификаторов — возложить обязанность исполнителя данной роли на один контроллер в домене. Отказ исполнителя данной роли приводит к тому, что создание объектов в домене станет невозможным.
- **Эмулятор основного контроллера домена** (PDC Emulator). Если домен находится на функциональном уровне Windows 2000 mixed, эмулятор основного контроллера домена (PDC) используется для обеспечения репликации изменений между контроллерами домена Windows NT и Windows 2000/Server 2003.

Доменная структура Active Directory

- ***Исполнитель роли фактически эмулирует домен Windows NT***. Поскольку в домене Windows NT допустимо наличие только одного основного контроллера, его эмулятор в домене Active Directory также может быть только один. На других функциональных уровнях эмулятор основного домена используется для изменения паролей учетных записей, а также играет ведущую роль в процессе синхронизации системных часов всех контроллеров домена. Эмулятор PDC по умолчанию выбирается оснасткой Group Policy Object Editor. Поэтому, если исполнитель данной роли недоступен, администратор может столкнуться с серьезными проблемами при редактировании объектов групповой политики.
- **Владелец инфраструктуры** (Infrastructure Master). Контроллер домена, отвечающий за структуру каталога. В процессе удаления или перемещения объектов один из контроллеров домена должен взять на себя обязанности по сохранению ссылки на данные объекты до тех пор, пока эти изменения не будут реплицированы на все остальные контроллеры домена. *Если в домене имеются несколько контроллеров домена, желательно не совмещать функции исполнителя данной роли и сервера глобального каталога. Лучше разнести эти функции на разные контроллеры домена, которые обязательно должны быть соединены высокоскоростным каналом. Если в домене имеется только один контроллер, этим требованием можно пренебречь.*

Доменная структура Active Directory

- По умолчанию все специализированные роли возлагаются на первый контроллер домена, установленный в новом лесе доменов. Аналогичным образом, в процессе создания нового домена первый установленный контроллер будет выбран в качестве исполнителя ролей, уникальных в пределах домена. Понижение контроллера домена, выбранного в качестве исполнителя специализированной роли, до выделенного сервера приводит к тому, что роли передаются другому контроллеру домена. ***При необходимости администратор может в любой момент передать обязанности исполнителя любой роли другому контроллеру домена.*** Это может потребоваться, например, в ситуации, когда ***планируется обновление аппаратного*** обеспечения сервера. В процессе нормальной передачи роли текущий исполнитель специализированной роли освобождается от исполнения специфических обязанностей и становится обычным контроллером домена. Одновременно с этим на другой контроллер домена, выбранного на роль нового исполнителя, возлагаются обязанности исполнителя специализированной роли.
- Если администратор не может обеспечить доступность сервера, являющегося исполнителем специализированной роли, либо восстановление его работоспособности не представляется возможным, он должен возложить обязанности исполнения данной роли на другой контроллер домена.

Доменная структура Active Directory

- Процесс принудительной передачи функций исполнителя специализированной роли другому контроллеру домена называется ***захватом, или присвоением роли*** (seize).

Доверительные отношения

- Доверительные отношения (trusts) представляют собой связь, устанавливаемую между доменами, позволяющую пользователям одного домена аутентифицироваться контроллером другого домена. Наличие механизма доверительных отношений позволяет организовывать совокупность доменов в некоторую структуру, в которой домены связываются между собой определенным образом отношениями доверия.
- Суть доверительных отношений между двумя доменами сводится к тому, что доверяющий домен (trusting domain) доверяет процесс аутентификации доверенному домену (trusted domain). Пользователь, аутентифицированный доверенным доменом, может получить доступ к ресурсам в доверяющем домене. Механизм аутентификации NTLM, архитектуры Windows NT, допускает создание только односторонних доверительных отношений. Служба каталога Active Directory допускает создание как односторонних, так и двусторонних доверительных отношений. Односторонние доверительные отношения реализуются посредством механизма аутентификации NTLM, как Windows NT. . Двусторонние доверительные отношения строятся на основе протокола аутентификации Kerberos v5 и обладают свойством транзитивности.

Доменная структура Active Directory

- Транзитивность доверительных отношений предполагает сквозную аутентификацию пользователей в цепочке доменов, связанных между собой подобными отношениями. Например, если домен A доверяет домену B, а домен B доверяет домену C, то между доменами A и C автоматически устанавливаются доверительные отношения (эти отношения неявные). Односторонние доверительные отношения NTLM не обладают свойствами транзитивности. Для создания отношений полного доверия между пятью доменами необходимо будет установить двадцать односторонних доверительных отношений. Аналогичного результата можно добиться при помощи всего лишь четырех двусторонних транзитивных доверительных отношений.
- Архитектура Windows Server 2003 позволяет использовать доверительные транзитивные отношения как для соединения доменов в пределах одного леса, так и для соединения разных лесов доменов. Кроме того, могут быть установлены доверительные отношения между различными областями Kerberos (Kerberos realms). Все поддерживаемые типы доверительных отношений перечислены в табл. 7-50.1.

Доменная структура Active Directory

Таблица 7-50.1***.*** *Доверительные отношения, поддерживаемые доменами на базе Windows Server 2003*

Доверительные отношения	Характеристика	Описание
Доверительные отношения внутри дерева	Двусторонние, транзитивные	Устанавливаются автоматически при создании в дереве нового домена. В рамках дерева доменов отношения описываются схемой "родитель-потомок"
Доверительные отношения внутри леса	Двусторонние, транзитивные	Устанавливаются автоматически при создании в существующем лесе нового дерева доменов. Фактически доверительные отношения устанавливаются между корневым доменом леса и создаваемым доменом, который будет являться корневым для нового дерева
Доверительные отношения между лесами доменов	Двусторонние или односторонние, транзитивные	Устанавливаются администраторами лесов доменов вручную. При этом администраторы сами решают — будут отношения двусторонними или односторонними
Перекрестные (shortcut) доверительные отношения	Односторонние или двусторонние, транзитивные	Устанавливаются между доменами различных деревьев, принадлежащих к одному лесу. Необходимость доверительных отношений данного типа не всегда очевидна, поскольку между доменами, принадлежащими одному лесу, через корневые домены автоматически устанавливаются неявные доверительные отношения. Перекрестные отношения доверия позволяют повысить эффективность взаимодействия между двумя доменами, уменьшая путь доверия (trust path). Путь доверия — последовательность переходов между доверяющими друг другу доменами, требуемых для аутентификации запроса. В случае неявных доверительных отношений этот путь может включать в себя несколько переходов, которые перекрестные отношения доверия позволяют избежать

Доменная структура Active Directory

Доверительные отношения с внешними доменами	Односторонние или двусторонние, нетранзитивные	Устанавливаются между доменами, принадлежащими к разным лесам, либо между доменом Windows Server 2003 и доменом Windows NT. Этот тип доверительных отношений может использоваться для соединения лесов, когда невозможно установить отношения доверия между лесами в целом (вследствие того, что один или оба леса не находятся на функциональном уровне Windows Server 2003)
Доверительные отношения между областями Kerberos	Односторонние или двусторонние, транзитивные или нетранзитивные	Устанавливаются между Windows Server 2003-доменом и областью Kerberos v5, реализованной не на базе Windows. Данный тип доверительных отношений может использоваться для обеспечения сквозной аутентификации на Windows и UNIX-системах

Доменная структура Active Directory

- *Примечание 1*
- *Доверительные отношения внутри леса и внутри дерева доменов устанавливаются системой автоматически, в процессе создания домена или дерева доменов. Администратор не может как-либо отозвать их или удалить. Все остальные типы доверительных отношений создаются администратором вручную.*
- *Примечание 2*
- *Для использования доверительных отношений не имеет значения, какой механизм аутентификации используется клиентом. Даже если клиент не поддерживает протокол Kerberos, он может быть аутентифицирован через двусторонние доверительные отношения.*

Доверительные отношения между лесами доменов

- Процесс создания отношений между лесами доменов заслуживает особого внимания. Организация взаимодействия двух лесов доменов, соединенных между собой отношениями доверия, имеет свои специфические моменты.

Доменная структура Active Directory

- Механизм маршрутизации суффиксов гарантирует, что все запросы аутентификации, адресуемые домену второго уровня, будут маршрутизироваться соответствующему домену. Дочерние домены, подключаемые к доменам второго уровня, наследуют от них информацию, необходимую для маршрутизации суффиксов. Поэтому они также смогут выполнить маршрутизацию запроса на аутентификацию пользователя.

Подразделения (Организационные единицы)

- Подразделения, или организационные единицы (organizational unit) представляют собой объекты каталога контейнерного типа, посредством которых администратор может организовать объекты в соответствии с некоторой логической структурой вычислительной сети. Основное предназначение подразделений состоит в логической организации сетевых ресурсов с целью наиболее эффективного управления ими. Рассмотрим задачи, решаемые с помощью организационные единицы OU.
  - **Формирование административной иерархии**. Механизм подразделений наряду с доменами может быть использован как средство формирования административной иерархии. Администраторы уровня корпорации принимают глобальные решения в рамках всего леса доменов. Администраторы доменов осуществляют управление доменами. ***При этом они передают (делегируют) определенным пользователям часть своих полномочий на уровне подразделений*** — это полномочия на управление объектами, расположенными внутри этих подразделений. При этом пользователи, которым делегированы административные полномочия, могут реализовать их исключительно внутри своего подразделения.

Доменная структура Active Directory

- **Отражение организационной структуры предприятия**. Механизм подразделений может использоваться для организации объектов каталога в соответствии с их географическим расположением или с принадлежностью к некоторому структурному подразделению предприятия. Например, реализовав вычислительную сеть университета в виде домена, можно создать для каждого факультета свое подразделение. Для кафедр, имеющихся на каждом факультете, можно также создать свои подразделения.
- **Управление процессом применения групповых политик**. ***Групповые политики могут быть применены на трех уровнях: на уровне домена, на уровне сайта и на уровне подразделений.*** Если необходимо в рамках одного домена реализовать несколько различных групповых политик, можно использовать иерархию подразделений.
- **Распределение ответственности**. Администратор может разместить объекты одного класса в отдельных подразделениях. Такой шаг позволяет распределить обязанности по управлению домена между администраторами низшего звена. Например, один из них ответственен за управление пользователями, второй - за управление компьютерами, третий же осуществляет публикацию принтеров.
- **Управление доступом к объектам**. Администратор может назначать права доступа к подразделениям. Соответственно, администратор может управлять уровнем доступа к объектам каталога, поместив их внутрь подразделения и предоставив определенным категориям пользователей соответствующие разрешения на доступ к его содержимому. Например, администратор помещает объекты, ассоциированные с информацией о контакте, внутрь подразделения, доступ к которой имеют только менеджеры отдела продаж и руководители компании.

Доменная структура Active Directory

- Каждый домен реализует собственную иерархию подразделений. Подразделения, принадлежащие к различным доменам, никак не связаны между собой. Применение подразделений позволяет разместить все объекты в одном доменном контексте имен, независимо от сложности иерархии подразделений. Как следствие, перемещение объектов (особенно таких, как пользователи) между подразделениями требует меньших административных усилий, чем перемещение между доменами. С другой стороны, разделение пространства имен на доменные контексты позволяет сократить трафик, вызванный репликацией.

Группы

- Подразделения являются не единственным механизмом, который администратор может использовать для группировки объектов по некоторому признаку. Объекты, ассоциированные с пользователями, компьютерами и контактной информацией, могут быть объединены в специальные группы (groups). Это позволяет упростить процесс управления, поскольку администратор может в процессе управления сослаться на всю группу, а не указывать отдельные объекты. Наиболее часто группы упоминаются в контексте объединения пользователей. Тем не менее, необходимо всегда помнить, что группа может включать в себя объекты следующих типов:
  - ***пользователи (users);***
  - ***компьютеры (computers);***
  - ***контакты (contacts).***

Доменная структура Active Directory

- Active Directory позволяет объединять объекты в группы двух типов: ***группы безопасности (security groups)*** и ***группы рассылки (distributed groups).***
- Группы безопасности рассматриваются подсистемой безопасности в качестве своих субъектов. Другими словами, они могут использоваться для разграничения доступа к ресурсам сети. Выдавая разрешение на доступ к объекту определенной группе, администратор автоматически разрешает доступ к данному объекту всем членам данной группы.
- *Внимание*
- *Группы безопасности могут также использоваться для ограничения действия групповой политики.*
- Группы рассылки изначально ориентировались на использование почтовой системой, как средство одновременной передачи сообщения некоторому коллективу пользователей. В настоящее время механизм групп рассылок Active Directory используется в почтовой системе Microsoft 2000 Exchange. С каждой группой объектов связано понятие области действия (group scope). Область действия определяет, в какой части леса доменов на данную группу можно ссылаться. Существует три области действия групп:
- доменная область действия (domain local scope);
- глобальная область действия (global scope);
- универсальная область действия (universal scope).

Доменная структура Active Directory

- На функциональных уровнях домена Windows 2000 native и Windows Server 2003 становится доступной универсальная область действия. Кроме того, становится доступной возможность вложенности групп. На этих функциональных уровнях администратор может без труда конвертировать группы из одного типа в другой. Охарактеризуем группы каждой области действия на этих функциональных уровнях.
  - **Группы с доменной областью действия**. Эти группы доступны исключительно в пределах того домена, в котором они определены. Членами группы с доменной областью действия могут являться объекты, а также другие группы с любыми областями действия. Объекты, а также группы с глобальной и универсальной областью действия могут принадлежать к любому домену леса. В состав группы могут также входить группы с доменной областью действия, принадлежащие к тому же домену.
  - **Группы с глобальной областью действия**. Группы с данной областью действия (глобальные группы)доступны в рамках всего леса доменов. *Членами группы могут являться объекты и группы с глобальной областью действия*, принадлежащие к тому же домену, что и сама группа.
  - **Группа с универсальной областью действия**. (универсальные группы) Эти группы также доступны в рамках всего леса доменов. В состав группы могут входить объекты, а также *группы с универсальной или глобальной областью действия, принадлежащие к любому домену леса.*

Доменная структура Active Directory

- С каждой группой в момент создания ассоциируется объект каталога, значения атрибутов которого определяют его (группы) свойства. Один из атрибутов содержит список всех членов группы. В случае изменения состава группы будут реплицироваться не все значения атрибута (в случае, если группа насчитывает тысячи объектов, подобная репликация может вызвать заметный трафик), а только произведенные изменения. В данном случае речь идет о механизме репликации связанных значений (linked value replication). Этот механизм будет работать только в случае, когда лес доменов находится на функциональном уровне Windows Server 2003.
- *Примечание*
- *В данном разделе речь велась о группах Active Directory. Существуют ещё локальные группы компьютеров с ОС Windows NT/2000/2003/XP. Эти группы доступны только в пределах того компьютера, к которому они принадлежат, как только компьютер становится контроллером домена эти группы исчезают.*

Физическая структура каталога

- Вычислительная сеть крупных компаний представляет собой совокупность подсетей, соединенных между собой коммуникационными линиями с различной пропускной способностью. В этом случае на передний план выходит задача оптимизации трафика через эти коммуникационные линии. Недостаточная пропускная способность отдельных коммуникационных линий может стать причиной возникновения проблем с поиском объектов, аутентификацией пользователей, а также репликацией изменения каталога.

- ***Сайты***

- Если в сети несколько LAN, соединенных региональной сетью (wide area network, WAN), вы, вероятно, создадите по одному сайту для каждой LAN. Сайт Windows Server 2003 — это группа контроллеров доменов, которые находятся в одной или нескольких IP-подсетях и связаны скоростными и надежными сетевыми соединениями. Под скоростным подразумеваются соединения не ниже 1 Мбит/с. Иначе говоря, сайт обычно соответствует границам локальной сети (local area network, LAN).
- Сайты представляют собой самостоятельные образования, напрямую не зависящие от доменной структуры вашей сети. Сайты не являются частью пространства имен каталога, они лишь характеризуют его физическую структуру. Это означает, что принадлежность объекта к

Физическая структура каталога

- *Например, в зависимости от того, на каком компьютере пользователь входит в сеть, он может рассматриваться как находящийся то в одном, то в другом сайте. Поскольку структура сайтов реализуется независимо от структуры доменов, один домен может быть разделен на несколько сайтов и, напротив, один сайт может быть образован фрагментами нескольких доменов.*
- **Сайты во-первых, в основном используются для управления трафиком репликации между LAN** в крупных корпоративных сетей. Внутри LAN, как правило устанавливаются свои контроллеры доменов, в том числе и глобальные, образующие сайт. Контроллеры доменов внутри сайта могут свободно реплицировать изменения в базу данных Active Directory всякий раз, когда происходят такие изменения. Однако контроллеры доменов в разных сайтах сжимают трафик репликации и передают его по определенному расписанию, чтобы уменьшить сетевой трафик. Различия в способах репликацией связано с тем, что внутри сайта применяются скоростные линии связи, а между сайтами более медленные линии WAN.
- Во-вторых, сайты позволяют сократить трафик во время аутентификации пользователей, особенно если речь идет о большом количестве пользователей (например, когда все сотрудники компании утром приходят на работу).

Физическая структура каталога

- . Администратор должен обеспечить возможность аутентификации пользователей сайта, даже если коммуникационные линии, связывающие сайт с остальной сетью, заняты или недоступны.
- При входе пользователя в сеть, его аутентификация осуществляется ближайшим контроллером домена, который должен располагаться в том же сайте, что и аутентифицируемый пользователь. В процессе аутентификации пользователи и другие компоненты службы каталога обращаются к серверу глобального каталога для поиска объектов.. Поэтому рекомендуется в каждом сайте размещать как минимум один сервер глобального каталога. В случае, если доступ к серверу глобального каталога осуществляется через линии связи с низкой пропускной способностью, многие операции службы каталога будут выполняться медленно.
- В ходе создания леса доменов мастером установки автоматически создается сайт по умолчанию с именем Defauit-First-site-Name. Формируя физическую структуру сети, администратор должен самостоятельно создать новые сайты и задать для них границы, создав объекты, ассоциированные с имеющимися подсетями.
- В процессе создания нового контроллера на основании выделенного ему IP-адреса служба каталога автоматически отнесет его к соответствующему сайту. При этом в разделе конфигурации каталога в рамках данного сайта будет создан объект класса Server, ассоциируемый с контроллером домена

Транспорт репликации

- Понятие транспорта репликации характеризует механизмы и протоколы, используемые для передачи изменений. Active Directory может использовать в качестве транспорта RPC over IP ("RPC поверх IP") (RPC remote procedure calls -удаленный вызов процедур) или протокол SMTP. В табл. 7-50.2 перечислены правила использования различных транспортных протоколов для репликации разных разделов.

Таблица 7-50.2. *Транспорты репликации*

Разделы каталога	Внутри сайта	Между сайтами	
		Один домен	Разные домены
Доменный раздел каталога	RPC over IP	RPC over IP	-
Разделы конфигурации и схемы	RPC over IP	RPC over IP	SMTP
	Трафик не сжимается	Трафик сжимается	

Физическая структура каталога

- Протокол RPC over IP обеспечивает низкоскоростную двухточечную синхронную репликацию всех разделов каталога. Этот транспорт лучше всего подходит для ситуаций, когда узлы соединены надежными линиями связи с низкой вероятностью потери пакетов. Протокол SMTP используется для низкоскоростной асинхронной репликации между сайтами и поддерживает репликацию только для разделов конфигурации и схемы, а также для глобального каталога. Репликация изменений каталога между контроллерами домена, принадлежащими к одному узлу, всегда осуществляется посредством протокола RPC over IP. Если контроллеры домена располагаются в различных сайтах, но принадлежат к одному домену, то репликация между ними осуществляется также при помощи протокола RPC over IP. Если контроллеры домена расположены в различных сайтах и принадлежат к разным доменам, то для репликации изменений между ними используется протокол SMTP, функционирующий поверх IP.

Соединения сайтов

- Топология репликации формируется при помощи специального класса объектов — соединений (connections). Соединение представляет собой однонаправленное соглашение между двумя контроллерами домена о передаче изменений. С каждым соединением ассоциируется объект в разделе конфигурации каталога. Атрибуты объекта, ассоциированного с соединением, определяют передающего партнера по репликации, а также расписание репликации и используемый при этом транспорт. Все соединения автоматически генерируются системным сервисом Knowledge Consistency Checker, KCC, который проверяет существующую топологию и доступность имеющихся соединений и при необходимости вносит соответствующие коррективы. Контроллеры домена, расположенные в различных сайтах и взаимодействующие между собой в процессе репликации, называются мостовыми серверами (bridgehead server). В каждом сайте один из контроллеров домена берет на себя обязанности по управлению входящими соединениями для всех мостовых серверов сайта. Этот контроллер домена называется генератором топологии между сайтами (Inter-Site Topology Generator, ISTG). Если контроллер домена, выполняющий функции ISTG, становится недоступен (например, выходит из строя), эта функция автоматически возлагается на другой контроллер домена.

Физическая структура каталога

- В случае репликации между сайтами используется термин связь сайтов (site link), который описывает соединения двух и более узлов, способных обмениваться информацией при помощи единого транспорта. Связь узлов используется для задания стоимости соединения (cost), расписания репликации и транспорта. Механизм стоимостей позволяет оценить связь сайтов с точки зрения доступности коммуникационных линий и их пропускной способности. Если имеется несколько связей сайтов, для репликации будет выбрана та, что обладает меньшим значением стоимости.

Несколько связей сайтов, использующих единый транспорт, образуют связующий мост между узлами (site link bridge). Использование связующих мостов между сайтами полезно в больших сетях, поскольку избавляет от необходимости описывать все возможные комбинации соединений между каждым из сайтов.

- **Расписание репликации и**зменений каталога может быть инициирован одним из двух способов:
  - уведомление об изменениях (change notification) используются между контроллерами домена внутри сайта. Если на некотором контроллере модифицируется атрибут какого-нибудь объекта, данный контроллер посылает уведомление первому партнеру по репликации, и это происходит через определенное время (по умолчанию 5 минут). После этого партнер запрашивает изменения у контроллера-источника изменений (originating DC) и получает их;
  - изменения реплицируются между сайтами согласно расписанию (schedule). Эти расписания определяются с помощью оснастки Active Directory Sites and Services.

- **Серверы глобального каталога**

Глобальный каталог (global catalog) представляет собой базу данных, содержащую фрагменты всех доменных контекстов имен, образующих пространство имен каталога. Глобальный каталог является важной и неотъемлемой частью Active Directory. В глобальном каталоге содержатся сведения обо всех объектах, принадлежащих к доменным контекстам имен. Однако в глобальном каталоге хранятся не все объекты целиком, а только подмножество их атрибутов. Выбираются те атрибуты, которые чаще всего присутствуют в запросах пользователей. Атрибуты, размещаемые в глобальном каталоге, определяются в рамках схемы каталога. У каждого класса атрибутов имеется параметр is Member of Fartial Attribute Set. Если значение этого параметра равно TRUE, атрибут будет размещен в глобальном каталоге. Администратор может определить для размещения в глобальном каталоге дополнительные атрибуты. Однако необходимо помнить, что расширение числа атрибутов, заносимых в глобальный каталог, приводит к росту его объема. Соответственно дороже обходится его обслуживание. Процесс добавления нового атрибута для размещения в глобальном каталоге влечет за собой синхронизацию всех его реплик.

Физическая структура каталога

- Если лес находится на функциональном уровне Windows Server 2003, добавление нового атрибута приведет к репликации только этого атрибута на все носители глобального каталога. Если же лес находится на функциональном уровне Windows 2000, добавление нового атрибута приводит к полной синхронизации всех реплик глобального каталога. Контроллер домена, выступающий в качестве носителя глобального каталога, принято называть сервером глобального каталога (global catalog server). Необходимо обратить внимание на то, что функции сервера глобального каталога могут быть возложены только на контроллер домена. При этом на контроллере домена создается дополнительный раздел, который используется для размещения базы данных глобального каталога. Сервер глобального каталога выполняет две функции.
  - **Поиск объектов**. Клиенты могут обращаться к глобальному каталогу с запросами на поиск объектов, основываясь на известных значениях атрибутов. Глобальный каталог хранит в себе информацию обо всех доменных разделах леса. Фактически использование сервера глобального каталога является единственным способом осуществлять поиск объектов по всему лесу доменов.

Физическая структура каталога

- **Аутентификация пользователей**. Сервер глобального каталога предоставляет информацию о членстве пользователя в различных группах с универсальной областью действия (universal group). Эта информация требуется в процессе аутентификации пользователя. Именно на основании членства пользователя в тех или иных группах происходит назначение прав доступа. Более того, сервер глобального каталога необходим в том случае, если для регистрации в системе пользователь использует свое основное имя. Разрешение основного имени осуществляется непосредственно сервером глобального каталога. Если сервер глобального каталога оказывается недоступным, контроллер домена, осуществляющий аутентификацию, не будет располагать данными, необходимыми для авторизации пользователя. В результате пользователю будет отказано в регистрации. Исключение составляют члены группы Domain Admins (Администраторы домена), аутентификация которых осуществляется даже в том случае, когда сервер глобального каталога недоступен.

- В лесу доменов должен быть как минимум один сервер глобального каталога. Поэтому по умолчанию обязанности сервера глобального каталога возлагаются на первый контроллер домена, установленный в лесу доменов. Тем не менее, любой контроллер домена может быть сконфигурирован в качестве сервера глобального каталога. Это может быть сделано в силу различных причин. Например, чтобы снизить нагрузку на медленные линии связи, обычно принято устанавливать как минимум по одному серверу глобального каталога для каждого узла.

Механизмы репликации каталога

- Каталог рассматривается как база данных, распределенная между множеством носителей. Каждый контроллер домена является носителем копии каталога. При этом каждая из копий является полнофункциональной. Это означает, что каждый контроллер домена может вносить изменения в собственную копию каталога. Все произведенные изменения должны быть автоматически распространены на другие копии. Служба каталога должна располагать механизмом, который бы обеспечил поддержание отдельных копий каталога в согласованном состоянии. В подобных случаях традиционно используют механизм синхронизации, основанный на обмене между носителями копии каталога информацией об изменениях. Поскольку на каждый носитель каталога передается реплика изменений, этот процесс получил название репликации (replication) изменений.

Разделы каталога

- С точки зрения механизма репликации Active Directory представляет собой не цельную иерархическую структуру, а отдельные фрагменты. Каждый фрагмент, являясь частью каталога, представляет собой самостоятельное дерево.

Физическая структура каталога

- В терминологии службы Active Directory подобная совокупность ветвей называется прилегающим поддеревом (contiguous subtree) или контекстом имен (naming context).
  Разделение пространства имен каталога на фрагменты позволяет оптимизировать процесс синхронизации копий каталога между множеством его носителей. Это достигается за счет того, что в каждом контексте имен хранится определенного вида информация. По умолчанию каталог Active Directory поделен на три контекста имен, которые называются разделы каталога (directory partition):
  - **доменный раздел каталога** (Domain partition) используется для размещения информации о сетевых ресурсах, принадлежащих к определенному домену. Реплики доменного раздела располагаются на всех контроллерах указанного домена. Соответственно изменения, происходящие в этом разделе, реплицируются только на эти реплики;
  - **раздел схемы** (Schema partition). Понятие схемы каталога было дано в начале главе. Для ее хранения используется специальный раздел каталога. Поскольку схема является общей для всех доменов леса, изменения в ней распространяются на все носители копии каталога;
  - **раздел конфигурации** (Configuration partition) содержит информацию, используемую различными системными службами, в том числе и самой службой каталога. В частности, в разделе конфигурации хранится информация, описывающая топологию репликации между контроллерами домена. Эта информация необходима для успешного функционирования службы каталога в целом, поэтому изменения в данном разделе реплицируются на [illegible]носители каталога в лесе доменов.

Физическая структура каталога

- Реплики трех указанных разделов каталога присутствуют в обязательном порядке на всех контроллерах домена. Доменный раздел каталога индивидуален для каждого домена. Реплики раздела схемы и раздела конфигурации одинаковы для всех контроллеров домена в лесу.
- *Примечание*
  На серверах глобального каталога присутствует еще один раздел — содержащий подмножество атрибутов объектов всех доменных разделов каталога. При этом данный раздел доступен только для чтения информации.
- Любой контроллер домена Active Directory может производить изменения в собственных репликах в любой момент времени. При этом все произведенные изменения будут синхронизированы с другими репликами. Подобная модель репликации получила название репликация с множеством равноправных участников (multimaster replication).

Разделы приложений

- Дополнительно к перечисленным разделам, в каталоге Active Directory на базе систем Windows Server 2003 могут быть созданы специализированные разделы, которые получили название разделов приложений (application directory partitions). Разделы приложений могут быть созданы при необходимости администратором либо непосредственно самими приложениями. В разделе приложений могут быть размещены любые объекты, определения которых содержатся в схеме, за исключением субъектов подсистемы безопасности (таких, например, как учетные записи пользователей или компьютеров).

Физическая структура каталога

- Служба каталога Active Directory, реализованная на базе Windows 2000 Server, использовала для размещения информации приложений доменные разделы и раздел конфигурации. Это приводило к тому, что информация приложений реплицировалась на все контроллеры домена (даже когда этого и не требовалось). Изменение этой информации приводило к синхронизации всех копий каталога. В крупной корпоративной сети подобное решение зачастую становилось причиной интенсивного трафика репликации. Разделы приложений были реализованы в Windows Server 2003. Их использование позволяет сократить накладные расходы, вызванные репликацией. В отличие от трех основных разделов каталога, реплицируемых на все контроллеры домена, разделы приложений могут располагаться на строго оговоренных контроллерах. Администратор может перечислить контроллеры домена, на которые необходимо разместить копии определенного раздела каталога. В данном вопросе основным является потребность приложения в доступности данных. Приложениям зачастую не требуется, чтобы размещенная ими в каталоге информация была доступна повсеместно в сети. Существуют приложения, применение которых ограничено отдельным доменом или деревом доменов. Если приложение, для которого создается раздел, используется только в двух доменах леса, то копии раздела приложения должны быть размещены только на контроллерах домена двух указанных доменов. Контроллеры других доменов не будут содержать данный раздел.

Физическая структура каталога

- Имеется два встроенных раздела приложений, которые используются службой DNS для размещения содержимого зон, интегрированных с Active Directory. Это разделы ForestDnsZones.forestName и DomamDnsZones.forestName. При этом вместо суффикса forestName в имени раздела указывается DNS-имя корневого домена леса. Существует три способа создания раздела приложений.
  - **Использование утилиты NtdsUtil.exe**. Эта утилита командной строки представляет собой основной инструмент администратора службы каталога Active Directory, используемый для диагностики и разрешения проблем. Этот способ предполагает создание раздела приложения администратором вручную.
  - **Использование утилиты Ldp.exe**. Данная утилита позволяет администратору работать с любым LDAP-совместимым каталогом (каким, по сути, является Active Directory). Этот способ, так же как и предыдущий, предполагает создание раздела приложения администратором вручную.
  - **Использование интерфейса прикладного программирования ADSI (Active Directory Service Interfaces)**. Приложения, использующие данный интерфейс для взаимодействия со службой каталога Active Directory, могут создавать разделы приложений в каталоге самостоятельно (например, в процессе развертывания).

Топология репликации

- Процесс репликации предполагает обмен изменениями в разделах каталога между отдельными участниками. Для обозначения односторонней передачи данных от одного партнера по репликации к другому используется термин соединение (connection). Соединение представляет собой однонаправленное соглашение о репликации, заключенное между двумя контроллерами домена. Одним из наиболее ответственных моментов в процессе функционирования подсистемы репликации службы каталога является формирование инфраструктуры соединений между имеющимися контроллерами домена. Подобная инфраструктура называется топологией репликации (replication topology). Каждый раздел каталога строит свою собственную топологию репликации.

  За формирование топологии репликации отвечает специальный системный процесс Knowledge Consistency Checker, КСС. Этот процесс выполняется на всех контроллерах домена, автоматически генерируя топологию репликации. При этом КСС основывается на информации о физической структуре каталога. Периодически активизируясь, КСС проверяет доступность существующих соединений. Основываясь на полученных данных, КСС может переформировать топологию репликации для некоторого раздела каталога. Именно КСС отвечает за установление соединения с партнером по репликации. Соединения генерируются автоматически, хотя служба каталога допускает определение соединений непосредственно администратором.

Физическая структура каталога

- *Примечание*
  Необходимо обратить внимание на то, что хотя топология репликации формируется индивидуально для каждого раздела каталога, единственное соединение с партнером по репликации может быть использовано для передачи ему сведений об изменениях сразу в нескольких разделах каталога.
- Отдельно следует сказать про формирование топологии репликации для разделов приложений. Хотя место размещения реплик разделов приложений осуществляется администратором вручную, генерация и поддержание топологии репликации для этих разделов осуществляется наблюдателем показаний целостности автоматически.

Служба репликации файлов

- Каталог рассматривается как централизованное место хранения информации о сетевых ресурсах. Однако в силу определенных причин некоторая часть информации не может быть размещена в каталоге. Например, старые версии операционных систем (Windows 9x/NT) используют специальный сетевой ресурс NETLOGON для размещения информации, необходимой для регистрации в сети. Эта папка используется для размещения перемещаемых или обязательных профилей пользователей, сценариев регистрации, системных политик и т. п. Эта информация жизненно необходима для корректного функционирования сети. При этом требуется, чтобы эта папка присутствовала на всех контроллерах домена.

Физическая структура каталога

- Служба репликации файлов (File Replication Service, FRS) представляет собой механизм репликации с множеством равноправных участников, осуществляющий синхронизацию содержимого системного тома SYSVOL между контроллерами домена. Том SYSVOL создается на каждом сервере непосредственно в ходе повышения его до контроллера домена и используется для размещения системных файлов общего доступа. В частности, именно внутри него располагается уже упоминавшаяся папка NETLOGON. Помимо этого, в томе SYSVOL размещаются настройки объектов групповых политик, системные политики контроллеров домена и сценарии регистрации.
- *Примечание*
  Поскольку служба репликации файлов использует модель с множеством равноправных участников (multimaster replication), изменение содержимого реплицируемой папки может быть произведено любым участником. При этом в цепочке серверов, участвующих в репликации, нельзя выделить какой-то один, координирующий процесс репликации. Каждый участник может изменить содержимое тома SYSVOL и передать сведения об изменении содержимого любым другим участникам. Служба репликации файлов может также осуществлять синхронизацию содержимого набора реплик распределенной файловой системы DFS (см. главу 8 "Работа с дисковыми ресурсами").

Создание системного тома SYSVOL

- Том SYSVOL создается непосредственно в ходе повышения сервера до контроллера домена. Когда вы устанавливаете первый контроллер домена в сети, в этой папке на базе имеющихся шаблонов создаются объекты политик по умолчанию. Служба FRS извещает службу NETLOGON о том, что системная папка доступна для общего доступа. Только после этого сервер может использоваться как контроллер домена.
  В случае установки последующих контроллеров домена после создания тома SYSVOL служба репликации файлов осуществляет его наполнение. Содержимое тома копируется с уже существующего контроллера домена. Только по окончании этого процесса наполнения сервер будет объявлен контроллером домена.
- *Внимание*
  По умолчанию том SYSVOL располагается непосредственно внутри системной папки %SystemRoot%. Однако в процессе повышения роли сервера до контроллера домена администратор может указать любое другое место расположения этого тома. Единственное условие — том должен располагаться на NTFS-разделе.

Физическая структура каталога

Служба каталога и служба FRS

- Для своей работы служба FRS запрашивает информацию о физической структуре службы каталога, серверах каталога и соединениях между ними. Другими словами, служба репликации файлов не создает своей инфраструктуры, а использует топологию репликации каталога для собственных целей. В частности, служба репликации файлов задействует объекты, ассоциированные с соединением (connection objects), для передачи файлов. При этом учитывается расписание репликации, определенное в рамках этих объектов. Такой подход позволяет упростить схему репликации, исключив дублирование схожих структур.
- *Внимание*
  Тем не менее, необходимо понимать, что фактически механизм репликации службы каталога и служба репликации файлов представляют собой две различных службы, действующие независимо друг от друга.

Групповые политики

- В настоящее время практически любой производитель системного программного обеспечения встает перед проблемой снижения общей стоимости владения системой (total cost ownership). Эта проблема заключается в том, что развитие и связанное с этим усложнение технологий приводит к увеличению затрат на администрирование. В таких условиях корпорации вынуждены либо постоянно увеличивать штат администраторов, либо упрощать процесс управления за счет отказа от тех или иных сервисов и технологий.

  Каждый разработчик подходит к решению этой проблемы по-своему. Компания Microsoft традиционно предлагает целый набор решений, позволяющих упростить процесс управления сетевыми ресурсами, а следовательно снизить общую сумму административных затрат.
- Одной из проблем, встающих перед системным администратором, является проблема формирования индивидуального окружения пользователей. Начиная с Windows 2000, для формирования окружения пользователей используется механизм групповых политик (group policy). Под групповой политикой понимается совокупность параметров и настроек системы, определяющая конкретное окружение пользователя. Администратор может использовать механизм групповых политик для централизованного управления средой пользователей.

Физическая структура каталога

- **Управление настройками операционной системы**. Все параметры операционной системы, определяющие ее функциональность, а также определяющие режимы работы ее служб и их настройки, хранятся в системном реестре. Посредством механизма групповой политики администратор может контролировать содержимое отдельных, наиболее важных ключей реестра.
- **Назначение сценариев**. С помощью групповой политики администратор может определить сценарии, которые будут выполняться при запуске и выключении компьютера, а также при входе пользователя в систему и выходе из нее.
- **Определение параметров системы безопасности**. С каждым пользователем или компьютером может быть ассоциирован определенный набор настроек системы безопасности. В данном случае принято говорить о политике безопасности (security policy) определяемой в контексте групповой политики. Политика безопасности позволяет однообразно конфигурировать большое количество субъектов безопасности. Например, определить уровень доступа к системному реестру или задать порядок осуществления аудита событий.
- **Управление приложениями**. Используя механизм групповой политики, администратор может назначать и публиковать приложения, выполнять их централизованное обновление и восстановление.
- **Перенаправление пользовательских папок**. Папка **My Documents** (Мои документы) традиционно рассматривается как место хранения пользовательских документов. В корпоративной сети, в которой работает множество мобильных пользователей, актуальной становится проблема доступности этих документов. Посредством механизма групповой политики администратор может задать перенаправление всех обращений пользователей к этой папке на некоторый сетевой ресурс.

Физическая структура каталога

Объекты групповой политики

- Параметры групповой политики хранятся в виде объектов групповой политики (Group Policy Object, GPO). Эти объекты хранятся в каталоге подобно другим объектам. Для именования объекта групповой политики используется глобальный уникальный идентификатор (GUID). Различают два вида объектов групповой политики — объекты групповой политики, создаваемые в контексте службы каталога, и локальные объекты групповой политики. Локальные объекты групповой политики (Local Group Policy Object, LGPO) создаются в процессе установки операционной системы Windows 2000/XP или Windows Server 2003. Локальный объект GPO используется в том случае, когда компьютер не включен в состав домена. Как только компьютер подключается к домену, компьютер и пользователь, работающий на нем, подпадают под действие объектов GPO, определенных в контексте данного домена, и параметры, заданные локальным объектом GPO, могут быть переопределены на более высоком уровне (на уровне сайта, домена или подразделения). Объекты групповой политики размещаются в каталоге в специальных контейнерах групповой политики (Group Policy Container, GTC). Кроме того, для размещения файлов, связанных с объектами GPO, система использует специальную папку SYSVOL\sysvol\<имя домена>\policies. В этой папке размещаются шаблоны групповой политики (Group Policy Template, GPT). Шаблон групповой политики представляет собой папку, в качестве- имени которой используется глобальный уникальный идентификатор (GUID) соответствующего объекта групповой политики. В шаблоне групповой политики размещаются административные шаблоны, сценарии и параметры безопасности.