Методология внедрения Microsoft Active Directory

1 ЛЕКЦИЯ: ВВЕДЕНИЕ В ACTIVE DIRECTORY

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

Цель лекции: Указать потребность в использовании единого инструмента для организации и упрощения доступа к информационным ресурсам. Дать общее представление о каталоге и службе каталогов, привести их назначение, основные функции и задачи, сформулировать преимущества использования Active Directory.

Вне зависимости от топологии сети компании, реальной инфраструктуры и организационной структуры географически распределенных филиалов, а также от имеющейся в компании разнородной информационной среды, существует общая методология развертывания и применения службы Active Directory.

1.1 Определение каталога и службы каталогов

Сначала мы должны определить, что такое служба каталогов вообще, каковы ее цели и задачи.

Каталог (directory) — это информационный ресурс, используемый для хранения информации о каком-либо объекте [1]. 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.

В данном документе термины "каталог" и "служба каталогов" относятся к каталогам, размещаемым в частных сетях и сетях общего пользования. Служба каталогов отличается от каталога тем, что она не только является информационным ресурсом, но также представляет собой услугу, обеспечивающую поиск и доставку пользователю необходимой ему информации [2].

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 [4].

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.

Active Directory - это не первая и не единственная служба каталогов. В современных сетях используется несколько служб каталогов и стандартов [3], [13]:

- 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.

Служба Active Directory, в отличие от перечисленных служб каталогов, является защищенной, распределенной, сегментированной и реплицируемой, что позволяет обеспечить следующие возможности [4]:

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

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

1.2 Назначение службы каталогов

Служба каталогов является как инструментом администрирования, так и инструментом пользователя (см. рис. 1.1). 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.

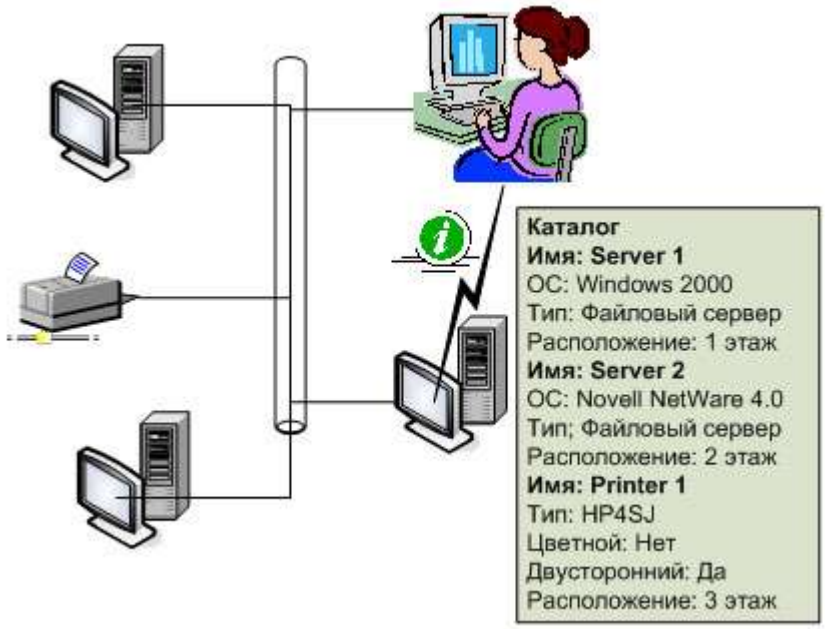


Рис. 1.1. Назначение Active Directory

Служба каталогов позволяет [1]:

- 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.

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.

1.3 Функции службы каталогов

Приведем основные функции службы каталогов и дадим их краткое описание [3].

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

единая точка входа для пользователей (или их компьютеров/приложений), которая нужна, когда возникает необходимость в поиске ресурсов.

- **Масштабируемость**. Служба каталогов должна допускать рост сети, не создавая при этом слишком больших издержек, - то есть она должна поддерживать какой-либо способ разбиения базы данных каталога на разделы, чтобы не утратить контроль над базой данных из-за ее чрезмерного разрастания и при этом сохранить преимущества централизации.
- **Стандартизация**. Служба каталогов должна предоставлять доступ к своей информации по открытым стандартам. Это гарантирует, что другие приложения смогут использовать ресурсы в службе каталогов (и публиковать их в ней), а не поддерживать собственные каталоги.
- **Расширяемость**. Служба каталогов должна тем или иным способом позволять администраторам и приложениям расширять в соответствии с потребностями организации набор информации, хранимой в каталоге.
- **Разделение физической сети**. Благодаря службе каталогов топология физической сети должна быть прозрачной для пользователей и администраторов. Ресурсы можно находить (и обращаться к ним), не зная, как и где они подключены к сети.
- **Безопасность**. 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.

В разрезе перечисленных функций можно указать и основные задачи, на выполнение которых нацелена служба 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.

Служба каталогов Active Directory также выполняет и другие функции [4]:

1.4 Преимущества Active Directory

Служба каталогов Active Directory является службой, интегрированной с MS Windows начиная с Windows 2000 Server. Active Directory обеспечивает иерархическую структуру построения организации, наращиваемость и расширяемость, а также функции

распределенной безопасности. Эта служба позволяет использовать простые и интуитивно понятные имена объектов, которые в ней содержатся, при этом доступ к ней может быть осуществлен с помощью таких инструментов, как программа просмотра ресурсов Интернет.

Распределенные службы безопасности также используют Active Directory в качестве хранилища учетной информации.

Преимущества интеграции управления учетными записями со службой каталогов Active Directory таковы:

- 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;
- 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;
- 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;
- 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;
- 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.

Если в компании-заказчике заинтересованы в выполнении наиболее сильно интегрированной службы каталога для Windows Server 2003, то Active Directory является логичным выбором. Другая очень популярная причина, подталкивающая к реализации службы Active Directory, состоит в поддержке Microsoft Exchange Server 2000 (Exchange Server 2000 полагается на Active Directory для своей службы каталога, поэтому многие администраторы реализуют Active Directory, чтобы модернизироваться до Exchange Server 2000.). Далее описаны несколько ключевых преимуществ службы Active Directory Windows Server 2003 [13].

- **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.
- **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.

1.5 Краткие итоги

В этой лекции были даны определения каталога и службы каталогов.

Перечислены службы и стандарты, используемые в современных сетях:

- X.500 и Directory Access Protocol (DAP).
- *Lightweight Directory Access Protocol (LDAP)*.
- Novell Directory Services (NDS).
- Windows NT и SAM.

Указано назначение служб каталога:

- 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.

Приведены основные функции службы каталогов, позволяющие обеспечивать следующие возможности:

- централизация;
- масштабируемость;
- стандартизация;
- расширяемость;
- разделение физической сети;
- безопасность.

Ключевые преимущества Active Directory:

- Централизованный каталог.
- Единая регистрация.
- Делегированное администрирование.
- Интерфейс общего управления.
- Интегрированная безопасность.
- Масштабируемость.

2 ЛЕКЦИЯ: ПРОЕКТИРОВАНИЕ ACTIVE DIRECTORY

Для понимания предметной области даны термины и их определения в контексте Active Directory. Определяется последовательность осуществляемых работ, необходимых для проектирования службы Active Directory: сбор информации, ее анализ, разработка структуры и архитектуры решения

Цель лекции: Ввести используемые в курсе понятия службы каталогов, дать представление об этапах проектирования службы Active Directory.

Планирование является важным подготовительным этапом при реализации проекта по созданию единой инфраструктуры Active Directory в компании. На этом этапе определяется последовательность осуществляемых работ, необходимых для проектирования предлагаемого решения: сбор информации, ее анализ, разработка структуры и архитектуры решения, а также вариантов развертывания системы при миграции данных.

2.1 Основные понятия службы каталогов

Прежде чем перейти к обзору процесса проектирования, включающего сбор и анализ данных о существующей структуре предприятия и подготавливающего реализацию Active Directory, необходимо ввести и определить ряд терминов, используемых в контексте службы каталогов Active Directory. Данная терминология приведена в соответствии с информационными материалами [1], [2], [3], [4].

2.1.1 Область действия

Область действия (scope) Active Directory достаточно обширна. Она может включать отдельные сетевые объекты (принтеры, файлы, имена пользователей), серверы и домены в отдельной глобальной сети. Она может также охватывать несколько объединенных сетей. Некоторые из рассматриваемых ниже терминов относятся к группе сетей, поэтому важно помнить, что Active Directory может быть настроена на управление как отдельным компьютером, так и компьютерной сетью или группой сетей.

2.1.2 Пространство имен

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. Например, телефонный справочник представляет собой *пространство имен*, в котором именам телефонных абонентов могут быть поставлены в соответствие телефонные номера. Файловая система Windows образует *пространство имен*, в котором имя файла может быть поставлено в соответствие конкретному файлу.

Active Directory образует *пространство имен*, в котором *имя объекта* в каталоге может быть поставлено в соответствие самому этому объекту.

2.1.3 Объект

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.

2.1.4 Контейнер

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*.

2.1.5 Дерево

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

2.1.6 Имя

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). 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.
- **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.

2.1.7 Контексты имен (сегменты, разделы)

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).

2.1.8 Домены

Домен - это единая область, в пределах которой обеспечивается безопасность данных в компьютерной сети под управлением ОС Windows (Более подробную информацию о доменах можно найти в документации по операционным системам Windows). 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. 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.

2.1.9 Доверительные отношения

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**. 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.
- **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.

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

2.1.10 Доменное дерево

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.

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 А доверяет домену В и домен В доверяет домену С, то домен А доверяет и домену С.
- **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.

2.1.11 Лес

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. 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.

2.1.12 Организационные единицы (подразделения)

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

2.1.13 Сайт (узел)

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. 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.

2.2 Сбор и анализ информации

На данном этапе предпроектного исследования собираются основные сведения по существующей инфраструктуре в компании.

- Для планирования структуры Active Directory - информация о доменной структуре и ее типе, структуре групп пользователей и распределении их по доменам, количестве существующих контроллеров доменов внутри каждого домена. Определение существующих доверительных отношений между доменами, односторонних и двухсторонних доверительных отношений и доменов, которые не должны включаться в леса Active Directory, пространства имен DNS, существующих в организации, и перечня существующих доменных имен организации, зарегистрированных в сети Интернет.
- Для планирования сайтов Active Directory - информация о существующей структуре сайтов, о топологии сети, о каналах связи и их пропускной способности.
- Для планирования переноса текущей структуры сетевых сервисов на платформу Active Directory - информация о топологии используемых сетевых сервисов DHCP, WINS, DNS.
- Для обеспечения возможности резервного восстановления данных во время миграции - схема резервного копирования информации.
- Для определения возможной расширяемости решения - исследование возможных вариантов изменения схемы при росте организации или ее реорганизации, определение области Active Directory (исследование подразделений, включая удаленные филиалы организации, необходимых для включения в Active Directory).
- Для планирования миграции приложений, использующих Active Directory - список приложений, связанных с Active Directory, и возможных ограничений, накладываемых ими на структуру Active Directory, определение механизмов идентификации пользователей.

2.3 План проектирования структуры Active Directory

Проектирование структуры Active Directory начинается с компонентов высшего уровня, а затем проектируются компоненты низших уровней. Это означает, что первый шаг состоит в создании проекта леса, затем следует проект доменов, проект DNS и, наконец, проект организационной единицы (OU) [13].

Проектирование структуры Active Directory должно включать следующие основные вехи.

1. Планирование структуры лесов:
    - Определение типовых лесов для основных типов региональных представительств.
    - Определение основных типов доверительных отношений между разными лесами.
    - Разработка политики контроля изменений леса.
    - Политика изменения схемы.
    - Политика изменения конфигурации.
    - Разработка структуры DNS для типовых лесов.
2. Планирование доменов для каждого леса:
    - Реструктуризация существующих доменов на домены в зависимости от административных потребностей.
    - Разбиение на домены в зависимости от физического месторасположения для оптимизации трафика репликации и запросов.
    - Выбор корневого домена для каждого леса.
    - Оптимизация аутентификации укороченными доверительными отношениями.
3. Планирование использования сайтов для каждого леса:
    - Определение сайтов на основании физической топологии сети.
    - Создание связей между сайтами.
    - План размещение серверов глобального каталога в сайтах.
    - План размещение серверов DNS в сайтах.
4. Планирование структуры организационных единиц для каждого домена:
    - Планирование реорганизации существующих доменов в организационных единицах.
    - Планирование организационных единиц для делегирования административных полномочий.
    - Планирование организационных единиц для скрытия объектов.
    - Создание организационных единиц для применения групповых политик.
5. Планирование реорганизации существующих доменов и их перевод на новую платформу Active Directory:
    - Планирование перемещения пользователей, компьютеров и групп.
    - Планирование модификации или удаления из структуры реструктуризируемых доменов.
    - Планирование изменения существующих доверительных отношений.
    - Планирование клонирования объектов безопасности.
6. Тестирование внедряемых решений и установка стенда:
    - Определение возможностей и целей тестирования.
    - Разработка сценариев тестирования: цель тестирования; тестируемые возможности и функции; требования к оборудованию, программному обеспечению и его конфигурации; описание проведения тестирования; ожидаемые результаты или критерии успеха теста; график тестирования.

При планировании новых учетных записей для предотвращения возможных проблем следует обратить внимание на решение следующих вопросов:

- правила именования, которые обеспечат уникальные, но понятные имена учетных записей;
- специалист, ответственный за определение паролей;
- временные периоды, в которые пользователю разрешено и запрещено входить в сеть;
- возможность блокировки учетной записи;
- тип профиля пользователя;
- хранение документов пользователя: в локальной папке или в домашней папке на сервере.

2.4 Краткие итоги

В этой лекции были приведены термины для понимания предметной области Active Directory, а также упомянуто об этапе предпроектного исследования, предназначенного для сбора и анализа информации.

Основные сведения по существующей инфраструктуре в компании:

- Информация о доменной структуре и ее типе, структуре групп пользователей и распределениИ их по доменам, о количестве существующих контроллеров доменов внутри каждого домена.
- Информация о существующей структуре сайтов, о топологии сети, о каналах связи и их пропускной способности.
- Информация о топологии используемых сетевых сервисов DHCP, WINS, DNS.
- Схема резервного копирования информации.
- Определение области Active Directory.
- Список приложений, связанных с Active Directory, и возможных ограничений, накладываемых ими на структуру Active Directory.

Помимо этого представлен типовой план проектирования структуры Active Directory, который без детализации выглядит следующим образом.

- Планирование структуры лесов.
- Планирование доменов для каждого леса.
- Планирование использования сайтов для каждого леса.
- Планирование структуры организационных единиц для каждого домена.
- Планирование реорганизации существующих доменов и их перевод на новую платформу Active Directory.
- Тестирование внедряемых решений и установка стенда.

3 ЛЕКЦИЯ: АРХИТЕКТУРА ACTIVE DIRECTORY

Приводятся модель данных и структура функционирования службы Active Directory в виде многоуровневой архитектуры. В архитектуре службы каталогов выделяются *логическая структура* и *физическая структура*, а также дается описание их компонентов

Цель лекции: Сформировать представление об архитектуре службы каталогов Active Directory, определить компоненты структур Active Directory.

3.1 Модель данных

Active Directory хранит информацию о сетевых ресурсах. Эти ресурсы (например, данные пользователей, описания принтеров, серверов, баз данных, групп, компьютеров и политик безопасности) называются *объектами*.

Объект - это отдельный именованный набор атрибутов, которыми представлен сетевой ресурс. Атрибуты объекта являются его характеристиками в каталоге (см. рис. 3.1).

Модель данных Active Directory строится на основе модели данных спецификации X.500 [2].

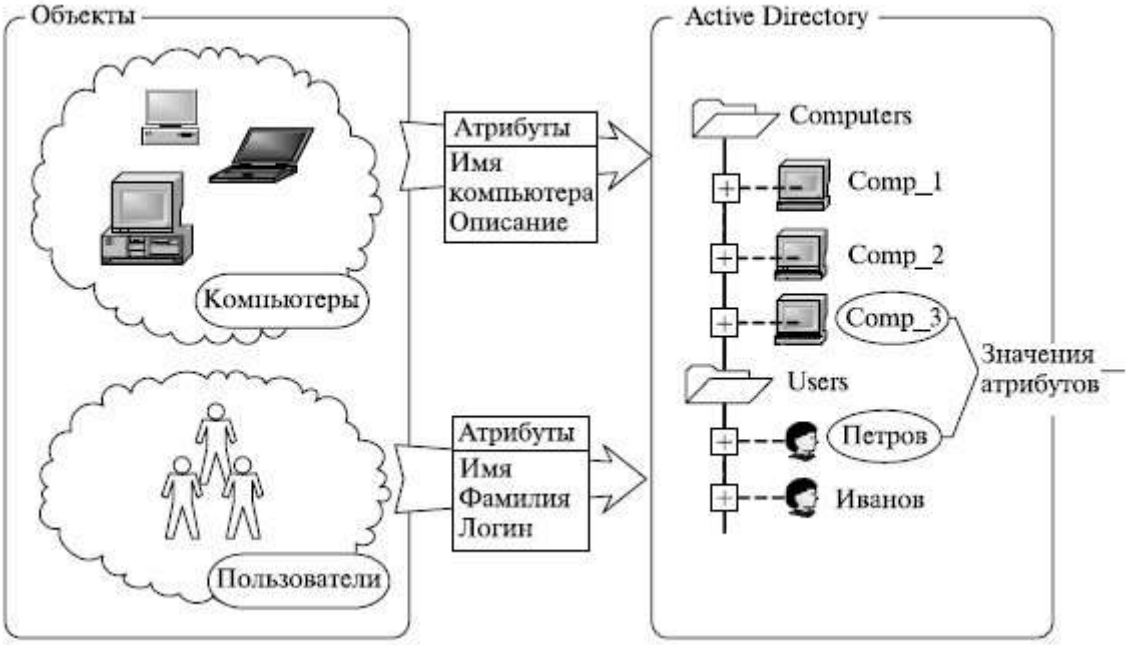


Рис. 3.1. Схема объектов Active Directory и их атрибуты

В каталоге хранятся объекты, которые представляют собой самые различные единицы хранения, описываемые с помощью атрибутов. Множество объектов, которые могут храниться в каталоге, задается в логической структуре (schema). Для каждого класса объектов *логическая структура* определяет, какие атрибуты обязательно должен иметь представитель данного класса, какие дополнительные атрибуты он может иметь и какой класс объектов может являться родительским по отношению к данному классу. Схема Active Directory содержит формальное описание содержания и структуры Active Directory, в том числе все атрибуты, классы и свойства классов.

3.2 Функциональная структура

Функциональную структуру Active Directory можно представить в виде многоуровневой архитектуры, в которой уровни являются процессами, предоставляющими клиентским приложениям доступ к службе каталога.

Active Directory состоит из трех уровней служб и нескольких интерфейсов и протоколов, совместно работающих для предоставления доступа к службе каталога. Три уровня служб охватывают различные типы информации, необходимой для поиска записей в базе данных (БД) каталога. Выше уровней служб в этой архитектуре находятся протоколы и API-интерфейсы, осуществляющие связь между клиентами и службой каталога.

На рис. 3.2 изображены уровни службы Active Directory и соответствующие им интерфейсы и протоколы. Здесь показано, как различные клиенты получают при помощи интерфейсов доступ к Active Directory.

Рис. 3.2. Многоуровневая архитектура Active Directory

Основные компоненты служб [4]:

- **Системный агент каталога (Directory System Agent, DSA)**. Выстраивает иерархию наследственных ("предок-потомок") отношений, хранящихся в каталоге. Предоставляет API-интерфейсы для вызовов доступа к каталогу. Клиенты получают доступ к Active Directory, используя механизмы, поддерживаемые DSA.
- **Уровень БД**. Предоставляет уровень абстрагирования между приложениями и БД. Вызовы из приложений никогда не выполняются напрямую к БД, а только через уровень БД.
- **Расширяемое ядро хранения**. Напрямую взаимодействует с конкретными записями в хранилище каталога на основе атрибута относительного составного имени объекта.
- **Хранилище данных (файл БД NTDS.dit)**. Управляется при помощи расширяемого механизма хранения БД, расположенного на *контроллере домена*.
- **LDAP/ADSI**. Клиенты, поддерживающие LDAP, используют его для связи с DSA. Active Directory поддерживает LDAP версии 2. Клиенты Windows с установленными клиентскими компонентами Active Directory для связи с DSA применяют LDAP версии 3. Хотя ADSI (Active Directory Service Interface) является средством абстрагирования API LDAP, Active Directory использует только LDAP.
- **API-интерфейс обмена сообщениями (Messaging API, MAPI)**. Традиционные клиенты MAPI, например Microsoft Outlook, подключаются к DSA, используя интерфейс поставщика адресной книги MAPI RPC.
- **Диспетчер учетных записей безопасности (Security Accounts Manager, SAM)**. Репликация с резервных контроллеров в домене смешанного режима также выполняется через интерфейс SAM.

- **Репликация (REPL)**. При репликации каталога агенты DSA взаимодействуют друг с другом, используя патентованный интерфейс RPC.

База данных Active Directory содержит следующие структурные объекты [13]:

- *Разделы (сегменты)*. Разделы Active Directory называются контекстами именования (NC - Naming Contexts) и содержат следующие сегменты: раздел домена каталога, раздел конфигурации каталога, раздел схемы каталога, раздел глобального каталога, разделы приложений каталога.
- **Домены**. *Домен* служит в качестве административной границы, он определяет и границу политик безопасности. Каждый домен имеет, по крайней мере, один *контроллер домена* (оптимально иметь два или более). Домены Active Directory организованы в иерархическом порядке. Первый домен на предприятии становится корневым доменом леса, обычно он называется корневым доменом или доменом леса.
- *Деревья доменов*. Домены, которые создаются в инфраструктуре Active Directory после создания корневого домена, могут использовать существующее пространство имен Active Directory совместно или иметь отдельное пространство имен. Чтобы выделить отдельное пространство имен для нового домена, нужно создать новое дерево домена.
- **Леса**. *Лес* определяет границу безопасности для предприятия, являясь общим для всех *контроллеров домена* в лесу. Все домены и доменные деревья существуют в пределах одного или несколько лесов Active Directory.
- **Сайты**. *Сайт* представляет область сети, где все *контроллеры домена* связаны быстрым, недорогим и надежным сетевым подключением. Независимость логических компонентов от сетевой инфраструктуры возникает вследствие использования сайтов в Active Directory: они обеспечивают соединение между логическими компонентами Active Directory и физической сетевой инфраструктурой.
- **Организационные единицы**. *Организационные единицы* предназначены для того, чтобы облегчить управление службой Active Directory. Они служат для создания иерархической структуры в пределах домена и используются, чтобы сделать более эффективным управление единственным доменом (вместо управления несколькими доменами Active Directory).

Компонентами логической структуры Active Directory являются домены, тогда как компонентами физической структуры являются сайты.

- Домен - объединение серверов и других сетевых ресурсов, собранных под одним именем.
- Сайт - комбинация одной или более IP-подсетей, которые должны быть соединены высокоскоростным каналом связи.

3.3 Логическая структура

В Active Directory ресурсы организованы в логическую структуру, отражающую структуру организации, что позволяет находить ресурс по его имени, а не по физическому расположению. Благодаря логическому

объединению ресурсов в Active Directory *физическая структура* сети не важна для пользователей.

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

На рис. 3.3 показаны взаимоотношения компонентов Active Directory.

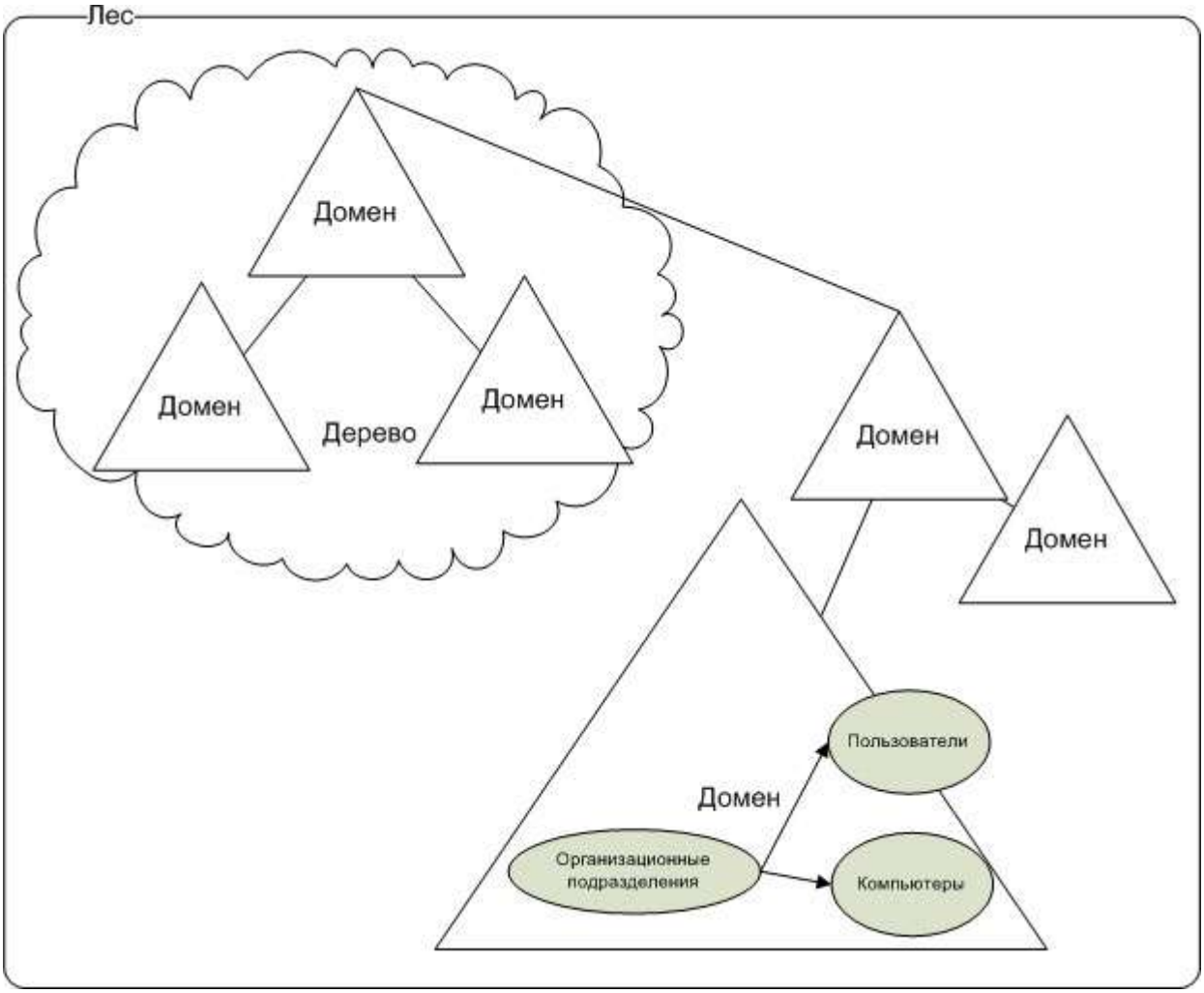


Рис. 3.3. Ресурсы, организованные в логическую структуру

Логические компоненты Active Directory [3]

- Объекты - ресурсы хранятся в виде объектов.
  - Классы объектов.
  - Схема Active Directory.
- Домены - базовая организационная структура.
- Деревья - несколько доменов объединяются в иерархическую структуру.
- Леса - группа из нескольких деревьев домена.
- Организационные единицы - позволяют делить домен на зоны и делегировать права на них.

Логическая структура Active Directory не базируется на физическом местонахождении серверов или сетевых соединениях в пределах домена. Это позволяет структурировать домены, отталкиваясь не от требований физической сети, а от административных и организационных требований.

При планировании логической структуры Active Directory необходимо определить иерархию доменов и организационных подразделений, а также разработать соглашения о пространстве имен (DNS/WINS), групповые политики и схемы делегирования полномочий.

Групповая политика службы Active Directory позволяет осуществлять детальное и гибкое централизованное управление группами пользователей, компьютеров, приложений и сетевых ресурсов, вместо того чтобы управлять этими объектами на индивидуальной основе. Служба Active Directory позволяет делегировать определенный набор административных полномочий с целью распределения задач управления и повышения качества администрирования. Делегирование полномочий также помогает компаниям сократить число доменов, необходимых для поддержки крупной организации с офисами в разных географических точках.

Примеры предоставления доступа к сетевым ресурсам

- **Пример "Единственный домен в центральном офисе"**. Предположим, что в компании имеется единственный домен в центральном офисе. Менеджерам компании для выполнения своих задач требуется доступ к инвентаризационной БД. Для предоставления доступа необходимо объединить всех менеджеров в глобальную группу, создать локальную доменную группу, обладающую полномочиями доступа к инвентарной базе, и добавить глобальную группу менеджеров в эту локальную доменную группу.
- **Пример "Среда с несколькими доменами в регионах"**. Предположим, что в компании используется среда с тремя доменами. Корневой домен находится в центральном офисе, а другие домены - в регионах. Менеджерам из всех трех доменов для выполнения задач требуется доступ к расположенной в центральном офисе инвентаризационной БД. Для предоставления доступа необходимо:
    - в каждом домене создать глобальную группу и добавить учетные записи менеджеров в этом домене в эту глобальную группу;
    - создать локальную доменную группу для доступа к инвентарной базе данных в домене центрального офиса;
    - добавить глобальную группу для доступа к базе данных инвентаря в домен центрального офиса;
    - добавить глобальные группы менеджеров из каждого домена в локальную доменную группу базы данных;
    - предоставить права доступа к инвентарной БД локальной доменной группе.

3.4 Физическая структура

Физическая структура сети с Active Directory довольно проста по сравнению с ее логической структурой. Физические компоненты Active Directory - это узлы (сайты) и *контроллеры домена*. Эти компоненты применяются для разработки структуры каталога, отражающей физическую структуру организации, которая, в свою очередь, влияет на создание сайтов для компании.

Физическое проявление службы Active Directory состоит в наличии отдельного файла данных, расположенного на каждом *контроллере домена*. Физическая реализация службы Active Directory описывается местоположением *контроллеров домена*, на которых расположена служба. При реализации службы Active Directory можно добавлять столько *контроллеров доменов*, сколько необходимо для поддержания служб каталога в данной организации. Имеется пять определенных ролей, которые может играть каждый из *контроллеров домена*. Они известны как **роли хозяина операций (operations master roles)**. Еще одна роль, которую может выполнять любой отдельный *контроллер* домена в домене, связана с глобальным каталогом (GC - Global Catalog). В этом разделе мы рассмотрим хранилище данных службы Active Directory и *контроллеры домена*, на которых оно расположено.

3.4.1 Контроллеры доменов и их роли

Контроллер домена - это компьютер-сервер, управляющий доменом и хранящий реплику каталога домена (локальную БД домена). Поскольку в домене может быть несколько *контроллеров домена*, все они хранят полную копию той части каталога, которая относится к их домену [6].

Ниже перечислены функции *контроллеров доменов* [4].

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

- Все контроллеры в домене автоматически реплицируют между собой все объекты в домене. Какие-либо изменения, вносимые в Active Directory, на самом деле производятся на одном из *контроллеров домена*. Затем этот *контроллер домена* реплицирует изменения на остальные контроллеры в пределах своего домена. Задавая частоту репликации и количество данных, которое Windows будет передавать при каждой репликации, можно регулировать сетевой трафик между *контроллерами домена*.
- Важные обновления, например отключение учетной записи пользователя, *контроллеры домена* реплицируют немедленно.
- Active Directory использует репликацию с несколькими хозяевами (multimaster replication), в котором ни один из *контроллеров домена* не является главным. Все контроллеры равноправны, и каждый из них содержит копию базы данных каталога, в которую разрешается вносить изменения. В короткие периоды времени информация в этих копиях может отличаться до тех пор, пока все контроллеры не синхронизируются друг с другом.
- Наличие в домене нескольких контроллеров обеспечивает отказоустойчивость. Если один из *контроллеров домена* недоступен, другой будет выполнять все необходимые операции, например записывать изменения в Active Directory.
- *Контроллеры домена* управляют взаимодействием пользователей и домена, например находят объекты Active Directory и распознают попытки входа в сеть.

Существует две роли хозяина операций, которые могут быть назначены единственному *контроллеру домена* в лесу (роли, действующие в границах леса) [3]:

- *Хозяин схемы* (Schema Master). Первый *контроллер домена* в лесу принимает роль хозяина схемы и отвечает за поддержку и распространение схемы на остальную часть леса. Он поддерживает список всех возможных классов объектов и атрибутов, определяющих объекты, которые находятся в Active Directory. Если схему нужно обновлять или изменять, наличие Schema Master обязательно.
- *Хозяин именования доменов* (Domain Naming Master). Протоколирует добавление и удаление доменов в лесу и жизненно необходим для поддержания целостности доменов. Domain Naming Master запрашивается при добавлении к лесу новых доменов. Если Domain Naming Master недоступен, то добавление новых доменов невозможно; однако при необходимости эта роль может быть передана другому контроллеру.

Существует три роли хозяина операций, которые могут быть назначены одному из контроллеров в каждом домене (общедоменные роли) [3].

- *Хозяин RID* (Relative Identifier (RID) Master). Отвечает за выделение диапазонов относительных идентификаторов (RID) всем контроллерам в домене. SID в Windows Server 2003 состоит из двух частей. Первая часть - общая для всех объектов в домене; для создания уникального SID к этой части добавляется уникальный RID. Вместе они уникально идентифицируют *объект* и указывают, где он был создан.
- *Эмулятор основного контроллера домена* (Primary Domain Controller (PDC) Emulator). Отвечает за эмуляцию Windows NT 4.0 PDC для клиентских машин, которые еще не переведены на Windows 2000, Windows Server 2003 или Windows XP и на которых не установлен клиент службы каталогов. Одна из основных задач эмулятора PDC - регистрировать устаревшие клиенты. Кроме того, к эмулятору PDC происходит обращение, если аутентификация клиента оказалась неудачной. Это дает возможность эмулятору PDC проверять недавно измененные

пароли для устаревших клиентов в домене, прежде чем отклонять запрос на вход.

- *Хозяин инфраструктуры* (Infrastructure Master). Регистрирует изменения, вносимые в контролируемые объекты в домене. Обо всех изменениях сначала сообщается Infrastructure Master, и лишь потом они реплицируются на другие контроллеры домена. Infrastructure Master обрабатывает информацию о группах и членстве в них для всех объектов в домене. Еще одна задача Infrastructure Master - передавать информацию об изменениях, внесенных в объекты, в другие домены.

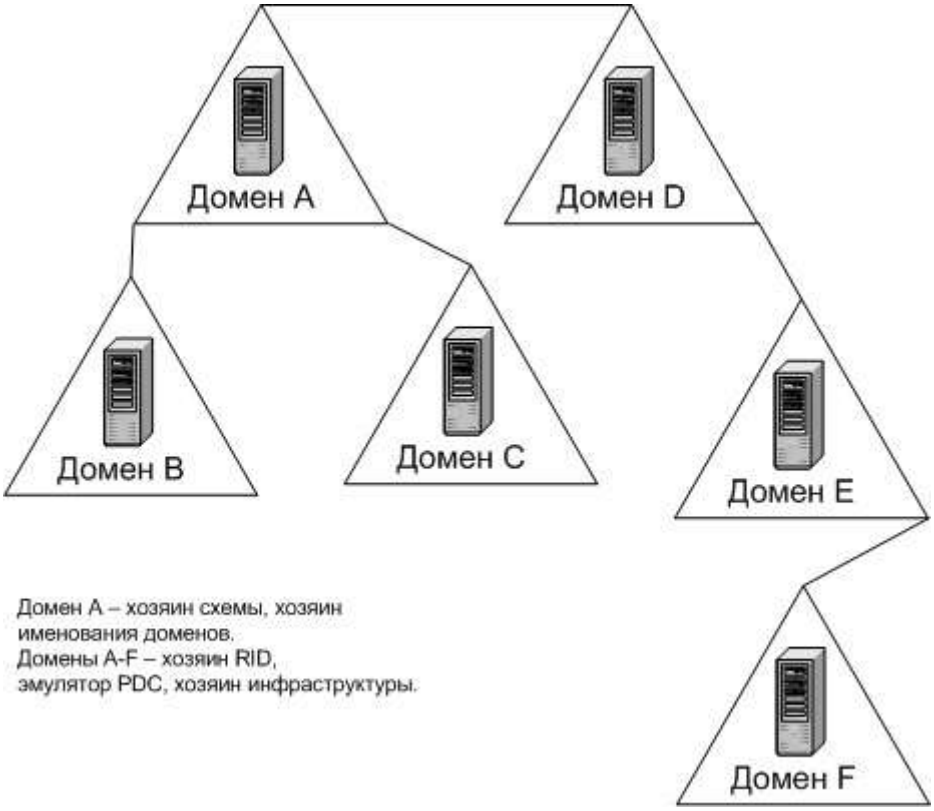


Рис. 3.4. Принятое по умолчанию распределение ролей хозяина операций в лесе

Роль "*Сервер глобального каталога*" (GC - Global Catalog) может выполнять любой отдельный *контроллер домена* в домене - одна из функций сервера, которую можно назначить *контроллеру домена* [13]. Серверы глобального каталога выполняют две важные задачи. Они дают возможность пользователям входить в сеть и находить объекты в любой части леса. Глобальный каталог содержит подмножество информации из каждого доменного раздела и реплицируется между серверами глобального каталога в домене. Когда пользователь пытается войти в сеть или обратиться к какому-то сетевому ресурсу из любой точки леса, соответствующий запрос разрешается с участием глобального каталога. Другая задача глобального каталога, полезная независимо от того, сколько доменов в вашей сети, - участие в

процессе аутентификации при входе пользователя в сеть. Когда пользователь входит в сеть, его имя сначала сверяется с содержимым глобального каталога. Это позволяет входить в сеть с компьютеров в доменах, отличных от того, где хранится нужная пользовательская учетная запись.

3.4.2 Концепция сайтов

Концепция сайтов используется продуктами семейства Microsoft BackOffice для минимизации трафика в глобальной сети и основывается на том, что ее основу составляет IP-сеть, для которой надо обеспечить наилучшие условия подключений вне зависимости от используемых приложений.

Сайт Windows Server 2003 - это группа *контроллеров доменов*, которые находятся в единой или нескольких IP-подсетях и связаны скоростными и надежными сетевыми соединениями. Сайты в основном используются для управления трафиком репликации. *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.

Сайты не являются частью пространства имен Active Directory. Когда пользователь просматривает логическое пространство имен, компьютеры и пользователи группируются в домены и OU без ссылок на сайты.

Сайты содержат объекты только двух типов [3]:

- *Контроллеры доменов* в границах сайта.
- Связи сайта (site links), сконфигурированные для соединения данного сайта с остальными. Связь состоит из двух частей: физического соединения между сайтами (обычно WAN-канала) и объекта связи сайта (site link object). Этот *объект* создается в Active Directory и определяет протокол передачи трафика репликации (IP или SMTP). Объект связи сайта также инициирует выполнение запланированной репликации.

Планирование сайтов и их размещение зависит от физической топологии сети, при этом необходимо учитывать потребность в линиях связи для осуществления межсайтовой репликации по создаваемому расписанию.

Сайт с Active Directory состоит из одной или нескольких подсетей IP, которые могут быть определены администратором и изменены им путем включения новых подсетей.

Деление на сайты не зависит от доменной (логической) структуры, то есть:

- в сайте может быть один домен (либо только его часть) или несколько доменов;
- в домене (или даже в организационном подразделении) может быть несколько сайтов.

Создание сайтов, структура которых отражает физическое расположение *контроллеров доменов* на площадках компании, может быть реализовано по одному из следующих вариантов:

- структура с одним сайтом (единый сайт, включающий все IP-подсети);
- структура с несколькими сайтами (отдельный сайт для каждой площадки).

Особенностями сайта являются:

- оптимизация трафика тиражирования между сайтами по медленным линиям;
- помощь клиентам быстрее обнаруживать ближайшие к ним контроллеры.

Понятие сайта неразрывно связано с топологией тиражирования. Тиражирование внутри сайта и между сайтами использует различные топологии:

- Внутри сайта - это двунаправленное кольцо. Тиражирование выполняется методом вызова удаленных процедур (Remote Procedure Calls, RPC). Внутри сайта *контроллер домена* задерживает оповещение о сделанных изменениях на некоторый устанавливаемый промежуток времени.
- Для тиражирования между сайтами применяется RPC или сообщения. Стандартно используется механизм SMTP, однако если в сети есть Microsoft Exchange, то он также может быть задействован для тиражирования Active Directory.

Служба каталогов отслеживает целостность топологии: ни один *контроллер домена* не может быть исключен из процесса тиражирования, что обеспечивается отдельным контрольным процессом (Knowledge Consistency

Checker, KCC), исполняемым на всех *контроллерах домена* - в случае нарушения топология тиражирования восстанавливается KCC.

Для поиска ближайших ресурсов или *контроллеров домена* клиенты могут использовать информацию о сайте. Концепция поиска ближайшего ресурса или *контроллера домена* позволяет сократить трафик в низкоскоростных частях глобальных сетей. В начале процесса входа в сеть клиент получает от *контроллера домена* имя сайта, к которому принадлежит, имя сайта, к которому относится *контроллер домена*, а также информацию о том, является ли данный *контроллер домена* ближайшим к клиенту. Если это не ближайший контроллер, то клиент может обратиться к *контроллеру домена* в его собственном сайте и в дальнейшем работать с ним как с ближайшим контроллером. Так как на клиенте данная информация сохраняется в реестре, она может быть использована во время следующего входа в сеть.

Для возможности управления сертификатами безопасности при многодоменной инфраструктуре (внедрение методов защиты информации), учитывающей интеграцию с другими платформами, а также для гарантированной идентификации пакетов при проведении межсайтовой репликации в структуре Active Directory планируется и создается архитектура открытых ключей (PKI).

Сервер сертификатов является важной частью архитектуры открытых ключей и позволяет издавать в компании собственные сертификаты для своих пользователей, реализуя такие возможности политик PKI, как проверка подлинности на основе сертификатов, IPSec, защищенная электронная почта и др.

3.5 Краткие итоги

В этой лекции была приведена *модель данных* и структура функционирования службы Active Directory в виде многоуровневой архитектуры:

- Системный агент каталога (Directory System Agent, DSA).
- Уровень БД.
- Расширяемое ядро хранения.
- Хранилище данных (файл БД NTDS.dit).
- LDAP/ADSI.
- API-интерфейс обмена сообщениями (Messaging API, MAPI).
- Диспетчер учетных записей безопасности (Security Accounts Manager, SAM).
- Репликация (REPL).

База данных Active Directory содержит следующие структурные объекты:

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

Логические компоненты Active Directory

- Объекты - ресурсы хранятся в виде объектов.
    - Классы объектов.
    - Схема Active Directory.
- Домены - базовая организационная структура.
- Деревья - несколько доменов объединяются в иерархическую структуру.
- Леса - группа из нескольких деревьев домена.
- Организационные единицы - позволяют делить домен на зоны и делегировать на них права.

Физическая структура сети с Active Directory довольно проста по сравнению с ее логической структурой, потому что физические компоненты Active Directory - это узлы (сайты) и *контроллеры домена*.

Необходимо четко представлять, что компонентами логической структуры Active Directory являются домены, тогда как компонентами физической структуры являются сайты.

Деление на сайты не зависит от доменной (логической) структуры, то есть:

- в сайте может быть один домен (либо только его часть) или несколько доменов;
- в домене (или даже в организационном подразделении) может быть несколько сайтов.

Сайты содержат объекты только двух типов:

- контроллеры доменов в границах сайта;
- связи сайта (site links), сконфигурированные для соединения данного сайта с остальными.

Роли хозяина операций, которые могут быть назначены контроллеру домена:

- Хозяин схемы (Schema Master);
- Хозяин именования доменов (Domain Naming Master);
- Хозяин RID (Relative Identifier (RID) Master);
- Эмулятор основного контроллера домена (Primary Domain Controller (PDC) Emulator);
- Хозяин инфраструктуры (Infrastructure Master);
- Сервер глобального каталога (GC - Global Catalog).

Особенностями сайта являются:

- оптимизация трафика тиражирования между сайтами по медленным линиям;
- помощь клиентам быстрее обнаруживать ближайшие к ним контроллеры.

Понятие сайта неразрывно связано с топологией тиражирования. Тиражирование внутри сайта и между сайтами использует различные топологии.

- Внутри сайта - это двунаправленное кольцо.
- Для тиражирования между сайтами используется RPC или сообщения.

Служба каталогов отслеживает целостность топологии: ни один контроллер домена не может быть исключен из процесса тиражирования, что обеспечивается отдельным контрольным процессом (Knowledge Consistency Checker, KCC), исполняемым на всех контроллерах домена - в случае нарушения топология тиражирования восстанавливается KCC.

4 ЛЕКЦИЯ: ПЛАНИРОВАНИЕ РАЗВЕРТЫВАНИЯ ACTIVE DIRECTORY

При подготовке вариантов развертывания Active Directory необходимо спланировать структуру доменов (корневой *домен* и дерево доменов), а также пространство имен DNS для возможности создания доменной иерархии. Приводится типовой план-график развертывания Active Directory, а также краткое описание его этапов

Цель лекции: Определить порядок развертывания службы каталога, дать представление о начальном этапе планирования Active Directory - проектировании структуры леса и доменной структуры.

Развертывание службы каталога Active Directory требует планирования и проектирования. Мы приведем краткий обзор процесса планирования, через который необходимо пройти, прежде чем начать развертывание Active Directory. Самый главный вопрос - сколько лесов требуется для сети организации. Затем обсуждается разбиение лесов на домены и планирование доменного пространства имен. При подготовке вариантов развертывания Active Directory необходимо спланировать структуру доменов (корневой *домен* и дерево доменов), а также пространство имен DNS для возможности создания доменной иерархии.

Кроме того, необходимо выработать подход по размещению объектов в организационных подразделениях, что подразумевает определение механизма разделения ресурсов компании по организационным подразделениям, а также анализ внешних условий, применяемых к их иерархии. После создания структуры организационных единиц для каждого домена необходимо сконфигурировать сайты.

Указанные действия позволяют учесть разветвленную структуру компании при развертывании единой инфраструктуры Active Directory.

4.1 План-график развертывания

Основные вехи в плане-графике развертывания Active Directory

- Формирование проектной группы.
- Инициация проекта, согласование плана работ, ролей и ответственности.
- Обследование существующей инфраструктуры:
    - Обследование существующей структуры Active Directory.
    - Обследование инфраструктуры (приложения, использующие Active Directory).
    - Формализация результатов обследования.
- Планирование структуры Active Directory:
    - Анализ требований заказчика к построению инфраструктуры Active Directory.
    - Планирование деревьев (леса) и доменов.
    - Планирование топологии сайтов.
    - Разработка архитектуры PKI.
    - Планирование политики резервного копирования.
    - Планирование системы мониторинга на период опытной эксплуатации.
    - Формализация и разработка технического задания.
- Развертывание тестовой среды, тестирование миграции:
    - Определение перечня приложений, подлежащих тестированию.
    - Определение аппаратной конфигурации тестового стенда.
    - Определение набора ресурсов Active Directory для миграции (для каждого приложения).
    - Развертывание репрезентативной копии боевой среды.
    - Верификация идентичности тестовой среды промышленной среде.
    - Развертывание спроектированной структуры Active Directory в тестовой среде.
    - Проведение тестовой миграции.
    - Деинсталляция копии боевой среды.
    - Верификация корректности проведенной миграции.
    - Формирование проектной документации (типовая процедура миграции).
- Развертывание структуры Active Directory корневого домена и центрального офиса.
    - Информирование пользователей.
    - Развертывание спроектированной структуры Active Directory.
    - Проведение миграции.
    - Наблюдение в период адаптации.
    - Доработка типовой процедуры миграции по результатам развертывания.
    - Обучение администраторов.
- Тиражирование решения на филиалы организации.
- Доработка и сдача документации.

4.2 Анализ существующей инфраструктуры

В первую очередь определяется географическая модель организации, то есть определяются следующие составляющие.

- Локальная модель.
- Региональная модель.
- Национальная модель.
- Международная модель.
- Филиалы.
- Дочерние компании.

На основании данной информации создается карта территориального размещения организации и проводится анализ топологии существующей сети. Для сбора сведений об информационных потоках в организации анализируется текущая модель администрирования и существующие процессы в организации.

4.3 Планирование структуры Active Directory

Первый шаг в планировании структуры Active Directory - определение лесов и доменов. Более подробная информация о вариантах построения лесов и вариантах определения доменной структуры приведена в следующей лекции.

4.4 Проектирование структуры леса

Самое главное решение, которое необходимо принять на раннем этапе разработки Active Directory, - сколько лесов потребуется. Развертывание единственного леса означает, что будет возможно простое совместное использование ресурсов и доступ к информации в пределах компании. Использование единственного леса для большой корпорации требует высокой степени доверия между разнообразными и, возможно, разъединенными деловыми подразделениями. В конечном счете количество развертываемых лесов зависит от того, что является наиболее важным для компании: легкость совместного использования информации в пределах всех доменов леса или поддержка полностью автономного и изолированного управления частями структуры каталога.

Для более успешного проектирования структуры лесов службы Active Directory необходимо привлечение бизнес-заказчиков, которые являются основными потребителями услуг, обеспечиваемых ИТ-инфраструктурой. Эти задачи касаются вопросов доступности информации, безопасности, простоты управления и практичности. Менеджеры обычно включаются в принятие решений, которые не могут быть изменены сразу после развертывания. Среди

этих решений - вопрос о том, сколько лесов и доменов требуется сети и сколько должно быть развернуто доменных пространств имен.

Лес Active Directory предназначен для того, чтобы быть отдельным самодостаточным модулем. Внутри леса должна быть реализована возможность совместно использовать информацию и сотрудничать с другими пользователями из того же самого подразделения. Проектируя самый высокий уровень инфраструктуры Active Directory, необходимо решить, нужно ли развертывать один *лес* или несколько. Каждый *лес* является интегрированным модулем, потому что он включает следующие составляющие [13]:

- **Глобальный каталог**. *Лес* имеет один глобальный каталог (GC). Каталог GC облегчает поиск объектов в любом домене леса и вход на любой домен леса независимо от того, на каком домене зарегистрирована учетная запись пользователя.
- **Раздел конфигурации каталога**. Все контроллеры домена совместно используют один и тот же раздел конфигурации каталога. Эта информация нужна для оптимизации репликации информации в пределах леса, для хранения приложений и информации Active Directory, поддерживающей приложения, и для совместного использования информации с помощью раздела приложений каталога.
- *Доверительные отношения*. Все домены в лесу связаны двусторонними транзитивными доверительными отношениями. Не существует никакой опции, позволяющей изменить это.

В то время как служба Active Directory облегчает совместное использование информации, она предписывает множество ограничений, которые требуют, чтобы различные подразделения в компании сотрудничали различными способами [13].

- **Одна схема**. Все домены в лесу используют одну схему. Это обстоятельство как будто упрощает дело, но оно может быть одной из причин развертывания нескольких лесов в компании. Если одно подразделение решает развертывать приложение, которое изменяет схему, то это оказывает воздействие на все подразделения. Каждая модификация схемы должна быть проверена для гарантии того, что она не находится в противоречии с другими изменениями схемы. Это потребует значительного времени и усилий.
- **Централизованное управление**. Развертывание единственного леса означает, что некоторые компоненты сетевого управления должны быть централизованы. Например, единственная группа, обладающая правом изменять схему, - это группа Schema Admins (администраторы схемы). Единственная группа, обладающая правом добавлять и удалять домены из леса, - это группа Enterprise Admins (администраторы предприятия). Группа Enterprise Admins автоматически добавляется к домену локальной группы Administrators (администраторы) на каждом контроллере домена в лесу.

- **Политика управления изменениями**. Поскольку изменения леса могут затрагивать каждый *домен* и должны выполняться только централизованно, требуется четкая политика управления изменениями.
- **Доверенные администраторы**. Развертывание одного леса требует определенной степени доверия администраторам всех доменов. Любой администратор, обладающий правами управления контроллером домена, может сделать такие изменения, которые затронут весь *лес*. Это означает, что все администраторы доменов должны быть высокодоверенными людьми.

Обдумывая вопрос, касающийся количества развертываемых лесов, необходимо оценить каждый из этих факторов для определения потребностей организации, в которой планируется внедрение Active Directory.

4.5 Проектирование доменной структуры

Как только вопрос о количестве развертываемых лесов улажен, необходимо определить доменную структуру в пределах каждого из лесов. Первая задача состоит в том, чтобы задокументировать конфигурацию текущих служб каталога и определить, какая часть текущей инфраструктуры может быть модернизирована, а какая должна быть реструктурирована или заменена. Затем определяется необходимое количество доменов и их иерархия.

Домены используются для разделения большого леса на более мелкие компоненты для целей репликации или администрирования. Следующие характеристики домена крайне важны при проектировании Active Directory [13]:

- Граница репликации. Границы домена являются границами репликации для раздела домена каталога и для информации домена, хранящейся в папке Sysvol на всех контроллерах домена. В то время как другие разделы каталога (раздел схемы, конфигурации и GC) реплицируются по всему лесу, раздел каталога домена реплицируется только в пределах одного домена.
- Граница доступа к ресурсам. Границы домена являются также границами для доступа к ресурсам. По умолчанию пользователи одного домена не могут обращаться к ресурсам, расположенным в другом домене, если только им не будут явно даны соответствующие разрешения.
- Граница политики безопасности. Некоторые политики безопасности могут быть установлены только на уровне домена. Эти политики, такие как политика паролей, политика блокировки учетных записей и политика билетов Kerberos, применяются ко всем учетным записям домена.

В то время как в большинстве компаний внедряется модель Active Directory с единым лесом, некоторые крупные компании развертывают

несколько доменов в пределах этого леса. Проще всего управлять единственным доменом, он обеспечивает пользователей наименее сложной средой. Однако имеется ряд причин для развертывания нескольких доменов [3].

- **Применение одного домена**
  - Упрощение управления пользователями и группами.
  - Нет необходимости планировать *доверительные отношения*.
  - Для делегирования прав применяются OU.
- Применение нескольких доменов
  - Возможность реализации разных политик безопасности.
  - Децентрализованное управление.
  - Оптимизация трафика.
  - Разные пространства имен.
  - Необходимо сохранить существующую архитектуру доменов Windows NT.
  - Размещение хозяина схемы в отдельный *домен*.

4.5.1 Применение одного домена

Простейшая модель Active Directory - единственный *домен*. Подавляющее большинство сетей во всем мире позволяет использовать единственный *домен*, поэтому такая модель, хотя и может показаться не столь гибкой, как другие, обычно заслуживает самого тщательного рассмотрения. В сущности, при планировании структуры Active Directory полезно исходить из предположения, что будет использоваться один *домен*, и пытаться остаться в рамках этой модели.

В модели с единственным доменом все объекты находятся в одной зоне безопасности, поэтому не приходится заниматься планированием доверительных отношений с другими доменами или реализовать кросс-доменные аутентификацию и разрешения. Кроме того, при использовании одного домена гораздо проще обеспечить централизованное управление сетью.

Модель с единственным доменом упрощает управление пользователями и группами, а также реализацию групповых политик. По сути, становится легче выполнять почти все операции по управлению сетью, а значит,

требуется меньше усилий на планирование, администрирование и устранение неполадок, что в итоге приведет к сокращению общих затрат.

4.5.2 Использование нескольких доменов

Хотя однодоменная модель дает существенное преимущество - простоту, иногда приходится использовать несколько доменов, потому что существует много серьезных оснований для такого решения [13].

- Трафик репликации должен быть ограничен. Раздел каталога домена, который является самым большим и наиболее часто изменяемым разделом каталога, копируется на все контроллеры домена в домене. В некоторых случаях это может вызывать слишком большой трафик репликации между офисами компании (даже если сконфигурировано несколько сайтов).
- Между офисами компании существуют медленные сетевые подключения или в офисах имеется много пользователей. Единственный способ ограничить в этом случае трафик репликации состоит в том, чтобы создать дополнительные домены.
- Любые офисы компании, связь между которыми обеспечивается только простым протоколом передачи почты (SMTP), должны конфигурироваться как отдельные домены. Информация домена не может реплицироваться через связи сайта, использующие протокол SMTP.
- Единственный способ иметь различную политику паролей, политику блокировки учетных записей и политику билетов Kerberos состоит в развертывании отдельных доменов.
- Необходимость ограничивать доступ к ресурсам и иметь административные разрешения.
- В некоторых случаях дополнительные домены создаются потому, что лучший путь перехода для организации состоит в модернизации нескольких уже имеющихся доменов.

Лучше планировать домены так, чтобы все они входили в одно дерево доменов. Так как все домены в одном дереве делят одно пространство имен, административные издержки будут значительно ниже, чем при использовании нескольких деревьев. При создании нескольких доменов определять их границы лучше в соответствии с теми разграничениями внутри компании, вероятность изменения которых меньше всего. Например, создание доменов по территориальному принципу, как правило, надежнее, чем создание доменов в соответствии с иерархией подразделений компании, поскольку изменение организационной структуры более вероятно, чем изменение территориальной.

При использовании модели Active Directory с несколькими доменами выполняются следующие правила [3]:

- в каждом домене требуется хотя бы один контроллер;
- групповая политика и управление доступом действует на уровне домена;
- при создании дочернего домена между родительским и дочерним доменами автоматически устанавливаются двусторонние транзитивные *доверительные отношения*;
- административные права, действующие между доменами, выдаются только для администраторов предприятия;
- необходимо создавать доверяемые каналы.

4.5.3 Проектирование корневого домена леса

Другое важное решение, которое целесообразно принять при планировании развертывания службы Active Directory: необходимость развернуть назначенный корневой домендомен (называемый также пустым корнем). Назначенный корневой *домен* (dedicated root domain) - это *домен*, который выполняет функции корневого домена леса. В этом домене нет никаких учетных записей пользователей или ресурсов, за исключением тех, которые нужны для управления лесом.

Для большинства компаний, развертывающих несколько доменов, настоятельно рекомендуется иметь назначенный корневой *домен* [13]. Корневой *домен* - это критический *домен* в структуре Active Directory, содержащий административные группы уровня леса (группы Enterprise Admins и Schema Admins) и хозяев операций уровня леса (хозяина именования доменов и хозяина схемы). Кроме того, корневой *домен* должен быть всегда доступен, когда пользователи входят на другие домены, не являющиеся их домашними доменами, или когда пользователи обращаются к ресурсам, расположенным в других доменах. Корневой *домен* нельзя заменять, если он разрушен, его нельзя восстановить - необходимо заново построить весь *лес*.

Дополнительные задачи при проектировании домена [3]:

- планирование DNS;
- планирование WINS;

- планирование инфраструктуры сети и маршрутизации;
- планирование подключения к Интернету;
- планирование стратегии удаленного доступа.

4.6 Краткие итоги

В данной лекции приведен план-график развертывания Active Directory, который без детализации выглядит следующим образом:

- Формирование проектной группы.
- Инициация проекта, согласование плана работ, ролей и ответственности.
- Обследование существующей инфраструктуры.
- Планирование структуры Active Directory.
- Развертывание тестовой среды, тестирование миграции.
- Развертывание структуры Active Directory корневого домена в центральном офисе.
- Тиражирование решения на филиалы организации.
- Доработка и сдача документации.

При анализе существующей инфраструктуры определяется в первую очередь географическая модель организации, на основании чего создается карта территориального размещения организации и проводится анализ топологии существующей сети.

Первый шаг в планировании структуры Active Directory - определение лесов и доменов.

Самое главное решение, которое необходимо принять на раннем этапе разработки Active Directory, - сколько лесов потребуется. Развертывание единственного леса означает, что будет возможно простое совместное использование ресурсов и доступ к информации в пределах компании.

Каждый *лес* является интегрированным модулем, потому что он включает следующие составляющие:

- Глобальный каталог.
- Раздел конфигурации каталога.
- Доверительные отношения.

В то время как служба Active Directory облегчает совместное использование информации, она предписывает множество ограничений, которые требуют, чтобы различные подразделения в компании сотрудничали различными способами:

- Одна схема.
- Централизованное управление.
- Политика управления изменениями.
- Доверенные администраторы.

Как только вопрос о количестве развертываемых лесов улажен, необходимо определить доменную структуру в пределах каждого из лесов.

Домены используются для разделения большого леса на более мелкие компоненты для целей репликации или администрирования. Следующие характеристики домена крайне важны при проектировании Active Directory:

- граница репликации;
- граница доступа к ресурсам;
- граница политики безопасности.

В то время как в большинстве компаний внедряется модель Active Directory с единым лесом, некоторые крупные компании развертывают несколько доменов в пределах этого леса. Проще всего управлять единственным доменом, он обеспечивает пользователей наименее сложной средой. Однако имеется ряд причин для развертывания нескольких доменов.

- Применение одного домена:
  - упрощение управления пользователями и группами;
  - нет необходимости планировать *доверительные отношения*;
  - для делегирования прав применяются OU.
- Применение нескольких доменов:
  - возможность реализации разных политик безопасности;
  - децентрализованное управление;
  - оптимизация трафика;
  - разные пространства имен;
  - необходимо сохранить существующую архитектуру доменов Windows NT;
  - размещение хозяина схемы в отдельный *домен*.

Более подробная информация о вариантах построения лесов и вариантах определения доменной структуры приведена в следующей лекции.

5 ЛЕКЦИЯ: МОДЕЛИ ПОСТРОЕНИЯ ЛЕСОВ И ДЕТАЛИЗАЦИЯ ДОМЕННОЙ СТРУКТУРЫ

Приведены варианты построения единого леса службы Active Directory, указана возможность применения нескольких лесов и недостатки такой модели. Приведены варианты детализации доменной структуры Active Directory и кратко описан процесс назначения владельцев доменов

Цель лекции: Дать представление о возможных моделях построения лесов и соответствующей им детализации доменной структуры.

Лес - это группа из одного или нескольких деревьев доменов, которые не образуют единое пространство имен, но используют общие схему, конфигурацию каталогов, глобальный каталог и автоматически устанавливают двусторонние транзитивные доверительные отношения между доменами.

В сети всегда есть минимум один *лес*, создаваемый, когда в сети устанавливается первый *контроллер домена*. Первый *домен* становится корневым доменом *леса*.

5.1 Варианты построения леса

В данном разделе мы дадим описание различных моделей построения лесов Active Directory и проведем их сравнительный анализ.

- Вариант 1 "Единый лес, каждый регион - отдельное дерево".
- Вариант 2 "Единый лес, административный корневой домен, каждый регион - домен".
- Вариант 3 "Единый лес, каждый регион - дочерний домен центрального домена".

Под регионами в контексте данной лекции подразумеваются удаленные офисы компании, в которой планируется развернуть службу Active Directory.

5.1.1 Единый лес, каждый регион - отдельное дерево

Существует отдельное дерево с корневым доменом, хранящим группы Enterprise Admins и Schema Admins, что позволит гибко контролировать членство в этих группах и исключить присутствие в них по умолчанию всех

администраторов центрального офиса (группа Admins корневого домена входит в группы Enterprise Admins, Schema Admins).

Разные деревья могут иметь различные пространства имен DNS. Корневые домены деревьев связаны транзитивными доверительными отношениями.

Плюсы модели:

- пользователи могут просматривать ресурсы центрального офиса и регионов при соответствующих правах доступа к объектам Active Directory;
- возможность регистрации мобильных пользователей в любой точке организации;
- единый обмен в организации;
- повышенная защищенность - аутентификация по протоколу Kerberos, группы Enterprise Admins, Schema Admins находятся в отдельном корневом домене, Schema master находится в отдельном домене;
- самый короткий путь доверия.

Минусы модели:

- видимость списка доменов всей организации;
- для наличия права создания новых деревьев/доменов администратор должен присутствовать в группе Enterprise Admins;
- тиражирование конфигурации и схемы Active Directory для всех регионов;
- если в организации уже развернута структура Active Directory, то контроллеры домена в этой организации необходимо переустановить.

5.1.2 Единый лес, административный корневой домен, каждый регион - домен

Существуют общее дерево Active Directory для регионов и общая система именования, основанная на географическом принципе. Каждое региональное подразделение представлено доменом. Региональные домены добавляются как дочерние к корневому домену. Административные группы Enterprise Admins, Schema Admins, дающие их членам административные полномочия в лесу, вынесены в отдельный корневой домен.

Существует единое пространство доменных имен, дочерние домены наследуют DNS имя родительского домена. Также существует единая поисковая служба, позволяющая находить объекты в любом домене службы Active Directory.

Плюсы модели:

- пользователи могут просматривать ресурсы центрального офиса и регионов при соответствующих правах доступа к объектам Active Directory;
- возможность регистрации мобильных пользователей в любой точке организации;
- единый обмен в организации;
- повышенная защищенность - аутентификация по протоколу Kerberos, группы Enterprise Admins, Schema Admins находятся в отдельном корневом домене, Schema master находится в отдельном домене.

Минусы модели:

- видимость списка доменов всей организации;
- для наличия права создания новых деревьев/доменов администратор должен присутствовать в группе Enterprise Admins;
- тиражирование конфигурации и схемы Active Directory для всех регионов;
- путь доверия длиннее.

5.1.3 Единый лес, каждый регион - дочерний домен центрального домена

В корневом домене наряду с группами Enterprise Admins и Schema Admins существуют остальные пользовательские учетные записи центрального офиса. Любой пользователь, попадающий в группу Admins, становится Enterprise Admins, так как группа Admins входит в группы Enterprise Admins и Schema Admins. Региональные домены становятся дочерними для корневого домена.

Существует единое пространство доменных имен, дочерние домены наследуют DNS имя родительского домена. Имеется единая поисковая служба, позволяющая находить объекты в любом домене службы Active Directory.

Плюсы модели:

- пользователи могут просматривать ресурсы центрального офиса и регионов при соответствующих правах доступа к объектам Active Directory;
- возможность регистрации мобильных пользователей в любой точке организации;
- единый обмен в организации; повышенная защищенность - аутентификация по протоколу Kerberos;
- сокращение количества компьютеров - контроллеров домена из-за отсутствия корневого "пустого" домена.

Минусы модели:

- видимость списка доменов всей организации;

- для наличия права создания новых деревьев/доменов, администратор должен присутствовать в группе Enterprise Admins;
- тиражирование конфигурации и схемы Active Directory для всех регионов;
- необходимы дополнительные усилия по контролю членства в группах Enterprise Admins, Schema Admins (не допускать в них группу Admins);
- структурное подчинение регионов;
- путь доверия длиннее.

5.2 Применение нескольких лесов

Леса представляют собой крайние границы зон безопасности. Между лесами невозможно административное управление или пользовательский доступ, если на то нет явного разрешения в конфигурации. Для этого предназначен тип доверия, введенный в Windows Server 2003, - доверие к лесу (forest trust), применяемый при управлении отношениями между двумя лесами.

Доверие к лесу не является транзитивным на уровне лесов. Другими словами, если первый лес доверяет второму, а второй - третьему, то это еще не означает, что первый автоматически доверяет третьему. Также необходимо учитывать, что для использования доверия к лесу нужно, чтобы оба леса находились на функциональном уровне Windows 2003 - все контроллеры доменов в обоих лесах должны работать под управлением Windows Server 2003.

Есть несколько случаев, описанных далее, в которых может потребоваться реализация нескольких лесов, однако в принципе следует по возможности избегать использования модели из нескольких лесов по причинам, указанным ниже.

5.2.1 Случаи реализации нескольких лесов

Реализация модели построения нескольких лесов допускается в следующих случаях [3]:

- **Объединение двух существующих организаций**. Независимо от того, слияние это или поглощение, можно столкнуться с тем, что появятся два полностью раздельных леса, которые нужно связать друг с другом для совместного использования ресурсов. Эта связь может быть временной, если в

дальнейшем один лес планируется сделать частью другого, или постоянной, если обе компании должны остаться относительно автономными.

- **Создание автономного подразделения**. Поскольку леса являются крайними зонами безопасности, отдельный лес можно использовать для того, чтобы создать сеть, в которой администрирование в значительной мере независимо от основного леса. В таком случае для отдельного леса схема может поддерживаться и изменяться, не оказывая влияния на другие леса.
- **Создание изолированного подразделения**. В изолированном лесу гарантируется, что администратор вне леса не сможет повлиять на управление им.

5.2.2 Недостатки структуры из нескольких лесов

Прежде чем приступить к планированию структуры нескольких лесов, необходимо принять к сведению, что большая часть функциональности, доступной в пределах одного леса, недоступна между лесами. Кроме того, поддержка нескольких лесов требует значительно больше усилий в администрировании, чем поддержка одного леса.

Архитектура с несколькими лесами имеет следующие недостатки [3].

- При поиске ресурсов от пользователей требуется более высокий уровень подготовки. С точки зрения пользователя, поиск ресурсов в рамках одного леса сравнительно прост благодаря единому глобальному каталогу. При наличии нескольких лесов существует несколько глобальных каталогов, и пользователям приходится указывать, в каком лесу вести поиск ресурсов.
- Сотрудники, которым требуется входить на компьютеры, включенные во внешние леса, должны указывать при входе основное имя пользователя (User Principal Name, UPN) по умолчанию. От таких сотрудников также требуется более высокий уровень подготовки.
- Администраторам приходится хранить несколько схем.
- Для каждого леса используются отдельные контейнеры конфигурации. Изменения в топологии необходимо реплицировать в другие леса.
- Любую репликацию информации между лесами приходится настраивать вручную. Администраторы должны конфигурировать разрешение DNS-имен между лесами, чтобы обеспечить функционирование контроллеров доменов и поддержку поиска ресурсов.
- Администраторам приходится настраивать списки управления доступом (ACL) к ресурсам, чтобы соответствующие группы из разных лесов могли обращаться к этим ресурсам, а также создавать новые группы, чтобы можно было использовать роли одних лесов в других лесах.
- Часто для наблюдения за отдельными лесами и управления ими нужен дополнительный персонал, а значит расходуются средства на подготовку большего штата сотрудников и на оплату их труда.

5.3 Детализация доменной структуры

Для детализации доменной структуры компании необходимо предварительно выбрать оптимальную структуру леса. Варианты построения

лесов были приведены в предыдущем разделе. Теперь необходимо определиться с вариантами детализации доменной структуры, которые будут описаны более подробно в следующих подразделах:

- Вариант 1 "Повторение существующей доменной структуры".
- Вариант 2 "Несколько лесов, минимальное количество доменов".
- Вариант 3 "Единый лес".

5.3.1 Повторение существующей доменной структуры

Домен для миграции существует в отдельном лесу. Необходимо создание двух учетных записей для каждого пользователя центрального офиса и регионального пользователя: одну в создаваемом домене, другую - в существующем. Все ресурсы DMZ (а также front-end почтовые сервера) располагаются в дочернем домене (DMZ Internal VLAN). При этом доступ учетных записей пользователей из существующего домена к ресурсам нового домена автоматически запрещен на уровне доверительных отношений между доменами. Учетным записям пользователей в мигрируемом домене дано право доступа к почтовому ящику соответствующего пользователя в создаваемом домене. Почтовые ящики пользователей находятся на сервере нового домена (LAN центрального офиса). Для упрощения создания двойной учетной записи можно использовать продукт "Microsoft Metadirectory Service" (MMS).

Необходимо отметить, что при создании DMZ в регионах по схеме, аналогичной центральному офису, неизбежно внедрение еще одного леса Active Directory для каждого региона и синхронизация этого леса с остальными лесами.

Плюсы данного варианта:

- структура Active Directory приближена к существующей доменной структуре, не потребует дополнительной конфигурации сетевого оборудования;
- пользователи, находясь внутри корпоративной сети, смогут получить доступ к ресурсам всей сети (регионы и центральный офис) согласно правам доступа.

Минусы:

- ведение двойной базы данных учетных записей пользователей;
- использование продукта MMS для синхронизации каталогов.

5.3.2 Несколько лесов, минимальное количество доменов

Данная схема предлагает консолидировать создаваемый домен и его дочерний домен в единый домен. Домен для миграции существует в отдельном лесу.

Необходимо создание двух учетных записей для каждого пользователя центрального офиса и регионального пользователя: одну в новом домене, другую - в существующем домене. Все ресурсы DMZ (а также front-end почтовые серверы) располагаются в создаваемом домене (DMZ Internal VLAN). Контроллеры нового домена находятся в зонах LAN и DMZ. При этом доступ учетных записей пользователей из существующего домена к ресурсам создаваемого домена, находящимся в зоне LAN, должен быть запрещен выставлением прав доступа к объектам нового домена и/или правилами на брандмауэре. Учетным записям пользователей в мигрируемом домене дано право доступа к почтовому ящику соответствующего пользователя в создаваемом домене. Почтовые ящики пользователей находятся на сервере нового домена (LAN центрального офиса). Для упрощения создания двойной учетной записи можно использовать продукт "Microsoft Metadirectory Service" (MMS), позволяющий синхронизовать объекты различных каталогов.

Необходимо отметить, что при создании DMZ в регионах по схеме, аналогичной центральному офису, неизбежно внедрение еще одного леса Active Directory для каждого региона и синхронизация этого леса с остальными лесами.

Плюсы данного варианта:

- структура Active Directory приближена к существующей доменной структуре, не потребует дополнительной конфигурации сетевого оборудования;
- пользователи, находясь внутри корпоративной сети, смогут получить доступ к ресурсам всей сети (регионы и центральный офис) согласно правам доступа;

- по сравнению с вариантом № 1 уменьшено количество доменов, в том числе сокращено количество используемых компьютеров и административная нагрузка.

Минусы:

- ведение двойной базы данных учетных записей пользователей;
- использование продукта MMS для синхронизации каталогов.

5.3.3 Единый лес

Негативным моментом предыдущих вариантов является существование двух лесов Active Directory, что заставляет внедрять дополнительную систему синхронизации двух лесов или вести дублирующие записи в двух лесах (фактически ручная синхронизация). Возникает желание уйти от существования двух лесов.

В данном варианте построения Active Directory все домены находятся в общем лесу. Бывший домен, подготовленный для миграции, отсутствует: он может быть дочерним по отношению к создаваемому домену или корневому домену.

Данный вариант построения Active Directory позволяет избежать ведения двух учетных записей для каждого пользователя. Все ресурсы DMZ (а также front-end почтовые серверы) располагаются в дочернем домене (DMZ Internal VLAN). Почтовые ящики пользователей находятся на сервере нового домена (LAN центрального офиса). Учетные записи пользователей центрального офиса заведены в создаваемом домене. Учетные записи мобильных пользователей, требующих доступ к ресурсам зоны DMZ Internal, заведены в дочернем домене. Для таких пользователей доступ к ресурсам будет ограничен с применением прав доступа пользователей и групповой политики дочернего домена. В частности, используя группу Domain Users дочернего домена, возможно настроить автоматический первоначальный запрет доступа к ресурсам Active Directory для новых пользователей для повышения безопасности системы.

Плюсы данного варианта:

- уникальность учетных записей в пределах Active Directory для любого пользователя;
- пользователи, находясь как внутри корпоративной сети, так и в Интернете, смогут получить доступ к ресурсам всей сети (регионы и центральный офис) согласно правам доступа.

Минус данного варианта: модернизация сетевой инфраструктуры компании, в которой планируется развернуть службу Active Directory.

5.4 Назначение владельцев доменов

Для каждого из доменов, включенных в проект Active Directory, необходимо назначить владельца домена. В большинстве случаев владельцы домена являются администраторами подразделений, в которых был определен домен.

Роль владельца домена состоит в управлении индивидуальным доменом [13].

- **Создание политик безопасности уровня домена**. Это включает политику паролей, политику блокировки учетных записей и политику аутентификации по протоколу Kerberos.
- **Проектирование конфигурации групповой политики (Group Policy) уровня домена**. Владелец домена может проектировать групповую политику для всего домена и делегировать право связывать групповую политику с администратором уровня OU.
- **Создание в домене OU-структуры высокого уровня**. После этого задача создания подчиненных OU может быть передана администраторам уровня OU.
- **Делегирование административных прав в пределах домена**. Владелец домена должен установить административную политику уровня домена (включая политики схем именования, проекта групп и т. д.), а затем делегировать права администраторам уровня OU.
- **Управление административными группами уровня домена**. Как уже говорилось, администраторы в каждом домене должны иметь высокую степень доверия, потому что их действия могут вызывать последствия на уровне леса. Роль владельца домена состоит в ограничении членства административной группы уровня домена и в делегировании административных прав низшего уровня всегда, когда это возможно.

5.5 Краткие итоги

В этой лекции дано описание различных моделей (с указанием достоинств и недостатков) построения лесов Active Directory:

- Вариант 1 "Единый лес, каждый регион - отдельное дерево".
- Вариант 2 "Единый лес, административный корневой домен, каждый регион - домен".
- Вариант 3 "Единый лес, каждый регион - дочерний домен центрального домена".

Приведены случаи реализации нескольких лесов и указаны недостатки структуры Active Directory, состоящей из нескольких лесов.

После выбора модели структуры леса необходимо определиться с вариантами (учитывая приведенные плюсы и минусы каждого варианта) детализации доменной структуры:

- Вариант 1 "Повторение существующей доменной структуры".
- Вариант 2 "Несколько лесов, минимальное количество доменов".
- Вариант 3 "Единый лес".

Для каждого из доменов, включенных в проект Active Directory, необходимо назначить владельца домена, который будет управлять индивидуальным доменом, а именно:

- создавать политики безопасности уровня домена;
- проектировать конфигурацию групповой политики (Group Policy) уровня домена;
- создавать в домене OU-структуру высокого уровня;
- делегировать административные права в пределах домена;
- управлять административными группами уровня домена.

6 ЛЕКЦИЯ: СТРАТЕГИЯ ИМЕНОВАНИЯ ОБЪЕКТОВ

Приведены различные форматы имен для объектов, используемые Active Directory. Дан краткий обзор службы разрешения имен DNS, которая определяет соглашение об именовании, используемом в Active Directory. Сформулированы правила именования доменов и участников системы безопасности

Цель лекции: Дать представление о планировании стратегии именования объектов в Active Directory.

После принятия решения о том, какую структуру доменов и лесов нужно создать, необходимо переключиться на планирование именования элементов Active Directory, входящих в эту структуру.

6.1 Соглашение об именовании

Каждый объект в Active Directory является экземпляром класса, определенного в схеме Active Directory. У каждого класса имеются атрибуты, обеспечивающие уникальную идентификацию каждого объекта каталога.

Чтобы это реализовать, в Active Directory действует соглашение об именовании, которое должны соблюдать и пользователи, и приложения. Данное соглашение позволяет логически упорядочить хранение объектов и предоставить клиентам стандартизированные методы доступа к объектам, - например, чтобы найти сетевой ресурс, необходимо знать *имя объекта* или одно из его свойств. Служба каталогов Active Directory, использующая и поддерживающая LDAP (стандартный протокол для поиска информации в каталоге), индексирует все атрибуты всех объектов, хранящихся в каталоге, и публикует их [6]. Клиенты, поддерживающие LDAP, могут выполнять всевозможные запросы к серверу.

Active Directory следует соглашению об именовании, принятому в *DNS*. Active Directory поддерживает несколько типов имен, поэтому при работе с Active Directory можно использовать разные форматы имен [3]:

- относительные составные имена;
- составные имена;
- канонические имена;
- основные имена пользователей.

6.1.1 Относительные составные имена

Относительное составное имя (RDN) объекта уникально идентифицирует объект, но только в его родительском контейнере. Таким образом, оно уникально идентифицирует объект относительно других объектов в том же самом контейнере. Например: CN=wjglenn, CN=Users, OC=kd, DC=ru.

Здесь относительным составным именем объекта является CN=wjglenn. RDN родительской организационной единицы (OU) - Users. У большинства объектов RDN - это то же самое, что и атрибут Common Name.

Active Directory автоматически создает RDN по информации, указываемой при создании объекта, и не допускает, чтобы в одном и том же родительском контейнере существовали два объекта с одинаковыми RDN.

В нотации относительных составных имен применяются специальные обозначения, называемые тэгами LDAP-атрибутов и идентифицирующие каждую часть имени:

- DC - тэг Domain Component, который идентифицирует часть DNS-имени домена вроде COM или ORG;
- OU - тэг Organizational Unit, который идентифицирует организационную единицу, являющуюся контейнером;
- CN - тэг Common Name, который идентифицирует простое имя, присвоенное объекту Active Directory.

6.1.2 Составные имена

У каждого объекта в каталоге имеется составное имя (DN), которое уникально на глобальном уровне и идентифицирует не только сам объект, но и место, занимаемое объектом в общей иерархии объектов. DN можно рассматривать как относительное DN объекта, объединенное с относительными DN всех родительских контейнеров, образующих путь к объекту.

Вот типичный пример составного имени: CN=wjglenn, CN=Users, DC=kd, DC=ru.

Это DN означает, что объект пользователя wjglenn содержится в контейнере Users, в свою очередь содержащемся в домене kd.ru. Если объект wjglenn переместят в другой контейнер, его DN изменится и будет отражать новое местоположение в иерархии. DN гарантированно уникальны в лесу, существование двух объектов с одинаковыми DN невозможно.

6.1.3 Канонические имена

Каноническое *имя объекта* используется во многом так же, как и составное. Просто у него другой синтаксис. Составному имени, приведенному в предыдущем подразделе, соответствовало бы следующее каноническое имя: kd.ru/Users/wjglenn.

Таким образом, в синтаксисе составных и канонических имен - два основных отличия. Первое - каноническое имя формируется от корня к объекту, а второе - в каноническом имени не используются тэги LDAP-атрибутов (например, CN и DC).

6.1.4 Основные имена пользователей

Основное имя пользователя (UPN), генерируемое для каждого объекта пользователя, имеет вид имя_пользователя@имя_домена. Пользователи могут входить в сеть под своими основными именами, а администратор при желании может определить для этих имен суффиксы. Основные имена пользователей должны быть уникальными, но Active Directory не проверяет соблюдение этого требования. Лучше всего принять соглашение об именовании, не допускающее дублирования основных имен пользователей.

6.2 Краткий обзор DNS

DNS является службой разрешения имен и использует иерархическое пространство имен для поиска компьютеров (см. рис. 6.1). Корневой домен обозначается точкой ("."). Он представляет собой верхний уровень *DNS*,

остальное пространство имен располагается ниже. На следующем уровне под корневым доменом располагаются домены первого уровня, включая несколько основных (generic) доменных имен (com, edu, mil, net, org и т. д.), около двухсот сокращений названий стран, несколько доменов, которые были введены позже (biz, info, pro и т. д.). Под доменами верхнего уровня расположены домены второго уровня, которые обычно относятся к названиям компаний и должны быть зарегистрированы властями Интернета. Ниже доменов второго уровня располагаются поддомены. Поддомены обычно относятся к отделам или подразделениям в пределах компании. Эти поддомены регистрируются и управляются с DNS-серверов, которые содержат информацию о доменах второго уровня.

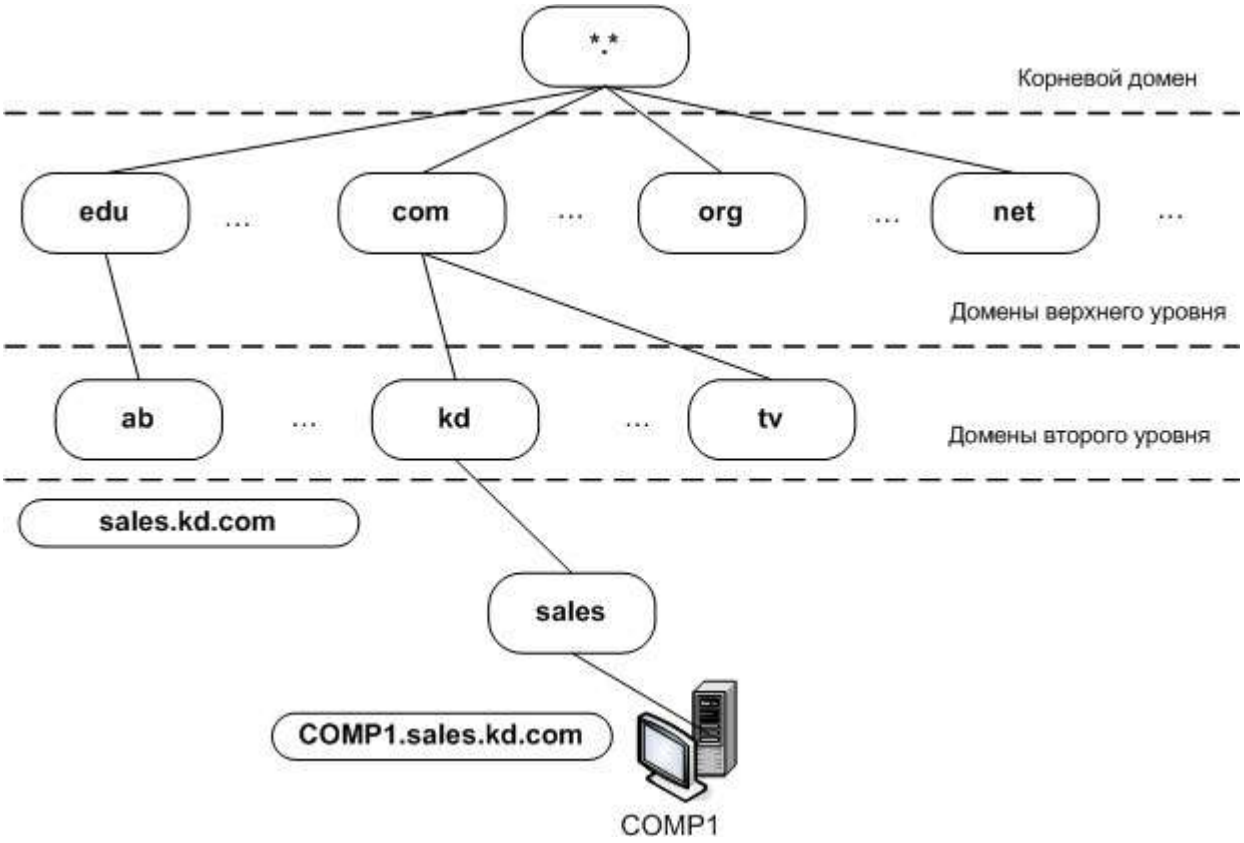


Рис. 6.1. Иерархическая структура пространства имен домена

Поскольку *DNS* использует иерархическое пространство имен, то достаточно просто сконфигурировать его как распределенную базу данных. Прежде чем в Интернете была реализована доменная система имен, вся информация, необходимая для разрешения имен, хранилась в единственном

файле. Поскольку количество хостов в Интернете очень сильно увеличилось, то управление одним файлом стало непрактичным. Была разработана система *DNS*, использующая распределенную базу данных. Применение распределенной базы данных означает, что информация *DNS* хранится на многих компьютерах во всем мире (в случае Интернета) и повсюду в корпоративной сети (в случае внутренней сети). Каждый DNS-сервер обслуживает только одну маленькую часть базы данных *DNS*. Вся база данных разделена на зонные файлы на основе имен доменов. Зонные файлы распределены между несколькими серверами. К примеру, существует около дюжины серверов, которые содержат зонные файлы для корневого домена. Они хранят информацию о DNS-серверах, которые несут зонную информацию для доменов высшего уровня. Корневые серверы не содержат всю информацию о доменах высшего уровня, но они знают, какие серверы имеют эту информацию.

DNS-серверы, хранящие информацию о доменах высшего уровня, содержат также информацию о том, на каких серверах находятся зонные файлы для доменов следующего уровня. Например, сервер может содержать зонные файлы для домена com, то есть этот сервер знает обо всех доменах второго уровня, которые зарегистрированы с доменом com, но он может не знать отдельные детали о домене второго уровня. Сервер домена высшего уровня знает, какой компьютер на следующем уровне содержит детали, касающиеся домена второго уровня, и так продолжается до самого низа пространства имен *DNS*. Сервер, ответственный за домен com, может иметь домен kd, зарегистрированный как домен второго уровня. Этот сервер может передавать любые запросы на информацию о домене kd на сервер, который содержит зонные файлы для kd.com.

Использование метода распределенной базы данных означает, что никакому серверу в Интернете не требуется иметь всю информацию *DNS*. Большинство серверов хранят информацию о некоторой части дерева, но когда приходит запрос, который они не могут выполнить, им известно, какой

DNS-сервер хранит необходимую информацию. DNS-серверы используют делегированные записи, ретрансляторы (forwarders) и корневые ссылки для определения того, какой DNS-сервер имеет необходимую информацию.

Текущие записи, хранящиеся в зонных файлах *DNS*, называются записями ресурсов (RR - Resource Records). Записи ресурсов содержат текущую информацию о домене, на DNS-сервере системы Windows Server 2003 можно создать двадцать два различных типа записей ресурсов [13].

6.2.1 Служба DNS Locator

Служба *DNS* Locator (указатель *DNS*) очень важна для Active Directory, потому что *DNS* обеспечивает информацию, которая необходима клиентам для поиска контроллеров домена в сети.

Чтобы облегчить нахождение контроллеров домена, Active Directory использует указатель служб (service locator) или записи SRV. Первая часть SRV-записи идентифицирует службу, на которую указывает запись SRV [13]:

- _ldap Active Directory является службой каталога, совместимой с LDAP-протоколом, с контроллерами домена, функционирующими как LDAP-серверы. Записи _ldap SRV идентифицируют LDAP-серверы, имеющиеся в сети. Эти серверы могут быть контроллерами домена Windows Server 2003 или другими LDAP-серверами;
- _kerberos - основной опознавательный протокол для всех клиентов Windows 2000 и Windows XP. SRV-записи _kerberos идентифицируют все ключевые центры распределения (Key Distribution Centers, KDC) в сети. Они могут быть контроллерами домена с Windows Server 2003 или другими KDC-серверами;
- _kpassword идентифицирует серверы изменения паролей Kerberos в сети (это контроллеры домена или с Windows Server 2003, или с другими системами изменения пароля Kerberos);
- _gc - специфическая запись, относящаяся к функции глобального каталога в Active Directory.

6.2.2 Интегрированные зоны Active Directory

Один из самых больших плюсов выполнения *DNS* в операционной системе Windows Server 2003 заключается в использовании интегрированных зон (integrated zones) Active Directory, которые дают множество преимуществ [13].

- Зонная информация больше не хранится в зонных файлах на жестком диске DNS-сервера, она сохраняется в базе данных Active Directory, что обеспечивает дополнительную защиту.
- Процесс зонной передачи заменен репликацией Active Directory. Поскольку зонная информация хранится в Active Directory, данные копируются через нормальный процесс репликации Active Directory. Это означает, что репликация происходит на уровне атрибутов так, что копируются только изменения зонной информации. Трафик репликации между сайтами можно сильно сжать, увеличив пропускную способность. Использование интегрированной зоны Active Directory дает возможность использовать разделы приложений для тонкой настройки репликации информации *DNS*.
- Интегрированные зоны дают возможность конфигурирования DNS-сервера с несколькими хозяевами. Без Active Directory *DNS* может поддерживать только один основной сервер имен для каждого домена. Это означает, что все изменения в зонной информации должны быть сделаны на основном сервере имен, а затем переданы на дополнительные серверы имен. С интегрированными зонами Active Directory каждый DNS-сервер имеет перезаписываемую копию доменной информации, так что изменения зонной информации могут быть сделаны в любом месте в организации. Информация затем копируется на все другие серверы *DNS*.
- Интегрированную зону можно сконфигурировать так, чтобы использовать только безопасные обновления, то есть контролировать, какие пользователи и компьютеры обновляют записи ресурсов в Active Directory.

Самым большим недостатком интегрированной зоны Active Directory является необходимость установки *DNS* на контроллере домена Windows Server 2003, что создает дополнительную нагрузку на него.

Когда зона сконфигурирована как интегрированная зона Active Directory, можно просматривать информацию *DNS* в Active Directory [6].

6.3 Определение стратегии именования

При выработке стратегии именования необходимо учитывать требования к именованию, предъявляемые как Active Directory, так и *DNS* [3]:

- поддерживается иерархия, длина имени до 64 символов;
- поддерживается подключение к внешним сетям.

Клиенты используют *DNS* для разрешения IP-адресов серверов, на которых выполняются важные сетевые сервисы Active Directory. Следовательно, Active Directory и *DNS* неразрывно связаны.

В *DNS* имена образуют иерархию и формируются путем "движения" от родительских доменов к дочерним доменам. Так, у домена kd.ru может быть дочерний домен sales.kd.ru, у того, в свою очередь, - дочерний домен europe.sales.kd.ru. Имя каждого домена соответствует пути,

идентифицирующему домен в иерархии *DNS*, т. е. пути к корневому домену (корневой домен обозначается точкой).

Когда создается первый домен Active Directory, он становится корневым для леса и первого дерева доменов в этом лесу. С этого корневого домена начинается пространство имен. Каждый добавляемый домен получает имя от родительского домена и иерархии, в которую входит родительский домен.

Все имена доменов Active Directory идентифицируются по *DNS*, но можно использовать и NetBIOS-имена (Network Basic Input/Output System) - унаследованную систему именования, которая применялась в старых версиях Windows и по-прежнему поддерживается в Windows Server 2003. Windows автоматически генерирует NetBIOS-имена для каждой службы, выполняемой на компьютере, добавляя к имени компьютера дополнительный символ. Доменам также присваиваются NetBIOS-имена, при этом совместимость с NetBIOS-именами - это плоская модель, длина имени не более 16 символов.

Существует возможность назначать разные NetBIOS- и DNS-имена, но такой подход не допустим.

В идеале следует создать стратегию именования, определяющую единообразный подход к формированию имен.

6.3.1 Идентификаторы защиты

Active Directory использует модель репликации с несколькими хозяевами, при которой на каждом контроллере домена хранится своя копия раздела Active Directory; контроллеры домена являются равноправными хозяевами. Можно внести изменения в объекты, хранящиеся на любом контроллере домена, и эти изменения реплицируются на другие контроллеры.

Модель с несколькими хозяевами хорошо подходит для большинства операций, но не для всех. Некоторые операции должны выполняться только одним контроллером в каждом домене или даже в каждом лесу. Чтобы

выполнять эти специальные операции, определенные контроллеры доменов назначаются хозяевами операций.

При выработке стратегии именования представляют интерес две роли хозяев операций [3]:

- *Хозяин именования доменов* **(domain naming master)**. Один домен в каждом лесу, обрабатывает добавление и удаление доменов и генерирует уникальный идентификатор защиты (SID);
- *Хозяин RID* **(relative ID master)**. Генерирует последовательности для каждого из контроллеров домена. Действует в пределах домена. Генерирует для каждого контроллера домена пул по 500 RID.

Два сервера, выполняющих эти роли, должны быть доступны, когда создаются и именуются новые участники системы безопасности (security principals).

6.3.2 Правила имен участников системы безопасности

Объекты участников системы безопасности - это объекты Active Directory, которым назначены идентификаторы защиты и которые указываются при входе в сеть и предоставлении доступа к ресурсам домена.

Администратор должен давать объектам участников системы безопасности (учетным записям пользователей, компьютеров и групп) имена, уникальные в рамках домена. Следовательно, необходимо выработать стратегию именования, которая позволит это реализовать.

Добавляя в каталог учетную запись нового пользователя, администратор должен задать следующую информацию [3]:

- имя, которое пользователь должен указывать при входе в сеть;
- имя домена, содержащего учетную запись пользователя;
- прочие атрибуты (имя, фамилия, телефон и т. п.)

К создаваемым именам для участников системы безопасности предъявляются следующие требования [3]:

- имена могут содержать любые символы Unicode, за исключением следующих символов: #, +, ", \, <, >;
- длина имен учетных записей пользователей не должна превышать 20 символов;
- длина имен учетных записей компьютеров не должна превышать 15 символов;

- длина имен учетных записей групп не должна превышать 63 символов;
- имена участников системы безопасности не могут состоять только из точек, пробелов и знаков @;
- любые точки или пробелы в начале имени пользователя отбрасываются.

Допускается применение одного и того же имени участника системы безопасности в разных доменах. Так, можно создать пользователя wjglenn в доменах hr.kd.ru и sales.kd.ru. Это не приведет к проблемам, поскольку составное, относительное составное и каноническое имена каждого объекта автоматически генерируются Active Directory и все равно позволяют глобально идентифицировать этот объект.

6.3.3 Правила именования доменов

Допускается изменение доменных имен после развертывания, но это может оказаться затруднительным. Лучше с самого начала выбрать правильные доменные имена, при выборе которых рекомендуется соблюдать следующие правила [3].

- Использовать только символы, разрешенные стандартами Интернета: a-z, 0-9 и дефис (-). Хотя реализация *DNS* в Windows Server 2003 поддерживает и другие символы, применение стандартных символов гарантирует возможность взаимодействия с другими реализациями *DNS*.
- Использовать короткие доменные имена, которые легко идентифицировать и которые соответствуют соглашению об именовании в NetBIOS.
- В качестве основы имени корневого домена применять только зарегистрированные доменные имена. Даже если в качестве имени корня леса не используется зарегистрированное DNS-имя, это поможет избежать путаницы. Например, у компании может быть зарегистрирован домен kd.ru. Если даже имя kd.ru и не задействовано в качестве имени корневого домена леса, то все равно целесообразно формировать имя, производное от kd.ru (скажем, sales.kd.ru).
- Не использовать дважды одно и то же доменное имя. Иное возможно только в сетях, которые не взаимодействуют между собой (например, можно создать домен microsoft.com в частной сети, не подключенной к Интернету). Но это плохой подход, который когда-нибудь обязательно приведет к путанице.
- Для большей безопасности создать отдельные внутреннее и внешнее пространства имен, чтобы предотвратить несанкционированный доступ к закрытым ресурсам. При этом рекомендуется создавать внутреннее имя на основе внешнего (например, kd.ru и local.kd.ru).

6.4 Краткие итоги

В этой лекции приведено соглашение об именовании в Active Directory, с описанием разных форматов имен:

- Относительные составные имена.
- Составные имена.
- Канонические имена.
- Основные имена пользователей.

Дан краткий обзор службы доменных имен *DNS* и указана ее взаимосвязь с Active Directory. Один из самых больших плюсов выполнения *DNS* в операционной системе Windows Server 2003 заключается в использовании интегрированных зон (integrated zones) Active Directory, которые дают множество преимуществ.

- Зонная информация больше не хранится в зонных файлах на жестком диске DNS-сервера, она сохраняется в базе данных Active Directory.
- Процесс зонной передачи заменен репликацией Active Directory.
- Интегрированные зоны дают возможность конфигурирования DNS-сервера с несколькими хозяевами.
- Интегрированную зону можно сконфигурировать так, чтобы использовать только безопасные обновления.

При выработке стратегии именования необходимо учитывать требования к именованию, предъявляемые как Active Directory, так и *DNS*:

- поддерживается иерархия, длина имени до 64 символов;
- поддерживается подключение к внешним сетям.

При выработке стратегии именования интерес представляют две роли хозяев операций:

- Хозяин именования доменов;
- Хозяин RID.

Два сервера, выполняющих эти роли, должны быть доступны, когда создаются и именуются новые участники системы безопасности (security principals).

Сформулированы правила именования участников системы безопасности и доменов.

7 ЛЕКЦИЯ: ПЛАНИРОВАНИЕ ИНФРАСТРУКТУРЫ DNS И СТРУКТУРЫ OU

В данной лекции продолжено рассмотрение вопроса, как планировать службу Active Directory перед ее развертыванием. Рассмотрены процессы планирования доменного пространства имен (от исследования существующей инфраструктуры DNS до выбора доменных имен) и создания структуры организационных единиц (различные модели иерархии, типовая конфигурация)

Цель лекции: Дать представление о процессах планирования доменного пространства имен и создания структуры организационных единиц.

7.1 Проектирование инфраструктуры DNS

В службе Active Directory домены имеют DNS-имена. Прежде чем использовать *DNS* в сети, необходимо спланировать пространство имен *DNS*, то есть нужно продумать, как будет применяться именование *DNS* и для каких целей.

Ключевое решение проекта состоит в том, чтобы определить, где расположить домены Active Directory в пределах этого пространства имен. В дополнение к этому необходимо также спроектировать конфигурацию сервера *DNS*. Если компания уже имеет свою инфраструктуру *DNS*, то придется спроектировать собственное пространство имен, чтобы вписаться в текущее пространство имен, а также сконфигурировать DNS-серверы Windows Server 2003 для взаимодействия с существующими серверами *DNS*.

7.1.1 Исследование существующей инфраструктуры DNS

Первый шаг в проектировании инфраструктуры *DNS* должен состоять в исследовании уже имеющейся инфраструктуры *DNS*. В большинстве случаев служба *DNS* в Active Directory должна взаимодействовать с имеющейся инфраструктурой *DNS*. Это может означать просто конфигурирование ретранслятора в существующем сервере *DNS*, использование имеющегося

DNS-сервера как основного для Active Directory или отсутствие развертывания *DNS* в Windows Server 2003. Active Directory требует, чтобы работала служба *DNS*, однако существует несколько вариантов ее развертывания.

При исследовании существующей инфраструктуры *DNS* необходимо выполнить следующие действия [13]:

- задокументировать все DNS-имена доменов, используемые в настоящее время в пределах компании. Сюда входят имена, встречающиеся в Интернете, а также внутренние имена;
- задокументировать все дополнительные имена, которые компания зарегистрировала для возможности использования в Интернете;
- задокументировать существующую конфигурацию серверов *DNS*. Эта документация должна включать типы DNS-серверов, в настоящее время развернутых в сети. Кроме того, конфигурация *DNS* должна содержать информацию о ретрансляторах, о делегировании зон и о конфигурации основных и дополнительных серверов.

7.1.2 Выбор доменных имен DNS

При настройке DNS-серверов рекомендуется сначала выбрать и зарегистрировать уникальное родительское имя *DNS*, которое будет представлять организацию в Интернете. Это имя является доменом второго уровня внутри одного из доменов верхнего уровня, используемых в Интернете.

Прежде чем задавать родительское имя *DNS* для организации, необходимо убедиться, что это имя не присвоено другой организации. Родительское имя *DNS* можно соединить с именем местоположения или подразделения внутри организации для формирования других имен доменов следующих уровней.

Для внедрения Active Directory существуют два вида пространств имен (внутреннее и внешнее), при этом пространство имен Active Directory совпадает с заданным зарегистрированным пространством имен *DNS* или отличается от него [4]:

- **Совпадающие внутреннее и внешнее пространства имен**. Согласно этому сценарию, организация использует одно и то же имя для внутреннего и

внешнего пространств имен - имя компании применяется как внутри, так и вне организации. Для реализации этого сценария надо соблюдать следующие условия. Пользователи внутренней частной сети компании должны иметь доступ как к внутренним, так и к внешним серверам (по обе стороны брандмауэра). Для защиты конфиденциальной информации клиенты, осуществляющие доступ извне, не должны иметь доступ к внутренним ресурсам компании или иметь возможность разрешать свои имена. Кроме того, необходимы две раздельные зоны *DNS*, одна из которых, за пределами брандмауэра, обеспечивает разрешение имен для общедоступных ресурсов. Она не сконфигурирована для разрешения имен внутренних ресурсов, поэтому доступ к ним извне получить нельзя.

- **Отличающиеся внутреннее и внешнее пространства имен**. В этом случае компания использует различные внутреннее и внешнее пространства имен - изначально в зонах по разные стороны брандмауэра имена различаются. Для этого необходимо зарегистрировать два пространства имен в *DNS* Интернета. Цель регистрации - предотвратить дублирование внутреннего имени другой общедоступной сетью. Если имя не зарезервировано, внутренние клиенты не смогут отличить внутреннее имя от имени, зарегистрированного в общедоступной сети пространства имен *DNS*. Таким образом, устанавливаются две зоны: одна отвечает за разрешение имен во внешнем пространстве, другая - во внутреннем. Пользователям не составит труда различать внутренние и внешние ресурсы.

7.2 Проектирование структуры OU

После определения структуры домена организации и планирования доменного пространства имен необходимо разработать структуру организационных единиц (OU или подразделений - ОП). По информации, собранной о компании и ее персонале, необходимо определить, как лучше всего делегировать административные полномочия в доменах. Можно создать иерархию ОП в домене: в отдельном домене разместить пользователей и ресурсы, повторив структуру компании в конкретном подразделении. Таким образом, можно создать логичную и осмысленную модель организации и делегировать административные полномочия на любой уровень иерархии.

В каждом домене разрешается внедрять собственную иерархию ОП. Если организация имеет несколько доменов, то можно создать структуры ОП внутри каждого домена независимо от структуры в других доменах.

Организационное подразделение позволяет [4]:

- отразить структуру компании и организации внутри домена. Без ОП все пользователи поддерживаются и отображаются в одном списке независимо от подразделения, местоположения и роли пользователя;
- делегировать управление сетевыми ресурсами, но сохранить способность управлять ими, то есть присваивать административные полномочия пользователям или группам на уровне ОП;
- изменять организационную структуру компании;

- группировать объекты так, чтобы администраторы легко отыскивали сетевые ресурсы.

Не следует создавать структуру OU исключительно ради того, чтобы просто иметь какую-то структуру: OU используются в определенных целях. К этим целям относятся [3]:

- **делегирование административного управления объектами**. Правильно разработанная структура OU позволяет администраторам эффективно делегировать полномочия. Каждое OU по умолчанию наследует разрешения, заданные для родительского OU. Аналогично объекты, содержащиеся в OU, наследуют разрешения, заданные для этого OU (и для каждого из его родителей). Наследование - эффективный способ предоставить или делегировать разрешения на доступ к объектам. Преимущество наследования в том, что администратор может управлять разрешениями на доступ ко всем объектам в OU, задавая разрешения для самого OU, а не конфигурируя все дочерние объекты по отдельности;
- **ограничение видимости объектов**. В некоторых организациях определенные объекты должны быть скрыты от определенных администраторов или пользователей. Даже если запретить изменение атрибутов объекта, пользователи, имеющие доступ к контейнеру с таким объектом, все равно смогут видеть, существует ли этот объект. Однако можно скрыть объекты, поместив их в OU и ограничив круг пользователей, которые имеют разрешение на список содержимого (List Contents) для этой OU. Тогда объекты, помещенные в контейнер, будут невидимы пользователям, не имеющим этого разрешения;
- **управление применением групповой политики**. Групповая политика позволяет применять одни и те же параметры конфигурации сразу к нескольким объектам. С ее помощью можно определять параметры пользователей (например, ограничения, налагаемые на пароли) или компьютеров. При использовании групповой политики создается *объект групповой политики* (Group Policy Object, GPO) - объект, связанный с доменом, сайтом или OU и содержащий параметры конфигурации, которые требуется применить.

Возможности ОП облегчат обеспечение безопасности и выполнение любых административных задач.

Первый этап проектирования административной структуры защиты - планирование использования организационных единиц (OU) в каждом домене. Следующий этап проектирования этой структуры - выработка стратегии управления учетными записями пользователей, компьютеров и групп. После этого необходимо разработать эффективную реализацию групповой политики.

OU служит контейнером, в который можно поместить ресурсы и учетные записи домена. Затем можно назначить OU административные разрешения и позволить содержащимся в нем объектам наследовать эти разрешения. OU могут содержать любые объекты следующих типов [3]:

пользователи; компьютеры; группы; принтеры; приложения; политики безопасности; общие папки; другие OU.

7.2.1 Планирование иерархии OU

При планировании иерархии ОП важно соблюсти следующие правила [4]:

- Хотя глубина иерархии ОП не ограничена, производительность мелкой иерархии выше, чем глубокой.
- ОП должны отражать неизменные структурные единицы организации.

Существует много способов структурирования ОП в организации. На этапе планирования развертывания Active Directory важно определить, какая модель ляжет в основу иерархии ОП. Например, существуют следующие модели классификации ОП в иерархии ОП [4]:

- **Модель деления на ОП согласно выполняемым задачам**. ОП можно создавать, учитывая функции, которые необходимо выполнять внутри организации. Верхний уровень ОП может соответствовать бизнес-подразделениям компании, при этом следующие уровни ОП - это функциональные подразделения внутри бизнес-подразделений.
- **Географическая модель деления на ОП. Иногда при создании ОП учитывается местоположение филиалов компании**. Верхний уровень ОП соответствует региональным подразделениям организации, а второй уровень представляет физическое местоположение офисов компании.
- **Модель деления на ОП согласно выполняемым задачам и географическому местоположению**. В некоторых случаях две описанные выше модели создания ОП совмещают. Верхний уровень ОП учитывает, где географически расположены офисы компании. Второй уровень ОП построен на основе функциональных особенностей каждого подразделения внутри организации.

Следует уделять особое внимание верхнему уровню структуры OU, который всегда должен отражать относительно неизменную часть структуры предприятия, чтобы его не приходилось изменять в случае реорганизации. Так, следующие типы структуры верхнего уровня основаны на постоянных характеристиках предприятия, изменение которых маловероятно [3]:

- **Физические участки**. В филиалах, физически расположенных в разных местах (особенно, когда компания действует на обширной территории, например в нескольких странах), часто имеются свои ИТ-отделы, поэтому у филиалов разные требования к администрированию. Создание отдельного OU верхнего уровня для каждого филиала - один из вариантов архитектуры, основанной на

задачах; в зависимости от местонахождения определяются разные административные задачи.

- **Типы административных задач**. Структура верхнего уровня, основанная на административных задачах, относительно постоянна. Какие бы реорганизации не происходили в компании, основные типы административных задач вряд ли сильно изменятся.
- **Типы объектов**. Как и структура, основанная на задачах, структура, в которой OU верхнего уровня соответствуют типам объектов, обеспечивает устойчивость архитектуры к изменениям.

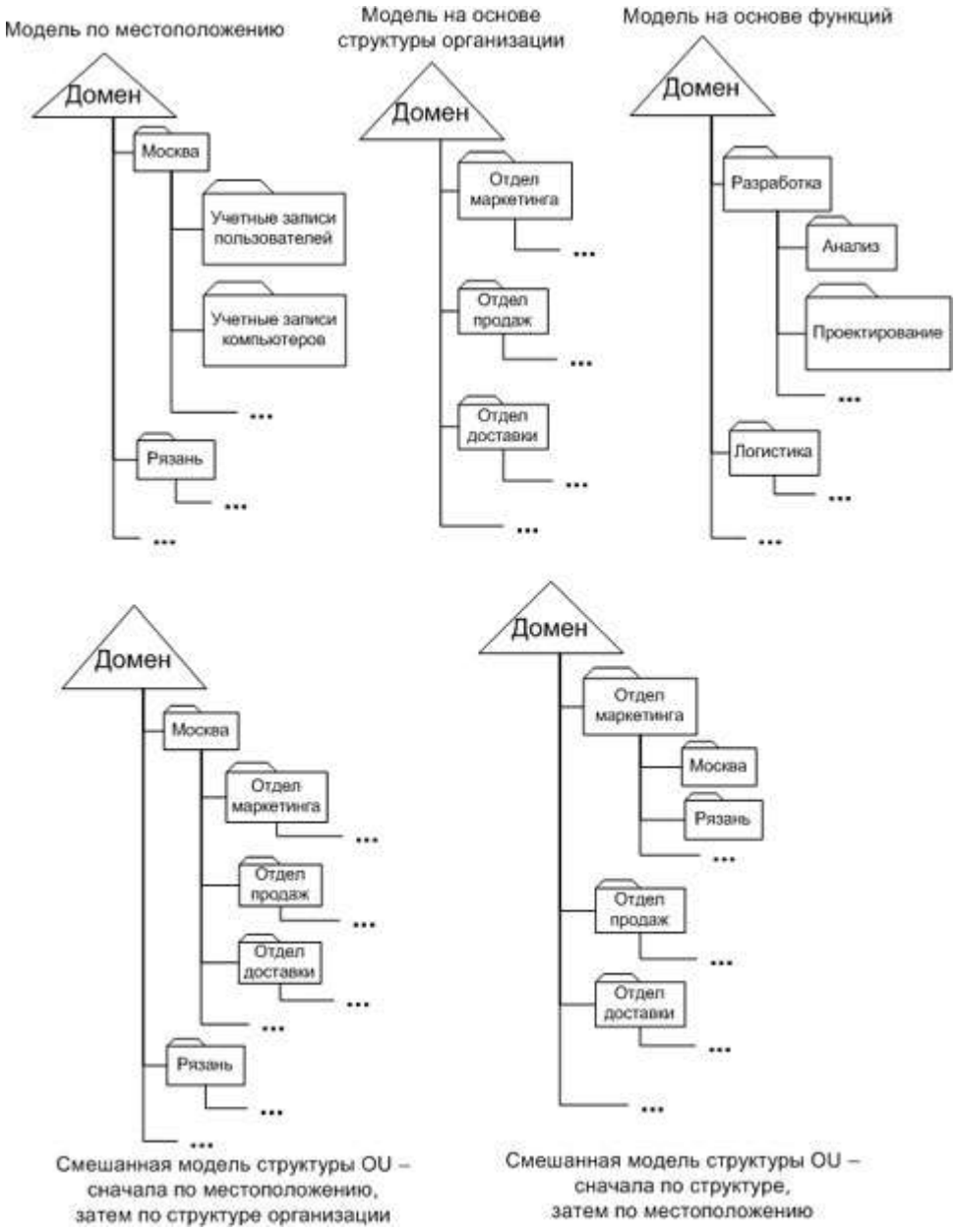
При планировании структуры OU верхнего уровня для среды с несколькими доменами есть смысл подумать о создании структуры верхнего уровня, которая будет одной и той же для каждого домена сети. Создание структуры OU, одинаковой для различных доменов, позволяет реализовать единый подход к администрированию и поддержке сети.

OU нижних уровней, создаваемые в OU верхнего уровня, должны использоваться для более тонкого управления административными полномочиями или в других целях, например для применения групповой политики. При этом надо учитывать, что по умолчанию OU нижних уровней наследуют разрешения от родительских OU. Поэтому при планировании архитектуры OU необходимо определить, когда наследуются разрешения и когда они не наследуются. Архитектура OU нижних уровней должна быть как можно проще: если создать слишком глубоко вложенную структуру OU, то можно столкнуться и со снижением производительности.

7.2.2 Стандартные модели структуры OU

Наряду с перечисленными выше моделями классификации ОП в иерархии ОП можно использовать следующую терминологию (см. рис. 7.1) для стандартных моделей [3]:

- Модель структуры OU на основе местоположения.
- Модель структуры OU на основе структуры организации.
- Модель структуры OU на основе функций.
- Смешанная модель структуры OU - сначала по местоположению, затем по структуре организации.
- Смешанная модель структуры OU - сначала по структуре, затем по местоположению.



увеличить изображение

Рис. 7.1. Модели построения структуры организационных единиц

7.2.3 Модель структуры OU на основе местоположения

В модели OU на основе местонахождения административные полномочия распределены между несколькими филиалами, расположенными в разных местах. Эта модель полезна, когда у каждого филиала свои требования к администрированию, отличные от требований других филиалов.

Преимущества модели:

- OU устойчивы к изменениям;
- для центрального ИТ-отдела легко реализовать общедоменные политики;
- легко определять положение ресурсов;
- легко создавать новые OU при расширении компании.

Недостатки:

- предполагается наличие администратора в каждом филиале;
- архитектура не соответствует административной структуре компании.

7.2.4 Модель структуры OU на основе структуры организации

В модели OU на основе структуры организации административные полномочия распределены между отделами или подразделениями, в каждом из которых имеется собственный администратор. Эта модель полезна, когда у компании есть четкая структура отделов.

Преимущества модели:

- обеспечивает определенный уровень автономии для каждого отдела;
- поддерживает слияния и расширения;
- удобна для администраторов.

Недостаток:

- уязвима при реорганизации, так как может потребоваться изменение верхнего уровня структуры OU.

7.2.5 Модель структуры OU на основе функций

В модели OU на основе функций административный персонал децентрализован и использует модель управления, которая основана на бизнес-функциях, существующих в организации. Это идеальный выбор для малых компаний, в которых ряд бизнес-функций выполняется несколькими отделами одновременно.

Основное преимущество модели - устойчивость при реорганизациях, недостаток модели - создание дополнительных OU для делегирования

административного управления пользователями, компьютерами, принтерами и т. п.

7.2.6 Смешанная модель структуры OU - сначала по местоположению, затем по структуре организации

В этой модели сначала создаются OU верхнего уровня, представляющие географические участки, на которых находятся филиалы компании, а потом - OU более низкого уровня, представляющие структуру организации.

Преимущества модели:

- поддерживает рост числа подразделений;
- позволяет создавать зоны безопасности.

Недостатки:

- при реорганизации административного персонала необходимо пересмотреть структуру;
- необходимо взаимодействие между администраторами, работающими в разных отделах одного филиала.

7.2.7 Смешанная модель структуры OU - сначала по структуре, затем по местоположению

В этой модели сначала создаются OU верхнего уровня, представляющие организационную структуру компании, а потом - OU более низкого уровня, представляющие территориальные участки.

Преимущества модели:

- надежная защита на уровне отделов и подразделений;
- возможность делегировать административные полномочия в зависимости от местоположения.

Недостаток:

- уязвимость при реорганизациях.

Типовая конфигурация OU

Как правило, обычная конфигурация - это как раз смешанная модель иерархии ОП, например: OU высшего уровня, основанные на географических регионах, со следующим уровнем OU в пределах каждого региона, основанных на деловых подразделениях. Некоторые компании могут выбрать OU высшего уровня, основанные на деловых подразделениях, а затем создавать под высшим уровнем структуру OU, основанную на географии.

OU высшего уровня могут включать OU службы учетных записей для всех служебных учетных записей, используемых в домене. Создание на высшем уровне OU для специальных учетных записей пользователей, таких как служебные учетные записи, упрощает их администрирование. OU высшего уровня могут включать OU серверов, если все серверы управляются централизованно. В дополнение к этим административным OU могут быть созданы также OU высшего уровня, основанные на географии корпорации. Организационные единицы высшего уровня, основанные на географии, могут использоваться для делегирования административных задач.

OU второго уровня в каждом географическом регионе основаны на деловых подразделениях региона. OU бизнес-подразделений могли бы применяться для делегирования администрирования, а также для назначения групповых политик. Под деловыми OU располагаются OU, основанные на отделах. На этом уровне OU будет использоваться для назначения групповых политик или определенных административных задач, типа права сброса паролей.

OU отделов могут содержать другие OU [13]:

- **OU учетных записей**. Содержит учетные записи пользователей и групп отдела. В некоторых случаях OU учетных записей разбиваются на OU, содержащие группы, учетные записи пользователей или удаленных пользователей.
- **OU компьютеров**. Содержит все пользовательские компьютеры и включает отдельные OU компьютеров с различными операционными системами.
- **OU ресурсов**. Содержит ресурсы, связанные с данной OU. Включает домены локальных групп, серверы, принтеры и совместно используемые папки.
- **OU приложений или проектов**. Если группа людей и ресурсов работают над определенным проектом (приложением), который требует уникального управления, можно создать структуру OU для этих пользователей, а затем

сгруппировать пользователей, ресурсы и компьютеры, необходимые для данного проекта, в OU.

7.3 Краткие итоги

8 ЛЕКЦИЯ: СТРАТЕГИЯ УПРАВЛЕНИЯ УЧЕТНЫМИ ЗАПИСЯМИ

Для возможности планирования учетных записей в Active Directory перечислены их типы, даны правила и рекомендации управления учетными записями компьютеров и пользователей. Освещены вопросы, связанные с безопасностью, - планирование политики сетевой безопасности, планирование групп и групповых политик

Цель лекции: Выработать стратегию управления учетными записями для возможности ее применения при развертывании Active Directory.

8.1 Типы учетных записей

Учетная запись в Active Directory - это список атрибутов, определяющих участника системы безопасности (security principal), например пользователя или группу пользователей.

В Active Directory можно создать пять типов учетных записей [3], перечисленных ниже.

- **Компьютер**. Всякий раз, когда в *домен* добавляется компьютер под управлением Microsoft Windows NT, Windows 2000, Windows XP или Windows Server 2003, для него создается *учетная запись* компьютера. Учетные записи компьютеров служат для аутентификации компьютеров, которые обращаются к сети и ресурсам домена.
- **Пользователь**. *Учетная запись* пользователя - это набор атрибутов для пользователя. Объект-пользователь хранится в Active Directory и позволяет пользователю входить в сеть. Пользователь должен указать удостоверения (имя и пароль) только один раз, затем ему предоставляются соответствующие разрешения на доступ к сетевым ресурсам.
- **Группа**. Это набор пользователей, компьютеров или других групп, для которого можно задать разрешения. Задавая разрешения группам и добавляя члены в эти группы, можно сэкономить время, поскольку не приходится назначать разрешения каждому отдельно взятому члену группы.
- **InetOrgPerson**. *Учетная запись* InetOrgPerson работает во многом аналогично учетной записи пользователя за исключением того, что учетные записи InetOrgPerson совместимы с другими службами каталогов, основанными на *LDAP*. Это обеспечивает совместимость между Active Directory и другими системами.
- **Контакт**. Этот *объект* хранится в Active Directory, но для него не задаются разрешения. То есть контакт нельзя использовать для входа в сеть или доступа к ресурсам. Часто контакты связывают с пользователями, работающими вне сети, которым отправляет сообщения почтовая система.

8.2 Планирование учетных записей компьютеров

Учетные записи компьютеров позволяют применять к компьютерам, входящим в *домен*, во многом такие же средства защиты, как и для

пользователей. Эти записи дают возможность выполнять аутентификацию компьютеров - членов домена прозрачным для пользователей образом, добавлять серверы приложений как рядовые серверы (member servers) в доверяемые домены и запрашивать аутентификацию пользователей или служб, которые обращаются к этим серверам ресурсов.

Так как разрешается помещать учетные записи компьютеров в OU и назначать им групповую политику, то можно управлять тем, как выполняется аутентификация и обеспечивается защита компьютеров различных типов. Например, для компьютеров, установленных в общедоступном информационном киоске, действуют другие требования безопасности, чем для рабочих станций, установленных в управляемой среде с ограниченным доступом.

Всякий раз, когда в *домен* добавляется новый компьютер, создается новая *учетная запись* компьютера. Таким образом, еще одна составляющая стратегии управления учетными записями - определение пользователей, которые вправе добавлять компьютеры в *домен*, создавая их учетные записи.

Кроме того, необходимо продумать соглашение об именовании компьютеров. Хорошее соглашение должно позволять без труда идентифицировать компьютер по владельцу, местонахождению, типу или любой комбинации этих данных.

8.3 Планирование учетных записей пользователей

Учетные записи пользователей позволяют идентифицировать пользователей, входящих в сеть, задавать, к каким ресурсам они вправе обращаться, и указывать о них всевозможную информацию. Администраторы - тоже пользователи, но с более широкими правами доступа к ресурсам, связанным с управлением сетью. Группы служат для того, чтобы формировать наборы пользователей, для которых нужно задать одни и те же требования к безопасности или права доступа.

Учетные записи пользователей предоставляют пользователям возможность входить в *домен* или на локальный компьютер и обращаться к ресурсам. Объекты учетных записей пользователей содержат информацию о пользователях и связывают с ними определенные привилегии или ограничения. Каждый *объект* Active Directory связан со списком управления доступом (Access Control List, ACL), который представляет собой список разрешений на доступ к объекту, заданных для пользователей и групп.

8.3.1 Типы учетных записей пользователей

В Windows Server 2003 существует два основных типа учетных записей пользователей [3]:

- **Локальные учетные записи пользователей**. Создаются в базе данных защиты локального компьютера и управляют доступом к ресурсам этого компьютера. Локальные учетные записи пользователей предназначены для управления доступом к изолированным компьютерам или к компьютерам, входящим в рабочую группу.
- **Доменные учетные записи пользователей**. Создаются в Active Directory и дают возможность пользователям входить в *домен* и обращаться к любым ресурсам сети. Такие учетные записи пользователей реплицируются на все контроллеры в домене, поэтому после репликации любой контроллер домена сможет аутентифицировать пользователя.

Помимо этих учетных записей, Windows автоматически создает несколько таких учетных записей пользователей, которые называются встроенными. И на локальных компьютерах, и в доменах создается две ключевые учетные записи [3]:

- **Администратор (Administrator)**. Данная *учетная запись* обладает наибольшими возможностями, поскольку она автоматически включается в группу "Администраторы" (Administrators). Члены этой группы имеют высший уровень прав по управлению компьютером, им предоставляются почти все пользовательские права. *Учетная запись* "Администратор уровня домена" дает максимум возможностей по управлению доменом в целом; по умолчанию она включается в группу "Администраторы домена" (Domain Admins) (а администратор корневого домена леса, кроме того, входит в группы "Администраторы предприятия" (Enterprise Admins) и "Администраторы схемы" (Schema Admins)]. Учетную запись "Администратор" нельзя удалить, но ее можно переименовать (и это следует сделать для большей безопасности). Также следует задать для этой учетной записи непустой пароль и не передавать его другим пользователям.
- **Гость (Guest)**. Данная *учетная запись* предназначена для того, чтобы администратор мог задать единый набор разрешений для любых пользователей,

которые иногда входят в сеть, но не имеют обычной учетной записи. *Учетная запись* "Гость" позволяет это сделать, так как автоматически включается в локальную группу "Гости" (Guests). В среде, где есть *домен*, эта *учетная запись* также включается в группу "Гости домена" (Domain Guests). По умолчанию *учетная запись* "Гость" отключена. И действительно, ее следует использовать только в сетях, не требующих особой защиты. Эту учетную запись нельзя удалить, но можно отключить и/или переименовать.

8.3.2 Правила именования учетных записей

Тщательное планирование схемы именования учетных записей пользователей позволяет стандартизировать идентификацию пользователей домена. Единое соглашение также облегчает распознавание и запоминание имен пользователей.

Существует много разных соглашений, применимых при создании имен, и у каждого администратора или проектировщика сети есть свои предпочтения. Однако хорошее соглашение об именовании должно быть таким, чтобы имена для входа легко запоминались, а также чтобы можно было различать сотрудников с похожими именами.

Есть несколько правил, которые нужно соблюдать при планировании стратегии именования пользователей [3]:

- Каждый пользователь должен иметь уникальное имя (логин) в домене.
- Длина имени не должна превышать 20 символов (для совместимости с предыдущими версиями Windows).
- Имена не чувствительны к регистру букв.
- Имена не должны содержать следующих символов: ", /, \, [,], :, ;, =, ,, +, *, ?, <, >.
- Должна поддерживаться гибкая система именования.
- Необходимо учитывать совместимость именования для других приложений (например, для электронной почты).

8.4 Планирование политики сетевой безопасности

Контроллеры домена должны проверять идентификацию пользователя или компьютера, прежде чем предоставить доступ к системным и сетевым ресурсам. Такая проверка называется аутентификацией и выполняется всякий раз при входе в сеть.

При планировании стратегии аутентификации рекомендуется соблюдать ряд правил [3]:

- Политика блокировки учетных записей (рекомендуемое значение для пользователя - 5 попыток).
- Ограничение времени, в которое разрешен вход.
- Политика истечения сроков билетов (tickets) (значение по умолчанию - 10 часов).
- Не использовать административные учетные записи для обычной работы.
- Переименовать или отключить встроенные учетные записи.

Следующий наиболее важный аспект сетевой безопасности - пароли, поэтому политику определения паролей пользователей необходимо тщательно продумать. В Windows Server 2003 по умолчанию действуют более строгие ограничения на пароли, чем в предыдущих версиях. Например, в Windows Server 2003 имеется новое средство, проверяющее сложность пароля учетной записи "Администратор" (Administrator). Если пароль пустой или недостаточно сложный, Windows предупреждает, что использовать нестойкий пароль опасно; при этом пользователь, оставивший поле для пароля пустым, не сможет обращаться к учетной записи через сеть.

Надежная политика управления паролями гарантирует, что пользователи в полной мере соблюдают принципы задания паролей, установленные компанией. При планировании политики управления паролями рекомендуется соблюдать ряд правил [3]:

- Политика сохранения последних паролей (рекомендуемое значение: 24).
- Смена пароля не чаще, чем 1 раз в сутки.
- Длина пароля не должна быть короче 7 символов.
- Использование сложной схемы для паролей (строчные, прописные буквы, цифры и другие символы).

8.5 Планирование групп

Группы упрощают предоставление разрешений пользователям. Например, назначить разрешения группе и добавить пользователей в эту группу гораздо проще, чем по отдельности назначать разрешения многочисленным пользователям и управлять этими разрешениями. Когда пользователи входят в группу, для изменения того или иного разрешения всех этих пользователей достаточно одной операции.

Как и в случае учетных записей пользователей, группы бывают локальные и уровня домена. Локальные группы хранятся в базе данных

защиты локального компьютера и предназначены для управления доступом к ресурсам этого компьютера. Группы уровня домена хранятся в Active Directory и позволяют помещать в них пользователей и управлять доступом к ресурсам домена и его контроллеров.

Типы групп [3]

- Группы безопасности:
  - используются для объединения в одну административную единицу;
  - используются ОС.
- Группы распространения:
  - используются приложениями (не ОС) для задач, не связанных с защитой.

Области действия групп [3]

- Глобальные группы:
  - содержат учетные записи пользователей и компьютеров только того домена, в котором создана эта группа;
  - им можно назначать разрешения или добавлять в локальные группы любого домена в данном лесу.
- Локальные группы домена:
  - существуют на контроллерах домена и используются для управления доступом к ресурсам локального домена;
  - могут включать пользователей и глобальные группы в пределах леса.
- Универсальные группы:
  - используются для назначения разрешений доступа к ресурсам нескольких доменов;
  - существуют вне границ доменов;
  - могут включать пользователей, глобальные группы и другие универсальные группы в пределах леса.

Active Directory позволяет вкладывать группы, то есть помещать одни группы в другие. Вложение групп - эффективный способ упорядочения пользователей. При вложении групп необходимо стремиться к тому, чтобы уровень вложения был минимальным; в сущности, лучше ограничиться одним уровнем. Чем глубже вложение, тем сложнее поддерживать структуру разрешений.

Группы пользователей помогают достичь наибольших успехов в стратегии управления учетными записями при выполнении следующих правил [3]:

- Избегать выдачи разрешений учетным записям.
- Создавать локальные группы домена.
- Для упорядочивания пользователей использовать глобальные группы.
- Помещать глобальные группы в локальные группы домена.

- Не включать пользователей в универсальные группы.

8.6 Планирование групповой политики

Групповая политика - мощное и эффективное средство, позволяющее задать параметры сразу для нескольких пользователей и компьютеров. Кроме того, *групповая политика* применяется для распространения и обновления программного обеспечения в организации.

Групповая политика определяет набор параметров конфигурации пользователей и компьютеров, который можно связать с компьютерами, сайтами, доменами и OU в Active Directory. Такой набор параметров групповой политики называется объектом групповой политики (Group Policy Object, GPO).

Любой компьютер под управлением Windows 2000, Windows XP или Windows Server 2003 (независимо от того, входит он в Active Directory или нет) содержит один локальный GPO, в котором заданы политики, применяемые к этому компьютеру. Если компьютер входит в Active Directory, к нему можно применить несколько дополнительных GPO, не являющихся локальными.

Существует два основных типа групповой политики [3]:

- **Конфигурация компьютера**. Используется для задания групповых политик, применяемых к определенным компьютерам.
- **Конфигурация пользователя**. Используется для задания групповых политик, применяемых к определенным пользователям.

Вне зависимости от типа параметров групповой политики имеется три следующие категории [3].

- **Параметры программ (Software Settings)**. Категория содержит параметры для установки программного обеспечения на клиентских компьютерах (поддерживаются ОС Windows 2000 и более новые), к которым применяется *групповая политика*. Используются два компонента:
    - **служба установки Windows**. Установка и обновление ПО в соответствии с инструкциями в установочных пакетах;
    - **установочные пакеты Windows**. Исполняемые файлы сценариев со всеми инструкциями (msi).
- **Параметры Windows (Windows Settings)**. Категория предназначена для изменения ряда параметров конфигурации, связанных со средой Windows:

    - **сценарии (Scripts)**. Настраивая конфигурацию компьютера, можно задать сценарии, которые выполняются при его включении или выключении. При настройке конфигурации для пользователя можно задать сценарии, выполняемые при входе или выходе пользователя;
    - **параметры безопасности (Security Settings)**. Это параметры безопасности, задаваемые для компьютеров и пользователей;
    - **настройка Internet Explorer (Internet Explorer Maintenance)**. Этот узел доступен только для пользователей и служит для управления работой Internet Explorer на клиентских компьютерах;
    - **службы удаленной установки (Remote Installation Services, RIS)**. RIS позволяет автоматически выполнять удаленную установку операционной системы на новые клиентские компьютеры. Эти параметры тоже доступны только для конфигураций пользователей. Они управляют удаленной установкой операционных систем;
    - **перенаправление папок (Folder Redirection)**. Эти параметры доступны только для конфигураций пользователей. Они позволяют переопределить специальные папки Windows, изменив их местонахождение по умолчанию на сетевой каталог. Благодаря этому можно централизованно управлять папками пользователей.
- **Административные шаблоны (Administrative Templates)**. Категория содержит все параметры групповой политики, хранящиеся в реестре, которые можно использовать для конфигураций компьютеров и пользователей.

8.6.1 Разрешение GPO из нескольких источников

Поскольку GPO, применяемые к пользователю или компьютеру, могут поступать из нескольких источников, нужен способ определения того, как эти GPO сочетаются друг с другом. GPO обрабатываются в следующем порядке [3]:

- **локальный GPO**. Обрабатывается локальный GPO компьютера, и применяются все параметры защиты, заданные в этом GPO;
- **GPO сайта**. Обрабатываются GPO, связанные с сайтом, к которому относится компьютер. Параметры, заданные на этом уровне, переопределяют любые параметры предыдущего уровня, с которыми они конфликтуют. Если с сайтом связано несколько GPO, администратор сайта может задать, в каком порядке обрабатываются эти GPO;
- **GPO домена**. Обрабатываются GPO, связанные с доменом, к которому относится компьютер, и применяются содержащиеся в них параметры. Параметры, заданные на уровне домена, переопределяют параметры, примененные на локальном уровне или на уровне сайта, с которыми они конфликтуют. Если с доменом связано несколько GPO, администратор, как и в предыдущем случае, может задать порядок их обработки;
- **GPO OU**. Обрабатываются GPO, которые связаны с любыми OU, содержащими пользователя или компьютер. Параметры, заданные на уровне OU, переопределяют параметры, примененные на локальном уровне или уровне домена и/или сайта, с которыми они конфликтуют. Один и тот же *объект* может входить в несколько OU. В этом случае сначала обрабатываются GPO, связанные с OU, находящейся на самом высоком уровне иерархии Active Directory, затем - с OU, находящейся на следующем уровне, и т. д. Если с одной OU связано несколько GPO, администратор, как и в предыдущих случаях, может задать порядок их обработки.

8.6.2 Наследование групповой политики

По умолчанию дочерние контейнеры наследуют групповую политику от родительских контейнеров. Однако можно переопределить унаследованные параметры, задав для дочернего объекта другие значения параметров. Кроме того, в GPO можно задать, что тот или иной параметр активен, неактивен или не определен. Параметры, которые не определены для родительского контейнера, вообще не наследуются дочерними контейнерами, а параметры, которые активны или неактивны, наследуются.

Если GPO определены и для родителя, и для потомка и если заданные в них параметры совместимы, эти параметры комбинируются. Например, если в родительской OU задана определенная длина пароля, а в дочерней OU - некая политика блокировки учетных записей, будут использоваться оба этих параметра. Если параметры несовместимы, то по умолчанию с дочерним контейнером связывается значение, переопределяющее значение параметра, который связан с родительским контейнером.

Если необходимо не применять политику к пользователю или группе, можно запретить чтение или применение этой политики для данного пользователя или группы.

В большинстве политик задействована лишь часть доступных параметров, поэтому неиспользуемые параметры конфигурации компьютера или пользователя, содержащиеся в GPO, рекомендуется отключать. Если неиспользуемые параметры включены, они все равно обрабатываются, что приводит к лишнему расходу системных ресурсов. Отключив неиспользуемые параметры, мы снизим нагрузку на клиентские компьютеры, обрабатывающие политику.

Имеется еще два дополнительных механизма, применяемых при управлении наследованием групповых политик [3]:

- **Не перекрывать (No Override)**. При связывании GPO с контейнером можно выбрать, чтобы параметры, заданные в этом GPO, не переопределялись параметрами в GPO, связанных с дочерними контейнерами. Это гарантирует, что для дочерних контейнеров будет применяться заданная политика.

- **Блокировать наследование политики (Block Policy Inheritance)**. При выборе этого параметра контейнер не наследует параметры GPO, заданные для родительского контейнера. Однако если для родительского контейнера указан параметр "Не перекрывать", дочерний контейнер не может заблокировать наследование от своего родителя.

8.6.3 Планирование структуры GPO

При реализации групповой политики сначала создаются GPO, затем эти объекты связываются с сайтами, доменами и OU. Может потребоваться применение некоторых GPO на уровне доменов или сайтов, но в большинстве случаев следует применять GPO на уровне OU [3].

8.6.4 Связывание GPO с доменом

GPO, связанный с доменом, применяется ко всем пользователям и компьютерам домена. Поскольку это мощная политика, следует свести к минимуму количество GPO этого уровня.

Типичное применение GPO уровня домена - реализация корпоративных стандартов. Например, в компании может действовать стандартное требование, состоящее в том, что ко всем компьютерам и пользователям должна применяться одна и та же политика управления паролями и аутентификацией. В этом случае применение GPO уровня домена было бы отличным решением.

8.6.5 Связывание GPO с сайтом

GPO связывают с сайтами очень редко, поскольку гораздо эффективнее связывать GPO с OU, структура которых основана на территориальном делении.

Но при определенных обстоятельствах связывание GPO с сайтом - приемлемое решение. Если параметры должны быть общими для всех компьютеров, физически находящихся в определенном месте, и для этого места создан *сайт*, есть смысл связать GPO с сайтом. Например, для

компьютеров, расположенных в некоем филиале, нужно задать определенную сетевую конфигурацию с поддержкой подключения к Интернету. В этом случае идеально подходит GPO, связанный с сайтом.

8.6.6 Связывание GPO с OU

В большинстве случаев лучше связывать GPO с хорошо продуманной структурой OU, чем с сайтами или доменами. OU обеспечивают наибольшую гибкость, поскольку позволяют спроектировать структуру, хотя бы отчасти упрощающую применение групповой политики. Кроме того, OU более гибкие в администрировании: можно без проблем перемещать пользователей и компьютеры между OU, изменять структуру OU и даже переименовывать сами OU.

8.7 Краткие итоги

9 ЛЕКЦИЯ: ПЛАНИРОВАНИЕ ТОПОЛОГИИ САЙТОВ

В данной лекции продолжено рассмотрение вопроса, как планировать службу Active Directory перед ее развертыванием. Рассмотрен процесс планирования топологии сайтов для моделирования физической структуры Active Directory

Цель лекции: Дать представление о процессе планирования топологии сайтов.

Напомним, что ***сайт*** - это группа контроллеров домена, которые существуют в одной или нескольких IP-подсетях, связанных быстрым и надежным сетевым соединением. Поскольку сайты основаны на IP-подсетях, они обычно соответствуют топологии сети, а значит соответствуют и географической структуре компании. Сайты соединяются с другими сайтами WAN-каналами.

В Active Directory структура сайта связана с физической средой и поддерживается отдельно от логической среды и структуры *домена*. Таким образом, сайты Active Directory позволяют отделить логическую организацию структуры каталогов (структуры *лесов*, *доменов* и OU) от *физической структуры* сети. Сайты представляют *физическую структуру* сети на основе Active Directory. Поскольку сайты не зависят от структуры доменов, в один *домен* может входить несколько сайтов, или, наоборот, один *сайт* может содержать несколько доменов или частей нескольких доменов.

Сайты содержат объекты только двух типов: контролеры доменов, входящие в *сайт*, и связи сайтов (site links), настраиваемые для соединения с другими сайтами.

В целом сайты служат для управления трафиком по WAN-каналам. Основная задача сайта - обеспечивать хорошее сетевое соединение.

Настройка сайтов влияет на работу ОС Windows следующим образом [4]:

- **Регистрация рабочей станции и проверка подлинности**. При входе пользователя операционная система попытается найти *контроллер домена* на сайте компьютера пользователя, чтобы обслужить запрос регистрации в системе и последующие запросы сетевой информации.

- **Репликация каталога**. Расписание и маршрут репликации каталога домена могут быть сконфигурированы для внутри- и межсайтовой репликации по отдельности. Обычно система настраивается так, чтобы межсайтовая репликация осуществлялась реже, чем внутрисайтовая.

9.1 Планирование структуры сайта

При планировании сайтов должны быть решены две следующие задачи [4]:

- **Оптимизация трафика регистрации рабочей станции**. Чтобы задать регистрацию рабочей станции только на определенных контроллерах доменов, необходимо спланировать сайты так, чтобы только эти контроллеры доменов располагались в той же подсети, что и рабочая станция.
- **Оптимизация репликации каталогов**. Поскольку каждый *контроллер домена* должен выполнять репликацию каталога с другими контроллерами своего домена, необходимо спланировать сайты так, чтобы репликация выполнялась в периоды минимальной нагрузки на сеть. Возможно, понадобится создание серверов-плацдармов (bridgehead servers), чтобы обеспечить выбор контроллера домена, используемого в качестве приемника для репликации между сайтами.

Основные этапы настройки сайта:

- Создание сайта.
- Сопоставление подсети сайту.
- Подключение сайта с использованием связей сайта.
- Выбор лицензирующего компьютера для сайта.

Основные этапы настройки репликации между сайтами:

- Создание связи сайта.
- Настройка атрибутов связей сайта - такие как стоимость связи сайта, частота репликации и возможность репликации (см. рис. 9.1).
- Создание мостов связей сайта (см. рис. 9.2).

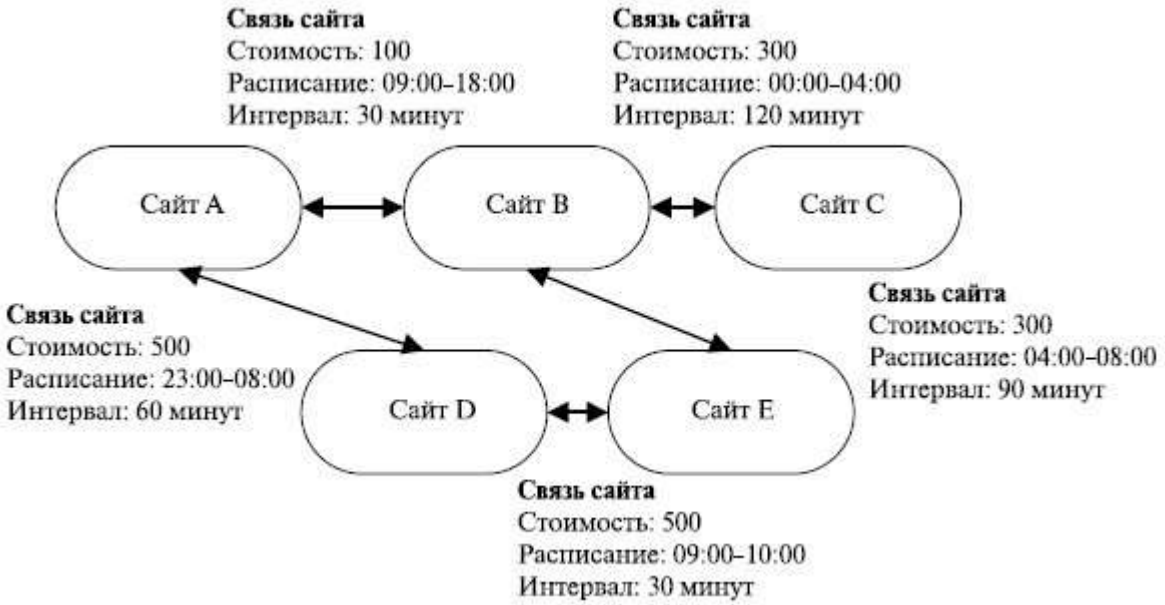


Рис. 9.1. Конфигурация связей между сайтами

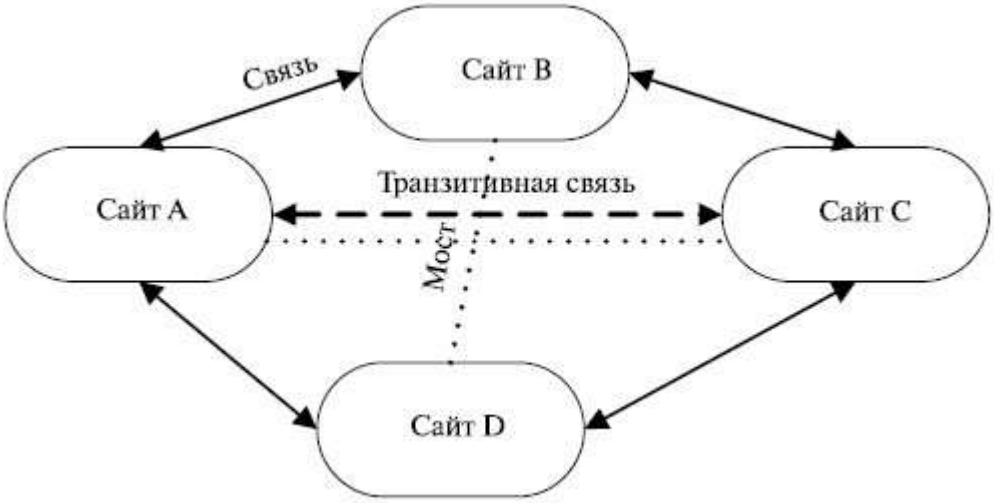


Рис. 9.2. Связи, мосты, транзитивность связей сайтов

Выбор структуры сайтов определяется следующей информацией [3].

- Информация о *физической структуре* сети:
  - территориальное местоположение филиалов;
  - структура и скорость LAN филиалов;
  - сведения о TCP/IP-подсетях филиалов;
  - скорость и стоимость WAN-соединений.
- Информация о логической архитектуре Active Directory:
  - план лесов;
  - план доменов;
  - план административной иерархии.

Основные принципы, которых рекомендуется придерживаться при планировании структуры сайтов [3]:

- создавать сайт для LAN или группы LAN;
- создавать сайт для каждого территориального участка с контроллером домена;
- создавать сайт для участков с сервером, на котором выполняется приложение, работающее с данными о сайтах.

При планировании сайта следует подумать и о том, кто будет управлять структурой сайта после его развертывания. Обычно ответственным за топологию сайтов назначают администратора (или администраторов). Он должен по мере роста и изменения физической сети вносить необходимые изменения в структуру сайтов. Ответственный за топологию сайтов выполняет следующие обязанности [3]:

- изменяет топологию сайтов в соответствии с изменениями в физической топологии сети;
- отслеживает сведения о подсетях в сети: IP-адреса, маски подсетей и местонахождения подсетей;
- наблюдает за сетевыми соединениями и задает цены связей между сайтами.

9.2 Инфраструктура топологии сети

Поскольку проектирование сайта сильно зависит от организационной инфраструктуры сети, то необходимо осуществить документирование этой инфраструктуры [13]:

- схемы топологии глобальной (WAN) и локальной сети (LAN), детализирующие сеть корпорации, в которых содержится информация о полной пропускной способности и доступной пропускной способности между всеми офисами компании;
- список всех офисов компании, в которых компьютеры связаны через высокоскоростные сетевые соединения. Определение высокоскоростного подключения меняется в зависимости от таких факторов, как количество пользователей в офисах компании, общее количество объектов в *домене* и доменов в *лесу*. Кроме того, нужно определить, какая часть из полной полосы пропускания сети доступна для репликации;
- количество пользователей, компьютеров, серверов и локальных подсетей IP для каждого офиса компании.

9.3 Создание модели сайта

Как только информация о сети компании собрана, можно приступать к проектированию сайта. Каждый *сайт* должен иметь *контроллер домена*, а большинство из них - и GC-сервер.

После определения количества сайтов для Active Directory осуществляется проектирование каждого сайта. Каждый *сайт* в Active Directory связан с одной или более подсетями IP, поэтому нужно определить, какие подсети будут включены в каждый *сайт*. Если принято решение не развертывать *контроллер домена* в каком-нибудь офисе компании, то нужно определить, к какому сайту будет принадлежать этот офис, и добавить эту подсеть IP к соответствующему сайту. В этом случае клиенты, находящиеся в удаленном офисе, соединятся с ближайшими контроллерами домена.

При проектировании структуры каждого сайта для организации можно следовать правилам, перечисленным далее [4].

1. Выяснить особенности физической среды. Изучить информацию, собранную при определении структуры *домена*, в том числе расположение сайтов, скорость обмена данными в сети, организацию и использование сетевых подключений и подсетей IP.
2. Определить физические сети, формирующие домены. Выяснить, какие из них включены в каждый *домен*.
3. Определить, какие участки сети планируется назначить сайтами. Если участку сети требуется контроль регистрации рабочих станций или репликация каталога, то этот участок необходимо сделать сайтом.
4. Определить физические соединения сайтов. Выяснить типы соединений, скорости и назначение, чтобы их удалось определить как объекты соединений сайтов. Объект межсайтовой связи (site link object) содержит план, где задано время выполнения репликации между сайтами, которые он соединяет.
5. Для каждого объекта межсайтовой связи задать расписание (график и интервал репликации) и стоимость. Для репликации применяется самая дешевая межсайтовая связь. Задать приоритет каждой связи, указав стоимость (по умолчанию - 100 единиц; чем меньше затраты, тем больше приоритет). По умолчанию репликация осуществляется каждые 3 часа. Необходимо задать время в соответствии с потребностями компании.
6. Обеспечить избыточность конфигурированием моста связей сайтов. Мост связей сайтов (site link bridge) обеспечивает отказоустойчивость репликации.
7. Если назначены серверы-плацдармы для репликации каждого сайта, то должны быть идентифицированы все разделы Active Directory, которые будут расположены в сайте, и назначен сервер-плацдарм для каждого раздела.

9.4 Проектирование размещения серверов

В проектирование сайта входит определение мест размещения серверов, необходимых для обеспечения нужных служб каталога Active Directory [13].

9.4.1 Размещение DNS-серверов

Без службы *DNS* пользователи не смогут находить контроллеры домена Active Directory, а контроллеры домена не смогут находить друг друга для репликации. *DNS* должна быть развернута в каждом офисе организации, за исключением, быть может, только очень маленьких офисов с несколькими пользователями. Служба *DNS* Windows Server 2003 обеспечивает несколько вариантов развертывания. Можно помещать DNS-серверы в офисе там, где нет контроллера домена. Например, контроллер домена нежелательно располагать в маленьком офисе с медленным сетевым подключением к центральному офису из-за большого трафика репликации, направленного на *контроллер домена*. Однако DNS-сервер в этот офис поместить можно, так как он может быть сконфигурирован так, чтобы трафик репликации был

очень мал или вообще отсутствовал. Если сконфигурировать DNS-сервер как сервер, предназначенный только для кэширования, то он будет оптимизировать поиски клиента, но не создаст трафика зонной передачи. Можно сконфигурировать DNS-сервер с сокращенными зонами для доменов Active Directory. Поскольку сокращенные зоны содержат только несколько записей, к удаленному офису будет направляться очень небольшой трафик репликации.

9.4.2 Размещение контроллеров домена

Как правило, контроллеры домена следует располагать в большинстве офисов компании, где есть значительное количество пользователей. Для этого существует по крайней мере две причины. Во-первых, в случае отказа в сети пользователи все равно смогли бы войти в сеть. Во-вторых, трафик входа клиентов в систему гарантировано не пересекается с WAN-подключениями к различным офисам. Для создания избыточности желательно поместить два контроллера домена в каждый офис. Если развертывать *контроллер домена* в данном месте компании, то необходимо создать и *сайт*, чтобы весь трафик входа в систему остался в пределах сайта.

Есть также две причины, почему можно не размещать *контроллер домена* в данном офисе компании. Если трафик репликации на *контроллер домена*, расположенный в данном месте, выше, чем трафик входа клиентов в систему, можно разработать такую конфигурацию, чтобы клиенты входили на смежный контроллер. Если данное место размещения не имеет никаких средств физической защиты серверов, возможно, не следует размещать здесь *контроллер домена*.

Когда принято решение не разворачивать *контроллер домена* в данном месте компании, существует два способа управлять регистрацией клиентов. Во-первых, можно сконфигурировать *сайт* для офиса, а затем

сконфигурировать связи сайта к одному из существующих сайтов. Во-вторых, можно добавить подсеть IP для данного офиса к существующему сайту.

Если планируется развернуть несколько доменов, то очень важно определить место размещения контроллера корневого домена леса. Он требуется всякий раз, когда пользователь обращается к ресурсу, расположенному в другом дереве домена, или когда пользователь входит в домен, расположенный в другом дереве домена, не в его собственном дереве. Из-за этого нужно размещать контроллеры корневого домена леса в любых офисах с большим количеством пользователей или там, где на контроллеры корневого домена будет направлен значительный трафик. Если сетевая топология компании включает централизованные региональные офисы, необходимо развернуть контроллер корневого домена в каждом из центральных офисов. Контроллеры корневого домена леса должно быть распределены по географическому принципу. Даже если нет важных причин помещать контроллер корневого домена в офисы, расположенные за пределами головного офиса, можно сделать это просто для обеспечения географической избыточности. Однако контроллеры корневого домена никогда не должны располагаться в офисе, где они не могут быть защищены физически.

9.4.3 Размещение серверов глобального каталога

GC-серверы нужны пользователям для входа на домены, которые работают на основном (native) функциональном уровне Windows 2000, или когда пользователи делают поиск информации каталога в Active Directory. Если домен работает на основном функциональном уровне Windows 2000, то нужно поместить GC-сервер в каждый *сайт*. В идеале все это должно быть сбалансировано трафиком репликации, который создается в результате помещения GC-сервера в каждом сайте. Общее правило состоит в том, чтобы

размещать GC-сервер в каждом сайте и несколько GC-серверов - в крупных сайтах.

Одно из улучшений Active Directory Windows Server 2003 состоит в том, что эта система поддерживает входы в систему домена без доступа к GC-серверу за счет кэширования универсального группового членства. Когда эта функция включена, контроллеры домена могут кэшировать универсальное групповое членство пользователей в домене. Когда пользователь входит на *сайт* в первый раз, универсальное членство группы пользователя должно быть найдено в GC-сервере. После первого входа в систему *контроллер домена* будет кэшировать универсальное групповое членство пользователя неопределенно долго. Кэш на контроллере домена модифицируется каждые 8 часов в результате контакта с назначенным GC-сервером.

9.4.4 Размещение серверов хозяев операций

Наиболее важным хозяином операций для ежедневной работы является *эмулятор основного контроллера домена* (PDC). Этот сервер особенно важен, если домен работает на смешанном функциональном уровне Windows 2000 или на временном функциональном уровне Windows Server 2003, потому что все резервные контроллеры домена (BDC) с системой Windows NT4 полагаются на эмулятор PDC для синхронизации каталога. Кроме того, если компания имеет много пользователей низкого уровня без установленной службы Directory Services Client (клиент услуг каталога), то эти пользователи должны подключаться к эмулятору PDC, чтобы изменить свои пароли. Даже в основном режиме эмулятор PDC получает приоритетные обновления изменений пароля пользователя, поэтому очень важно, где он расположен. Эмулятор PDC должен быть расположен в центральном офисе, где максимальное количество клиентов соединяется с сервером.

Размещение других хозяев операций не так критично. Принимая решение о том, где располагать этих хозяев, можно воспользоваться следующими рекомендациями:

- По возможности *хозяин схемы*, хозяин именования домена и хозяин относительных идентификаторов (RID) должны быть расположены в сайте, имеющем другой *контроллер домена* в качестве прямого партнера по репликации. Причина связана с восстановлением системы в случае отказа. Если один из этих серверов перестанет работать, то, возможно, придется захватить роль хозяина операций и передать ее другому контроллеру домена. Эту роль желательно передать на такой *контроллер домена*, который полностью реплицируется с первоначальным хозяином операций. С наибольшей степенью вероятности это произойдет в том случае, если два контроллера домена будут находиться в одном и том же сайте и будут сконфигурированы как прямые партнеры по репликации.
- *Хозяин RID* должен быть доступен для всех контроллеров домена через подключение по удаленному запросу процедуры (RPC). Когда контроллеру домена потребуется больше идентификаторов RID, он будет использовать RPC-подключение, чтобы запросить их у хозяина RID.
- *Хозяин инфраструктуры* не должен располагаться на GC-сервере, если в компании имеется более одного домена. Роль хозяина инфраструктуры состоит в обновлении ссылок на отображаемые имена пользователей между доменами. Например, если учетная запись пользователя переименована и пользователь является членом универсальной группы, хозяин инфраструктуры обновляет имя пользователя. Если хозяин инфраструктуры расположен на GC-сервере, он не будет функционировать, потому что GC постоянно обновляется самой современной глобальной информацией. В результате хозяин инфраструктуры не обнаружит никакой устаревшей информации и, таким образом, никогда не обновит перекрестную междоменную информацию.
- Если организация имеет центральный офис, где располагается большинство пользователей, всех хозяев операций следует помещать в *сайт* этого офиса.

9.5 Краткие итоги

10 ЛЕКЦИЯ: РЕПЛИКАЦИЯ В ACTIVE DIRECTORY

Указана модель репликации, используемая в Active Directory. Приведены типы и протоколы репликации, виды реплицируемой информации

Цель лекции: Дать представление о процессе репликации в Active Directory.

Каждая компания, реализующая проект по внедрению службы каталога Active Directory, развертывает несколько контроллеров домена. Они могут располагаться в одном центре обработки данных в главном офисе компании и связываться высокоскоростными сетевыми соединениями. Они могут быть распределены по всему миру и использовать для связи глобальные сети (WAN). Некоторые компании имеют единственный *домен* в лесу, другие компании - много доменов в нескольких доменных деревьях в общем лесу.

Независимо от того, сколько контроллеров домена имеет компания и где они расположены, контроллеры домена должны реплицировать информацию друг у друга. Если они не будут делать этого, каталоги на контроллерах станут противоречивыми. Например, если на одном контроллере домена будет создан пользователь и эта информация не скопируется на все другие контроллеры домена, то этот пользователь сможет входить только на один *контроллер домена*.

Служба Active Directory использует модель репликации с несколькими хозяевами, в которой изменения в каталоге могут быть сделаны на любом контроллере домена и скопированы на другие контроллеры.

10.1 Модель репликации Active Directory

Active Directory состоит из нескольких логических разделов. *Репликация* информации между контроллерами домена с репликами всех разделов осуществляется одинаково для всех разделов. Когда изменяется атрибут в разделе конфигурации каталога, он реплицируется так же, как и в случае изменения атрибута любого другого раздела. Единственное отличие состоит в списке контроллеров домена, которые получат копию реплицируемого

изменения. *Репликация* между контроллерами домена в одном и том же сайте обрабатывается иначе, чем между контроллерами домена различных сайтов, но основная модель не изменяется.

В отличие от модели репликации с единственным хозяином, которая используется в системе Microsoft Windows NT, Active Directory применяет модель репликации с несколькими хозяевами. В Windows NT основной *контроллер домена* (Primary Domain Controller, PDC) является единственным контроллером домена, который может принимать изменения информации *домена*. После того как изменение сделано, оно реплицируется на все резервные контроллеры домена (Backup Domain Controllers, BDC). Недостатком модели репликации с единственным хозяином является то, что она не масштабируется для большой распределенной среды. Поскольку изменения (например, пароля пользователя) могут выполняться только на контроллере PDC, это может стать узким местом, если делаются сразу тысячи изменений. Контроллер PDC находится только в одном месте компании, и любые изменения информации *домена*, расположенного в удаленном месте, должны быть сделаны на этом контроллере PDC. Другая проблема заключается в том, что контроллер PDC является единственной точкой отказа. Если он недоступен, никаких изменений информации каталога сделать нельзя до тех пор, пока он не вернется в интерактивный режим или пока другой BDC-контроллер не будет назначен на роль контроллера PDC.

В Active Directory изменения информации *домена* могут быть сделаны на любом контроллере домена, то есть каждый *контроллер домена* имеет перезаписываемую копию каталога, а контроллера PDC не существует. Как только изменение было сделано, оно копируется на все другие контроллеры домена. Такая модель репликации с несколькими хозяевами направлена на повышение надежности и масштабируемости, ведь изменения в каталоге можно делать на любом контроллере домена независимо от того, где он расположен. Поскольку все контроллеры домена обеспечивают одни и те же службы, отказ одного из них не является критичным для всей системы.

Модель репликации, используемая в Active Directory, представляет модель с нежестким согласованием, обладающую сходимостью [13]. *Репликация* не является жестко согласованной, так как контроллеры домена, содержащие реплику раздела, не всегда имеют идентичную информацию. Например, если новый пользователь создан на одном из контроллеров домена, другие контроллеры домена не получат эту информацию до следующего цикла репликации. Процесс репликации всегда сходится, то есть если система поддерживается в стационарном состоянии, без внесения новых изменений к каталогу в течение некоторого времени, то все контроллеры домена достигнут единообразного состояния и будут иметь идентичную информацию.

При репликации используется также процесс хранения и ретрансляции (store and forward). Это означает, что *контроллер домена* может получать изменение к каталогу, а затем отправлять его на другие контроллеры домена. Это выгодно в тех случаях, когда несколько контроллеров домена, находящихся в разных офисах компании, соединены медленными WAN-соединениями. Изменение к каталогу может реплицироваться с контроллера домена одного из сайтов на единственный *контроллер домена* второго сайта. *Контроллер домена*, который получает обновление, может затем переправить изменения на другие контроллеры домена во втором сайте. *Контроллер домена*, на котором были сделаны изменения каталога, не должен копировать изменения непосредственно на все контроллеры домена, как это происходит в модели репликации с единственным хозяином.

10.2Планирование стратегии репликации

Репликация Active Directory - жизненно важная операция, которую необходимо тщательно планировать. Правильно спланированная *репликация* ускоряет ответ каталога, уменьшает сетевой трафик по WAN-каналам и сокращает административные издержки.

В Windows Server 2003 используется модель репликации с несколькими хозяевами, при которой на всех контроллерах домена хранятся равноправные копии БД Active Directory. Когда создается, удаляется или переносится объект либо изменяются его атрибуты на любом контроллере домена, эти изменения реплицируются на остальные контроллеры домена.

Внутрисайтовая (между контроллерами домена одного сайта) и межсайтовая *репликация* (между контроллерами домена, относящимися к разным сайтам) выполняется по-разному [3], [4].

10.2.1 Репликация внутри сайта

В пределах сайта Active Directory автоматически создает топологию репликации между контроллерами одного *домена* с использованием кольцевой структуры. Топология определяет путь передачи обновлений каталога между контроллерами домена до тех пор, пока обновления не будут переданы на все контроллеры домена.

Кольцевая структура обеспечивает существование минимум двух путей репликации от одного контроллера домена до другого, и если один *контроллер домена* временно становится недоступен, то *репликация* на остальные контроллеры домена все равно продолжится.

При внутрисайтовой репликации трафик репликации передается в несжатом формате. Это объясняется тем, что контроллеры домена, принадлежащие одному сайту, как предполагается, связаны каналами с высокой пропускной способностью. Помимо того, что данные не сжимаются, используется механизм репликации, основанный на уведомлении об изменениях. Значит, если в данные *домена* вносятся изменения, эти изменения быстро реплицируются на все контроллеры домена.

10.2.2 Репликация между сайтами

Для обеспечения репликации между узлами нужно представить сетевые соединения в виде связей сайтов. Active Directory использует информацию о сетевых соединениях для создания объектов-соединений, что обеспечивает эффективную репликацию и отказоустойчивость.

Необходимо предоставить информацию о применяемом для репликации протоколе, стоимости связи сайтов, о времени доступности связи и о том, как часто она будет использоваться. Исходя из этого Active Directory определит, как связать сайты для репликации.

При межсайтовой репликации все данные передаются в сжатом виде. Причина в том, что трафик, вероятно, передается по более медленным WAN-каналам (см. рис. 10.1) в сравнении с соединениями локальной сети, используемыми при внутрисайтовой репликации.

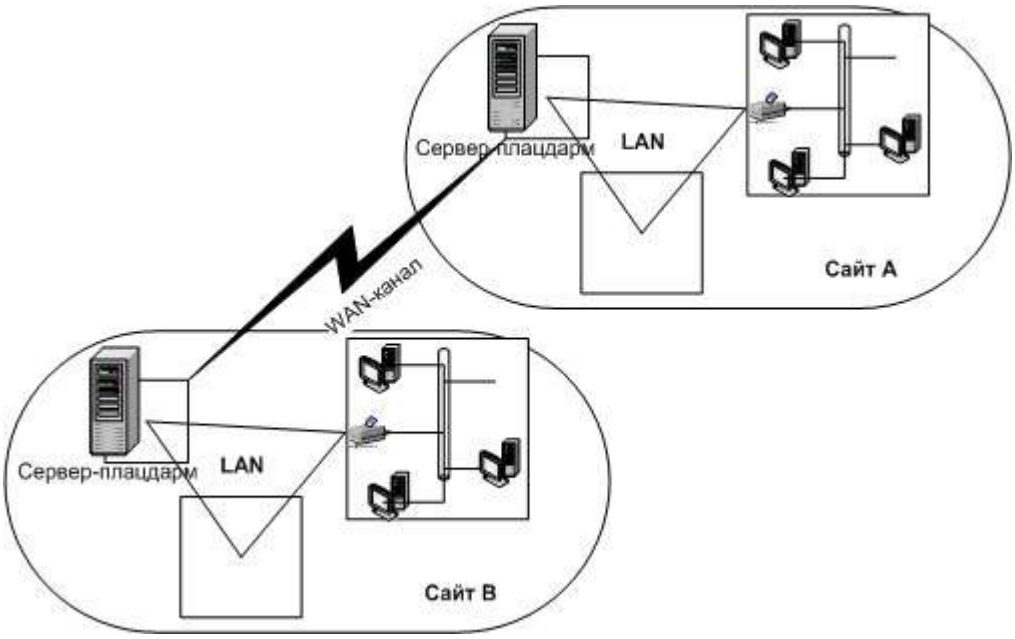


Рис. 10.1. Межсайтовая репликация

Однако при этом увеличивается нагрузка на серверы, поскольку, помимо прочих операций по обработке, им приходится упаковывать/распаковывать данные. Кроме того, *репликация* выполняется по расписанию в момент времени, лучше всего подходящий для данной организации.

10.2.3 Виды реплицируемой информации

Хранимая в каталоге информация делится на три категории, которые называются разделами каталога. Раздел каталога служит объектом репликации. В каждом каталоге содержится следующая информация [4]:

- информация о схеме - определяет, какие объекты разрешается создавать в каталоге и какие у них могут быть атрибуты;
- информация о конфигурации - описывает логическую структуру развернутой сети, например структуру *домена* или топологию репликации. Эта информация является общей для всех доменов в дереве или лесе;
- данные *домена* - описывают все объекты в *домене*. Эти данные относятся только к одному определенному *домену*, подмножество свойств всех объектов во всех доменах хранится в глобальном каталоге для поиска информации в дереве доменов или лесе.

Схема и конфигурация реплицируются на все контроллеры домена в дереве или лесе.

Все данные определенного домена реплицируются на каждый контроллер именно этого *домена*. Все объекты каждого *домена*, а также часть свойств всех объектов в лесе реплицируются в глобальный каталог.

Контроллер домена хранит и реплицирует [4]:

- информацию о схеме дерева доменов или леса;
- информацию о конфигурации всех доменов в дереве или лесе;
- все объекты и их свойства для своего домена. Эти данные реплицируются на все дополнительные контроллеры в домене, часть всех свойств объектов домена реплицируется в глобальный каталог для организации поиска информации.

Глобальный каталог хранит и реплицирует:

- информацию о схеме в лесе;
- информацию о конфигурации всех доменов в лесе;
- часть свойств всех объектов каталога в лесе (реплицируется только между серверами глобального каталога);
- все объекты каталога и все их свойства для того домена, в котором расположен глобальный каталог.

10.2.4 Протоколы репликации

Удаленные вызовы процедур выполняются при отправке сообщений репликации внутри сайта и между сайтами. Протокол RPC используется по умолчанию при всех операциях репликации Active Directory, поскольку

является отраслевым стандартом и совместим с большинством типов сетей [3].

Обмен данными из каталога производится с помощью разных сетевых протоколов, таких как IP или SMTP [4]:

- **IP-репликация**. Использует удаленный вызов процедур (Remote Procedure Call, RPC) для репликации через связи сайтов (межсайтовой) и внутри сайта (внутрисайтовой). По умолчанию межсайтовая IP-репликация выполняется по соответствующему расписанию, однако можно настроить репликацию Active Directory, чтобы игнорировать расписания. Для IP-репликации не требуется центр сертификации.
- **SMTP-репликация**. Производится только через связи сайтов (межсайтовая), но не в пределах сайта. Так как протокол SMTP асинхронный, обычно все расписания им игнорируются. Необходимо установить и настроить центр сертификации (Certification Authority, CA) компании для использования SMTP-связей сайтов. Центр сертификации подписывает сообщения SMTP, которыми обмениваются контроллеры домена для подтверждения подлинности обновлений каталога.

10.3 Процесс репликации

Репликация позволяет отражать изменения в одном контроллере домена на остальных контроллерах в домене. Информация каталога реплицируется на контроллеры домена как в пределах узлов, так и между ними. При этом с любого компьютера в дереве доменов или лесе пользователи и службы могли все время получать доступ к информации в каталоге.

Существуют два типа обновлений информации Active Directory, касающейся определенного контроллера домена [13]. Первый тип обновлений - исходное обновление (originating update). Исходное обновление выполняется при добавлении, изменении или удалении объекта на контроллере домена. Второй тип обновлений - реплицируемое обновление (replicated update). *Репликация* выполняется тогда, когда изменение, сделанное на одном контроллере домена, копируется на другой *контроллер домена*. По определению исходное обновление, касающееся любого конкретного изменения, только одно, оно выполняется на том контроллере домена, где было сделано. Затем исходное обновление копируется на все контроллеры домена, которые имеют реплику раздела Active Directory, затронутого обновлением.

Исходные обновления Active Directory происходят в следующих случаях [13]:

- к Active Directory добавлен новый объект;
- из Active Directory удален существующий объект;
- атрибуты существующего объекта Active Directory изменены. Эта модификация может включать добавление нового значения атрибуту, удаление значения атрибута или изменение существующего значения;
- объект Active Directory перемещен в новый родительский контейнер. Если изменяется имя родительского контейнера, то каждый объект контейнера перемещается в переименованный контейнер.

Все исходные обновления Active Directory являются элементарными операциями. Это означает, что в процессе передачи модификация должна быть передана полностью, как целая транзакция, и никакая ее часть не передается отдельно от других частей.

После передачи исходного обновления изменение должно реплицироваться на другие контроллеры домена, которые содержат реплику этого раздела. В пределах сайта *контроллер домена*, на котором произошло исходное обновление, ждет 15 секунд перед началом копирования изменений своим прямым партнерам по репликации. Это ожидание предназначено для того, чтобы несколько модификаций к базе данных можно было реплицировать одновременно, что увеличивает эффективность репликации. Между сайтами исходное обновление будет копироваться партнерам по репликации в соответствии с графиком, сконфигурированным на связях сайта.

Active Directory реплицирует информацию в пределах сайта чаще, чем между сайтами, сопоставляя необходимость в обновленной информации каталога с ограничениями по пропускной способности сети. Лучше выполнять репликацию в то время, когда сетевой трафик минимален, что сведет к минимуму временные задержки, связанные с репликацией данных.

Дабы убедиться, что топология репликации все еще эффективна, Active Directory периодически ее анализирует. Если добавить или убрать *контроллер домена* из сети или узла, то Active Directory изменит топологию соответствующим образом. Проверка топологии репликации заключается в

следующем. Active Directory запускает процесс, который определяет стоимость межсайтовых подключений, проверяет, доступны ли известные контроллеры домена и не были ли добавлены новые, и затем на основе полученных сведений добавляет или удаляет объекты-подключения для формирования эффективной топологии репликации. Этот процесс не затрагивает объекты-подключения, созданные вручную.

Каждый *контроллер домена* в сайте представляется объектом-сервером. У каждого объекта-сервера есть дочерний объект NTDS Settings, управляющий репликацией данных контроллера домена внутри сайта, а у каждого объекта NTDS Settings - объект-соединение, в котором хранятся атрибуты соединения и который представляет коммуникационный канал, применяемый при репликации данных с одного контроллера домена на другой. Для репликации нужно, чтобы на обеих сторонах было по объекту-соединению.

Сервис *Knowledge Consistency Checker (KCC)* автоматически создает набор объектов-соединений для репликации с одного контроллера домена на другой. Однако при необходимости можно создать объекты-соединения вручную.

КСС создает различные топологии (то есть задает местонахождение объектов-соединений и их конфигурацию) для внутрисайтовой и межсайтовой репликации. Кроме того, КСС изменяет созданные им топологии всякий раз, когда добавляются или удаляются контроллеры домена, а также при их перемещении из одного сайта в другой.

10.4Краткие итоги

11 ЛЕКЦИЯ: ВНЕДРЕНИЕ ACTIVE DIRECTORY

Описан процесс поэтапного развертывания Active Directory, включающий такие этапы, как установка и внедрение. Кратко дано представление об условиях, необходимых для установки Active Directory, и о функционировании мастера инсталляции. Приведено описание этапа тестовой эксплуатации с последующим переходом из существующей структуры промышленной среды компании в спроектированную структуру Active Directory

Цель лекции: Научиться внедрять Active Directory, сформулировать условия установки, разобрать вопросы тестирования.

После выбора стратегии развертывания Active Directory осуществляется поэтапное внедрение единой службы каталогов в соответствии с планом-графиком развертывания.

11.1 Развертывание Active Directory

При установке Active Directory выполняются следующие функции:

- **Добавление контроллера домена к существующему домену**. Создается равноправный *контроллер домена*, обеспечивающий отказоустойчивость и уменьшение нагрузки на имеющиеся контроллеры доменов.
- **Создание первого контроллера домена в новом домене**. Создается новый *домен*, необходимый для распределения информации, что позволит настроить Active Directory в соответствии с потребностями организации. При создании нового домена разрешается создать новый дочерний *домен* или новое дерево.
- **Создание нового дочернего домена**.
- **Создание нового дерева домена**.
- **Установка DNS-сервера**.
- **Создание БД и журналов БД**.
- **Создание общего системного тома**.

Причины создания нескольких доменов: распределенное администрирование сети, управление репликацией, разные требования к паролям в разных организациях, большое число *объектов*, разные имена доменов Интернета, региональные требования и требования внутренней политики.

11.2 Установка службы каталога Active Directory

Процесс установки службы каталога Active Directory на компьютере с Microsoft Windows Server 2003 несложен: простота обеспечивается за счет мастера инсталляции Active Directory (Active Directory Installation Wizard).

Два других метода установки Active Directory [13] - инсталляция без помощи мастера и установка из восстановленных резервных файлов.

11.2.1 Предварительные условия установки Active Directory

Любой сервер, который удовлетворяет условиям, описанным далее, может содержать Active Directory и стать контроллером домена. Каждый новый *контроллер домена* фактически является автономным сервером, пока не завершится процесс инсталляции Active Directory. В ходе этого процесса решаются две важные задачи [13] - создается или заполняется база данных каталога и запускается Active Directory, чтобы сервер отвечал на попытки входа в систему домена и на запросы облегченного протокола службы каталога *LDAP*.

База данных каталога хранится на жестком диске контроллера домена в файле Ntds.dit. В процессе инсталляции Windows Server 2003 файл Ntds.dit сохраняется в папке %systemroot%\system32 на локальном диске. В процессе инсталляции Active Directory файл Ntds.dit копируется в место, идентифицированное во время инсталляции, или в заданную по умолчанию папку %systemroot%\NTDS, если не определено другое место. При наличии файла Ntds.dit, скопированного на жесткий диск в процессе инсталляции Windows Server 2003, Active Directory может быть установлена в любое время без необходимости обращаться к инсталляционной среде.

Далее приводятся условия, необходимые для того, чтобы Active Directory могла работать в Windows Server 2003 [13].

- **Жесткий диск**. Размер пространства на жестком диске, необходимого для хранения службы Active Directory, будет зависеть от количества *объектов* в домене и от того, является ли данный *контроллер домена* сервером глобального каталога (GC). Для поддержки установки папки Sysvol по крайней мере один логический диск должен быть отформатирован под файловую систему NTFS v.5 (версия NTFS, которая используется в системах Microsoft Windows 2000 и Windows Server 2003).Чтобы установить Active Directory на сервер, на котором выполняется система Windows Server 2003, жесткий диск должен удовлетворять следующим минимальным требованиям:

    - 15 Мб свободного пространства - на раздел установки системы;
    - 250 Мб свободного пространства - для базы данных Active Directory (Ntds.dit);
    - 50 Мб свободного пространства - для файлов регистрационного журнала транзакций процессора наращивания памяти (ESENT). ESENT представляет собой систему взаимодействия базы данных, которая использует файлы регистрационных журналов для поддержки семантики откатов (rollback), чтобы гарантировать передачу транзакций базе данных.
- **Обеспечение сетевой связи**. После установки Windows Server 2003 и до начала установки Active Directory необходимо убедиться, что сервер должным образом сконфигурирован для обеспечения сетевой связи.
- **Служба *DNS*, необходимая Active Directory в качестве указателя ресурсов**. Клиентские компьютеры полагаются на *DNS* при поиске контроллеров домена, чтобы они могли аутентифицировать себя и пользователей, которые входят в сеть, а также делать запросы к каталогу для поиска опубликованных ресурсов. Кроме того, служба *DNS* должна поддерживать записи службы указателя ресурсов (SRV) и динамические модификации. Если служба *DNS* не была установлена предварительно, то мастер инсталляции Active Directory установит и сконфигурирует *DNS* одновременно с Active Directory. Если *DNS* уже установлена в сети, необходимо проверить ее конфигурацию, чтобы она могла поддерживать Active Directory.
- **Административные разрешения, которые должна иметь учетная запись пользователя для возможности установки Active Directory**.

11.2.2 Мастер установки

Мастер установки Active Directory выполняет следующие функции [4]:

- добавляет *контроллер домена* к существующему домену;
- создает первый *контроллер домена* в новом домене;
- создает новый дочерний *домен*;
- создает новое *дерево домена*;
- устанавливает DNS-сервер;
- создает БД и журналы БД;
- создает общий системный том;
- удаляет службы Active Directory с контроллера домена.

Когда служба Active Directory устанавливается на сервер с Windows Server 2003, компьютер фактически становится контроллером домена. Если это первый *контроллер домена* в новом домене и *лесу*, то создается чистая база данных каталога, ожидающая поступления *объектов* службы каталога. Если это дополнительный *контроллер домена* в уже существующем домене, процесс репликации размножит на этот новый *контроллер домена* все *объекты* службы каталога данного домена. Если это контроллер домена, имеющий модернизированную систему Microsoft Windows NT 4, база данных

учетных записей будет автоматически обновлена до Active Directory после того, как на этом контроллере домена будет установлен Windows Server 2003.

При установке Active Directory можно добавить новый контроллер домена к существующему домену или создать первый контроллер нового домена [4].

- **Добавление контроллера к существующему домену**. В этом случае создается равноправный *контроллер домена*. Он обеспечит отказоустойчивость и уменьшит нагрузку на имеющиеся контроллеры доменов.
- **Создание первого контроллера для нового домена**. В этом случае создается новый *домен*. Он нужен для распределения информации, что позволит настроить Active Directory в соответствии с потребностями организации. При создании нового домена разрешается создать новый дочерний *домен* или новое дерево.

При установке службы каталогов Active Directory на первом контроллере домена *сайта* в контейнере Sites создается *объект* с именем Default-First-Site-Name. В этом *сайте* необходимо установить первый *контроллер домена*. Дополнительные контроллеры располагаются в *сайте* первого контроллера домена (предполагается, что IP-адрес жестко связан с *сайтом*) или в другом существующем *сайте*. После установки первого контроллера домена имя Default-First-Site-Name можно изменить на любое другое.

Когда производится установка Active Directory на дополнительные серверы, а в хранилище определены дополнительные *сайты*, то возможны два варианта. Если IP-адрес устанавливаемого компьютера соответствует имеющейся в существующем *сайте* подсети, то контроллер добавляется в этот *сайт*. Иначе контроллер добавляется в *сайт* исходного контроллера домена.

11.2.3 Конфигурирование DNS для Active Directory

Active Directory использует *DNS* в качестве службы поиска, позволяя компьютерам находить контроллеры доменов. Для поиска контроллера в определенном домене клиент запрашивает *DNS* о записях ресурсов, содержащих имена и IP-адреса LDAP-серверов домена. ***LDAP*** - это протокол, используемый для осуществления запросов и обновления Active Directory и

выполняющийся на всех контроллерах домена. Нельзя установить Active Directory, не имея на компьютере службы *DNS*, потому что Active Directory использует *DNS* в качестве службы поиска. Однако можно установить *DNS* без установки Active Directory.

Для автоматического конфигурирования DNS-сервера надо воспользоваться мастером установки Active Directory: не придется вручную настраивать *DNS* для поддержки Active Directory, но это не касается тех случаев, когда планируется использовать DNS-сервер без Windows 2000/2003 или требуется создать особую конфигурацию. Чтобы задать конфигурацию, отличную от задаваемой мастером установки по умолчанию, можно вручную сконфигурировать *DNS*, воспользовавшись консолью *DNS*.

11.2.4 База данных и общий системный том

При установке Active Directory создается БД и ее журнал, а также общий системный том [4].

- БД и ее журнал - это каталог для нового домена. По умолчанию БД и ее журнал располагаются в каталоге %systemroot%\NTDS, где %systemroot% - это каталог Windows. Для повышения производительности рекомендуется размещать БД и журнал на разных жестких дисках.
- Общий системный том - это структура папки, существующая на всех контроллерах доменов Windows. Он хранит сценарии и некоторые объекты групповой политики для текущего домена и предприятия. По умолчанию общий системный том располагается в каталоге %systemroot%\SYSVOL. Общий системный том должен располагаться в разделе или томе, отформатированном под NTFS 5.0.

Репликация общего системного тома идет по тому же расписанию, что и *репликация* Active Directory, поэтому можно не заметить репликацию файлов вновь созданного общего системного тома, пока не пройдет два цикла репликации (обычно это занимает минут 10). Дело в том, что первый цикл репликации файла обновляет конфигурацию других системных томов, уведомляя их о добавлении нового системного тома.

11.2.5 Режимы домена

Существуют два режима домена - смешанный и основной [4].

- **Смешанный режим**. При первой установке или обновлении контроллера домена до Windows 2000 Server контроллер запускается в смешанном режиме (mixed mode), что позволяет ему взаимодействовать с любыми контроллерами доменов под управлением предыдущих версий Windows NT.
- **Основной режим**. Если на всех контроллерах домена установлен Windows 2000 Server и не планируется больше добавлять в этот *домен* контроллеры нижнего уровня, то рекомендуется перевести *домен* в основной режим (native mode).

При изменении режима со смешанного на основной происходит следующее:

- прекращается поддержка репликации нижнего уровня, после чего в этом домене запрещается иметь контроллеры, не работающие под управлением Windows 2000/2003 Server;
- запрещается добавление новых контроллеров нижнего уровня в данный *домен*;
- сервер, исполнявший роль основного контроллера домена, перестает быть таковым, поэтому все контроллеры становятся равноправными.

Изменение режима домена возможно лишь в одном направлении - из смешанного в основной режим, но не наоборот.

11.3Тестирование Active Directory

Согласно плану проведения развертывания, все решения должны предварительно тестироваться на стенде, развернутом на оборудовании в тестовой среде. В тестовой среде компании создается модель, идентичная модели промышленной среды либо ее фрагментам.

На тестовом стенде, который надлежащим образом сконфигурирован в зависимости от перечня необходимых для тестирования приложений, производятся предварительные работы по отладке работы данных приложений, связанных с Active Directory, а также тестовая миграция данных и проверка корректности ее проведения.

Тестирование проводится в соответствии с процедурами и сценариями тестирования (осуществляется функциональное и нагрузочное тестирование); одной из его целей является проверка отказоустойчивости решения с высоким показателем надежности.

Тестирование миграции доменов обычно начинается с работ по созданию односайтовой модели *леса* Active Directory, состоящей из корневого домена и разноуровневых дочерних доменов. Затем планируется реализовать поэтапную миграцию данных с созданных доменов, добавляя в них тестовые рабочие станции Windows, чтобы иметь возможность проверить вход пользователей и выполнение сценариев входа в новые домены.

На следующем этапе создания стенда необходимо протестировать:

- распределение ролей между серверами;
- работу сервиса *DNS*, установленного на серверах;
- прохождение репликации между контроллерами доменов;
- настройку соединения между контроллерами доменов;
- добавление контроллера домена в Internet VLAN;
- перенос баз WINS, DHCP;
- аутентификацию пользователей на контроллере.

После этого необходимо выполнить следующую последовательность действий:

- Установить в Internet VLAN standalone-сервер (сервер не должен быть установлен как *контроллер домена* или member-сервер), принадлежащий рабочей группе.
- Настроить на standalone-сервере обмен данными по протоколу IPSec в туннельном режиме с остальными контроллерами доменов.
- Добавить standalone-сервер в *домен* в качестве member-сервера, указать в свойствах TCP/IP адрес DNS-сервера.
- Установить на сервер сервисы DHCP, WINS и перенести на него копированием базы, затем преобразовать их в формат Windows.
- Обновить member-сервер Windows до статуса контроллера домена.
- Авторизовать сервер DHCP в Active Directory.
- Провести синхронизацию между standalone-сервером и контроллерами домена.
- На контроллере домена установить DNS-сервис. В свойствах TCP/IP этого сервера указать адрес DNS-сервера, равный собственному адресу сервера.
- Назначить функцию глобального каталога для standalone-сервера.
- Проверить прохождение репликации между контроллерами домена.
- Запустить тест проверки функционирования контроллеров домена.
- Проверить вход пользователей в сеть и выполнение сценариев входа.
- Создать имидж первого раздела контроллера домена и сохранить его на втором разделе.

Тестирование реструктуризации домена - протестировать перенос учетных записей пользователей и компьютеров из существующего домена в новый *домен* с помощью утилиты ADMT [4].

- Настроить двухсторонние доверительные отношения между доменами.
- Включить аудит успешных и неуспешных событий по управлению пользователями и группами в обоих доменах.

- Перенести пользователей и группы из существующего домена в новый *домен*.
- Проверить вход пользователей в *домен*.
- Удалить доверительные отношения между новым доменом и существующим доменом.

Тестирование переноса баз DHCP, WINS - протестировать корректность переноса баз в процессе миграции.

- Установить на сервере сервисы DHCP, WINS и перенести на него копированием базы с существующих серверов, затем преобразовать их в формат Windows.
- Авторизовать сервер DHCP в Active Directory.

Тестирование многосайтовой конфигурации физической топологии Active Directory - создать дополнительный *сайт* для удаленной площадки, установить *контроллер домена* в этот *сайт* и проверить следующие характеристики:

- Время репликации между контроллерами домена, расположенными в центральном офисе и на удаленной площадке.
- Аутентификация пользователей.
- Время прохождения репликации для "мгновенных событий" (изменение пароля).

После завершения тестовой эксплуатации (осуществляется деинсталляция установленного стенда), на основании выработанных документов о миграции, осуществляется перенос данных (приложений, пользователей, компьютеров) из существующей структуры промышленной среды компании в спроектированную структуру Active Directory.

11.4Краткие итоги

12 ЛЕКЦИЯ: МИГРАЦИЯ ДАННЫХ

Приведено краткое описание процесса миграции данных при внедрении службы Active Directory, осуществляемого в единую структуру службы каталогов Active Directory. Сформулированы задачи, которые необходимо выполнить при миграции, даны варианты модернизации и критерии их выбора. Указаны вероятные проблемы при проведении миграции данных, их причины и возможные способы устранения

Цель лекции: Дать представление о процессе миграции при развертывании Active Directory

Для возможности функционирования в компании различных приложений, используемых в бизнес-процессах до внедрения службы Active Directory, необходимо осуществить корректный перенос этих приложений и их настроек в новую спроектированную структуру. Реализация указанной задачи осуществляется путем разработки плана миграции существующей доменной структуры компании на доменную структуру Active Directory - определения порядка модернизации доменов.

- Определение *домена*, который должен быть модернизирован первым.
- Определение последовательности модернизации доменов *учетных записей*.
- Определение последовательности модернизации ресурсных доменов.
- Определение момента переключения для каждого *домена* из смешанного режима (Mixed mode) в основной режим (Native mode) Windows.
- Тестирование имеющихся критичных приложений в окружении Active Directory в смешанном режиме работы контроллеров доменов.

В процессе миграции данных обеспечивается непрерывность работы пользователей и минимальное время простоя информационных систем компании.

12.1 Общие положения модернизации доменной инфраструктуры

При модернизации доменной инфраструктуры осуществляется миграция данных: перенос в единую службу каталога информационных систем и приложений, работа которых тесно связана с Active Directory. При этом возможна миграция с существующей структуры DNS/WINS, с интеграцией новой и существующей структуры DNS/WINS на этапе миграции.

При проведении миграции необходимо выполнить следующие задачи [4]:

- перевести существующие домены ресурсов в организационные единицы новых доменов, что позволит упростить управление сетевыми ресурсами;
- "имитировать" ход миграции, при этом реального переноса данных не происходит;
- отменить сделанные действия, связанные с миграцией;
- переместить *учетные записи* служб;
- восстановить доверительные отношения между исходным и целевым доменами;
- преобразовать множество доменов в один или несколько крупных доменов в уже созданной среде Active Directory;
- реструктуризировать существующие группы или объединить несколько групп в одну в целевом *домене*;
- провести анализ процесса переноса данных с помощью журнализации миграционных событий.

Миграция пользователей и рабочих станций в единую структуру Active Directory реализуется с сохранением существующих прав доступа.

12.1.1 Варианты модернизации

Существует два основных варианта модернизации доменной инфраструктуры [4]:

- Обновление доменов. Данный способ является наиболее распространенным и простым для реализации при миграции доменов. Этот способ позволяет сохранить текущую структуру доменов, настройки системы, структуру пользователей и групп. Обновление *домена* (in-place обновление) включает перевод контроллеров существующего *домена* в создаваемый *домен*.
- Реструктуризация доменов. Данный способ позволяет изменить существующую структуру доменов, объединить домены или преобразовать домены в организационные подразделения.

Помимо указанных выше вариантов, существует также смешанный вариант, основанный на них, - обновление доменов с их последующей реструктуризацией [13].

Эти варианты называются *путями перехода при внедрении Active Directory*. Выбранный из них путь перехода будет являться главным звеном в общей стратегии обновления доменной инфраструктуры. Эта стратегия будет включать описание того, какие объекты службы каталога и в каком порядке необходимо переместить. Наилучший способ любого перемещения

приложений при внедрении Active Directory состоит в документировании каждой детали в рабочий документ, называемый планом перехода.

12.1.2 Критерии выбора пути перехода

При выборе пути перехода подразумевается, что это решение касается только одного *домена*, то есть совершенно справедливо использовать различные пути перехода для различных доменов в пределах одной организации.

Рассмотрим основные критерии, которые используются при выборе наиболее подходящего пути перехода [13], приведенные в таблицах 12.1, 12.2, 12.3, 12.4, 12.5, 12.6.

- Критерий 1. Удовлетворенность имеющейся моделью существующего *домена*.

Таблица 12.1. Выбор пути перехода по критерию 1

Путь перехода	Соответствие критерию
Обновление домена	Если нет никаких существенных изменений, которые хотелось бы сделать в доменной модели, то обновление домена обеспечит самый легкий путь. Имя домена останется тем же самым, так же как и существование всех *учетных записей* пользователей и групп
Реструктуризация домена	Если имеющаяся доменная модель больше не удовлетворяет организационным потребностям либо больше не является наиболее оптимальной для подразделений организации, то наилучшим выбором будет реструктуризация домена

- Критерий 2. Степень риска при переходе к новой модели домена.

Таблица 12.2. Выбор пути перехода по критерию 2

Путь перехода	Соответствие критерию
Обновление домена	Обновление домена представляет собой метод с минимальным риском. Процесс модернизации контроллера

	домена выполняется автоматически, следовательно, без взаимодействия с пользователем возможностей для ошибок возникает немного. Методология восстановления после сбоя при обновлении домена также относительно проста: если обновление прошло неудачно, необходимо выключить основной контроллер домена (PDC), назначить любой резервный контроллер домена (BDC), имеющий свежие данные, на роль PDC, и начать процедуру снова
Реструктуризация домена	Реструктуризация домена представляет собой путь с более высоким риском, чем обновление домена. Надо выполнить большее количество задач, и поэтому многие процессы могут идти не так как надо. В результате растет недовольство пользователей, которые не могут войти в систему, обратиться к необходимым ресурсам или получить доступ к своим почтовым ящикам

- Критерий 3. Время выполнения перехода

(График времени перехода не является решающим фактором при выборе пути перехода, тем не менее он может быть определяющим для небольших организаций с ограниченными ресурсами).

Таблица 12.3. Выбор пути перехода по критерию 3

Путь перехода	Соответствие критерию
Обновление домена	Обновление домена - это линейный процесс: если он был начат, то должен быть закончен. Для него требуется меньше действий, чем для реструктуризации, и, соответственно, меньше времени требуется для выполнения всего перехода
Реструктуризация домена	Реструктуризация домена всегда длится дольше. Например, при реструктуризации тратится много времени на создание и проверку инфраструктуры целевого домена, на перемещение всех *учетных записей* с исходного домена на целевой домен. Крупные организации, возможно, не смогут переместить все объекты за один раз, так что достаточно часто реструктуризация домена производится в несколько этапов

- Критерий 4. Рабочее время службы каталога, которое необходимо затратить на процесс перехода.

Таблица 12.4. Выбор пути перехода по критерию 4	
Путь перехода	**Соответствие критерию**
Обновление домена	Объекты учетных записей недоступны в процессе перехода, потому что они самостоятельно модернизируются при обновлении домена
Реструктуризация домена	Хороший выбор для организаций, в которых рабочее время системы является критической величиной. Так как она включает создание незаполненного, "чистого" леса и оставляет исходную среду по существу без изменений, то работоспособность службы каталога сохраняется, поскольку пользователи продолжают функционировать в существующей среде. Можно переносить большие или маленькие партии пользователей в течение непиковых часов работы и оставлять эти новые *учетные записи* бездействующими до того времени, как появится готовность покинуть старую систему

- Критерий 5. Наличие ресурсов для выполнения перехода.

Таблица 12.5. Выбор пути перехода по критерию 5	
Путь перехода	**Соответствие критерию**
Обновление домена	Поскольку обновление домена является автоматизированной операцией, то на реализацию этого пути перехода потребуется меньшее количество людских ресурсов
Реструктуризация домена	Реструктуризация домена влечет за собой большее количество задач, чем обновление домена, и поэтому требуется большее количество ресурсов, то есть необходимо, чтобы штат сотрудников был адекватно укомплектован для выполнения дополнительной рабочей нагрузки, связанной с реструктуризацией домена. В качестве альтернативы можно переложить часть задач или весь проект на внешних сотрудников: существует множество консультативных групп, которые специализируются на таких проектах, что позволит сэкономить время и деньги, необходимые для обучения внутренних сотрудников

- Критерий 6. Бюджет проекта перехода.

Таблица 12.6. Выбор пути перехода по критерию 5	
Путь перехода	**Соответствие критерию**
Обновление домена	Факторы, способствующие уменьшению необходимых бюджетных средств: ○ возможность использовать существующие серверные аппаратные средства; ○ более низкие затраты на людские ресурсы; ○ уменьшение расходов на тестирование, поскольку нужно будет тестировать меньшее количество задач модернизации
Реструктуризация домена	По многим причинам реструктуризация домена потребует большего бюджета, чем обновление домена. Аппаратные требования, необходимые для построения незаполненной среды леса, в которую необходимо переносить объекты службы каталога, следует рассмотреть с точки зрения бюджетных затрат

Если компания не совсем удовлетворяет условиям, позволяющим уверенно выбрать обновление или реструктуризацию *домена* в качестве пути обновления, или если для нее подходят оба пути, то можно выбрать третий путь - обновление *домена* с последующей реструктуризацией.

Данный путь перехода к Active Directory позволит получить немедленную выгоду (делегирование администрирования, *групповые политики*, публикация приложений и многое другое), а также долговременную выгоду от реструктуризации *домена* (меньшее количество доменов с увеличенным объемом домена, проект домена в соответствии с деловыми и организационными целями компании).

12.2Переход к Active Directory

Подготовка перехода к Active Directory происходит в три этапа [13]:

1. Планирование перехода.
2. Испытание плана перехода.
3. Проведение экспериментального перехода.

Кроме того, рекомендуется запланировать время на этап обслуживания и поддержки, который следует за переходом к Active Directory.

12.2.1 Планирование модернизации

Первый шаг в планировании модернизации Active Directory состоит в документировании существующего каталога и платформы сетевых служб, описание которых необходимо включить в план [13]:

- **Текущая доменная структура**. Эта информация будет необходима для возможности отката перехода. Наилучшая практика состоит в документировании следующей информации о текущем каталоге, сетевых службах и среде, в которой они выполняются:
    - все домены организации (домены ресурсов и учетных записей);
    - все доверительные отношения между доменами (включая тип и направление доверительных отношений);
    - все *учетные записи* пользователей, глобальных и локальных групп, а также учетные записи компьютеров;
    - все *учетные записи* служб и другие *учетные записи*, которые необходимы для запуска сетевых служб или приложений;
    - все системные политики и политики безопасности, которые внедрены в организации.
- **Текущие сетевые службы**. Необходимо задокументировать следующие службы, использующиеся в организации, включая сервер, на котором они выполняются:
    - серверы *DNS*;
    - серверы протокола динамической конфигурации хоста (DHCP), а также параметры настройки области действия (scope);
    - серверы службы имен Интернета для Windows (WINS);
    - серверы службы удаленного доступа (RAS);
    - файловые серверы и серверы печати.
- Аппаратные средства сервера и конфигурации программного обеспечения. Важно также задокументировать аппаратные средства и программную конфигурацию каждого сервера для гарантии того, что все приложения и службы будут учтены в новой среде. Для контроллеров домена и серверов - членов домена этот список должен включать следующую информацию:
    - количество процессоров и их скорость;
    - оперативная память;
    - системы хранения информации;
    - сетевая операционная система, выполняющаяся на каждом сервере;
    - операционная система, выполняющаяся на рабочих станциях;
    - все приложения, связанные с бизнесом, выполняющиеся на контроллере домена.

Как только текущая среда будет описана, необходимо принять решение о том, как и когда модернизировать Active Directory, то есть создать сценарий (план) модернизации - пошаговый список задач и порядок их выполнения.

В плане модернизации рекомендуется иметь следующие составляющие [13]:

- порядок модернизации;
- действия, которые необходимо предпринять для того, чтобы гарантировать продолжение работы сетевых служб в процессе обновления;
- действия по проверке правильности выполнения;
- пользователи, группы, компьютеры и *учетные записи* служб, которые необходимо переносить;
- исходные и целевые домены;
- время для выполнения процесса модернизации;
- действия, необходимые для переключения пользователей на новую среду;
- шаги по проверке правильности перехода;

В плане модернизации рекомендуется определить не только то, что необходимо делать для проверки правильности шагов, выполняемых в процессе перехода, но и то, что необходимо сделать для восстановления *домена* до последнего работоспособного состояния.

Таким образом, будет создан план восстановления системы, который необходим для реализации возможности поддерживать доступ пользователей к ресурсам, для поиска ошибок в плане модернизации и возможности попробовать все снова. План восстановления системы в случае сбоя эквивалентен плану модернизации, но он используется тогда, когда действия по проверке правильности модернизации окончились неудачей.

12.2.2 Тестирование плана модернизации

Есть несколько серьезных оснований для тестирования плана модернизации [13].

- Тестирование подтвердит, что действия по обновлению приведут к желаемым результатам.
- Тестирование даст возможность определить время, необходимое для полного завершения модернизации.
- Тестирование даст возможность ознакомиться с инструментальными средствами и процедурами, которые будут использованы при переходе к Active Directory.

Необходимо проверить все элементы перехода, рассмотрев план модернизации, и создать набор тестов для всех процедур, которые надо выполнить, а также протестировать план восстановления на предмет

обнаружения ошибки в нем. Если тестирование показывает ошибки, то необходимо модифицировать и проверять сценарии до тех пор, пока они не будут работать так, как планировалось.

При тестировании сценариев перехода рекомендуется создать испытательную среду, похожую на производственную среду компании, но полностью изолированную от нее.

12.2.3 Проведение экспериментальной модернизации

Прежде чем развертывать модернизацию по всей организации, нужно провести экспериментальный переход с ограниченной и управляемой группой пользователей. Это даст возможность тщательно проанализировать результаты перехода в управляемой среде перед выполнением полного плана модернизации. Экспериментальная модернизация имеет несколько преимуществ [13].

- Тестирует план перехода в производственной среде.
- Позволяет обнаружить непредвиденные ошибки в плане модернизации.
- Дает возможность ознакомиться с инструментальными средствами модернизации.

Благодаря экспериментальной модернизации можно оценить результаты плана перехода и внести необходимые изменения, которые нужно повторно проверить и развернуть их в экспериментальной группе перед развертыванием модернизации во всей организации.

12.3 Резервное копирование данных

Миграцию данных при переходе к Active Directory необходимо сопровождать их *резервным копированием*, при этом надо учитывать, что централизованное хранение данных упрощает этот процесс. *Резервное копирование* предназначено для сохранения данных и, в случае неудачной попытки миграции, их повторного использования для совершения перехода к Active Directory.

Важная часть *резервного копирования* Active Directory - выполнение подготовительных операций. Например, следует проверить, закрыты ли файлы, которые планируется архивировать. Сеансы приложений, запущенных системами или пользователями, известить которых не представляется возможным (например, пользователь подключился через Интернет), будут завершены, Windows Backup не архивирует файлы, заблокированные приложениями.

При использовании съемных носителей необходимо убедиться в следующем [4]:

- устройство *резервного копирования* подсоединено к компьютеру сети и включено;
- соответствующее устройство перечислено в списке совместимых с Windows устройств (Hardware Compatibility List, HCL).

12.4 Типовые проблемы при проведении миграции

При проведении миграции данных в единую структуру службы каталогов Active Directory могут возникать следующие проблемы:

- Неэффективная репликация вызывает падение производительности службы Active Directory, например, могут не распознаваться новые пользователи.
- Из-за полной синхронизации всех данных в *домене* расширение схемы может влиять на большие сети в связи с возникновением больших временных задержек. Чтобы свести к минимуму временные задержки, связанные с репликацией данных, лучше выполнять репликацию в ночное время.
- Проблемы с репликацией данных:
  - репликация информации каталога прекратилась;
  - замедление репликации данных.
- В большинстве случаев в результате неэффективной обработки запросов информация каталога устаревает, а контроллеры домена становятся недоступными.
- Сохранение имеющихся почтовых сообщений при миграции почтовых ящиков пользователей из UNIX-системы в Exchange Server.
- Автоматизация прописывания путей к перемещаемым профилям после миграции пользователей - для решения создается специализированный сценарий (VBScript).
- Увеличение базы данных каталога по мере расширения организации без ограничений по производительности сервера или по местонахождению в сети - каталог разделяется на распределенные разделы.

12.5 Краткие итоги

13 ЛЕКЦИЯ: МОНИТОРИНГ ACTIVE DIRECTORY

В этой лекции обсуждается, что такое мониторинг Active Directory, почему его следует проводить, как это делать и какие именно параметры функционирования службы необходимо отслеживать. Рассматриваются некоторые инструменты для целей мониторинга Active Directory, доступные в системе Microsoft Windows Server 2003

Цель лекции: Осветить процесс мониторинга Active Directory.

Служба Active Directory представляет собой сложную распределенную сетевую службу. В больших организациях она будет подвержена тысячам изменений каждый день (создание или удаление учетных записей пользователя и их атрибутов, группового членства и разрешений). Для гарантии того, что эти изменения в сети и рабочей среде не будут отрицательно влиять на работу Active Directory, нужно ежедневно предпринимать профилактические действия - мониторинг состояния службы каталога, который необходим для поддержания надежности Active Directory.

Отдельного инструмента или пакета программ, предназначенного для мониторинга Active Directory, не существует, поэтому мониторинг службы каталога является комбинацией задач, имеющих общую цель [4], [13] - измерение текущей характеристики некоторого ключевого индикатора (занимаемый объем диска, степень использования процессора, период работоспособного состояния службы и т. д.) по сравнению с известным состоянием (отправная точка) (Существуют наборы инструментов, которые могут соединить мониторинг этих ключевых индикаторов в один легко управляемый интерфейс, и для больших организаций наличие таких средств очень существенно, но они дороги, сложны и требуют много ресурсов.).

13.1 Причины проведения мониторинга, реализуемые преимущества и сопутствующие затраты

Основная причина проведения мониторинга Active Directory (как и мониторинга любой другой службы) состоит в том, что он идентифицирует потенциальные проблемы прежде, чем они проявятся и закончатся

длительными периодами простоя службы. Необходимо следить за состоянием Active Directory, чтобы разрешать возникающие проблемы как можно скорее, до того как произойдет прерывание работы службы.

Мониторинг дает возможность поддерживать соглашение об уровне сервиса (Service-Level Agreement, SLA) с пользователем сети. В контексте Active Directory соглашение SLA между ИТ-отделом и сообществом пользователей может содержать такие параметры, как максимально приемлемый уровень времени простоя системы, время входа в систему и время получения ответа на справочный запрос.

Еще одна причина для проведения мониторинга Active Directory состоит в том, что необходимо отслеживать следующие изменения инфраструктуры (Возможно, эта информация не поможет предотвратить возникновение сегодняшней ошибки, но она позволит получить ценные данные, с которыми можно строить планы по дальнейшему развитию инфраструктуры компании.) [13]:

- увеличение размера базы данных Active Directory;
- функционирование серверов глобального каталога (GC) в интерактивном режиме;
- время репликации между географически разнесенными *контроллерами доменов*.

Преимущества, которые можно получать от проведения мониторинга Active Directory, включают следующие компоненты [13]:

- способность поддерживать SLA-соглашение с пользователями, избегая простоя службы;
- достижение высокой производительности службы путем устранения "узких мест" в работе, которые иначе нельзя обнаружить;
- снижение административных затрат с помощью профилактических мер в обслуживании системы;
- повышенная компетентность при масштабировании и планировании будущих изменений инфраструктуры в результате глубокого знания компонентов службы, их функциональных возможностей и текущего уровня использования;
- увеличение доброжелательности в отношении ИТ-отдела в результате удовлетворения клиентов.

При всех указанных преимуществах мониторинг Active Directory связан с затратами, которые необходимы для его эффективной реализации [13]

- Для проектирования, развертывания и управления системой мониторинга нужны соответствующие людские ресурсы (человеко-часы), требующие оплаты.
- На приобретение необходимых средств управления, на обучение и на аппаратные средства, которые предназначены для реализации мониторинга, требуются определенные фонды.
- Часть пропускной способности сети будет задействована для мониторинга Active Directory на всех *контроллерах домена* предприятия.
- Для выполнения приложений-агентов на целевых серверах и на компьютере, являющемся центральным пультом мониторинга, используются память и ресурсы процессора.

Стоит отметить, что стоимость мониторинга быстро повышается при внедрении глобального мониторинга предприятия типа комплекса Microsoft Operations Manager (MOM 2005 или его современный аналог - MSCOM 2007). Инструментальные средства MOM хотя и расширяют возможности мониторинга, но достаточно дороги, требуют обучения оператора и расходуют большее количество системных ресурсов в отличие от мониторинговых решений Windows Server 2003, которые являются проверенными, интегрированными и поддерживаемыми продуктами, но с базовыми возможностями мониторинга.

Уровень мониторинга будет зависеть от результатов анализа преимуществ и затрат. В любом случае, стоимость ресурсов, которые будут потрачены на систему мониторинга, не должна превышать ожидаемую от мониторинга экономию. По этой причине большие организации находят более рентабельным вкладывать капитал в комплексные решения по управлению предприятием. Для менее крупных организаций более оправдано использовать инструментальные средства мониторинга, встроенные в систему Windows Server 2003.

13.2Процесс мониторинга Active Directory

Осуществляя мониторинг Active Directory, необходимо отслеживать ключевые индикаторы производительности и сравнивать их с базовыми показателями, которые представляют работу службы в пределах нормальных параметров. Когда индикатор работоспособности превышает указанный порог, выдается предупреждение, уведомляющее администрацию сети (или оператора мониторинга) о текущем состоянии системы. Предупреждение

может также инициировать автоматические действия, направленные на решение проблемы или уменьшение дальнейшего ухудшения состояния службы.

Ниже приводится схема процесса мониторинга службы Active Directory высокого уровня [13].

1. Определить, какой из индикаторов функционирования службы необходимо отслеживать.
2. Выполнить мониторинг индикаторов функционирования службы, чтобы установить и задокументировать базовый (нормальный) уровень.
3. Определить пороги для этих индикаторов функционирования, то есть указать, при каком уровне индикатора необходимо принимать меры, предотвращающие расстройство функционирования службы.
4. Спроектировать необходимую аварийную систему, предназначенную для обработки событий при достижении порогового уровня. Аварийная система должна включать в себя следующие компоненты:
    - уведомления оператора;
    - автоматические действия, если они возможны;
    - действия, инициируемые оператором.
5. Спроектировать систему создания отчета, фиксирующую историю состояния Active Directory.
6. Реализовать решение, которое будет измерять выбранные ключевые индикаторы в соответствии с расписанием, отражающим изменения данных индикаторов и их воздействие на состояние Active Directory.

13.3Элементы мониторинга

Для мониторинга состояния Active Directory нужно отслеживать работу, связанную со службой, и индикаторы функционирования, связанные с сервером, а также события. Цель мониторинга - гарантировать, что Active Directory и *контроллеры домена*, на которых она выполняется, работают в оптимальном режиме.

При проектировании мониторинга рекомендуется планировать наблюдение за следующими элементами (областями работы) [5], [13]:

- **Производительность служб Active Directory**. Эти индикаторы функционирования отслеживаются с помощью счетчиков NTDS в инструменте администрирования Performance.
- **Репликация Active Directory**. Функционирование репликации существенно для обеспечения сохранности данных в пределах *домена*.
- **Функционирование службы DNS и состояние DNS-сервера**. Поскольку Active Directory полагается на *DNS* при поиске ресурсов в сети, то сервер *DNS* и сама служба должны работать в нормальном режиме, чтобы Active Directory удовлетворяла заданному уровню качества обслуживания.
- **Хранилище Active Directory**. Дисковые тома, которые содержат файл базы данных Active Directory Ntds.dit и файлы журналов .log, должны иметь достаточно свободного пространства, чтобы допускать нормальный рост и

функционирование. Кроме того, если мониторинг функционирования службы показывает, что диск, на котором расположена база данных Active Directory, фрагментирован, необходимо его дефрагментировать.

- **Служба репликации файлов (File Replication Service, FRS)**. Служба FRS должна работать в пределах нормы, чтобы гарантировать, что общий системный том (Sysvol) реплицируется по всему *домену*.
- **"Здоровье" системы** *контроллера домена*. Мониторинг этой области должен охватывать все аспекты состояния сервера, включая счетчики, характеризующие использование памяти, процессора и разбиение на страницы.
- **"Здоровье"** *леса*. Эта область должна отслеживаться для того, чтобы проверить доверительные отношения и доступность *сайта*.
- **Хозяева операций**. Необходимо отслеживать каждого *хозяина операций*, чтобы гарантировать "здоровье" сервера. Кроме того, следует проводить мониторинг для обеспечения доступности GC-каталога, позволяющего пользователям входить в систему и поддерживать членство универсальных групп.

Далее приведено краткое описание некоторых основных элементов Active Directory, мониторинг которых необходим.

13.3.1 Мониторинг производительности

Как и любая критичная для бизнеса система, Active Directory должна находиться под постоянным контролем. Для решения этой задачи Microsoft встроило в механизм Active Directory целый ряд возможностей, включающий как расширенную диагностику в EventLog *контроллеров домена*, отчеты и логи в текстовые файлы, так и встроенные счетчики производительности.

Данные о производительности Active Directory позволяют [4]:

- оценить производительность Active Directory и ее влияние на ресурсы системы;
- наблюдать за изменениями и тенденциями производительности и использованием ресурсов и соответствующим образом планировать модернизацию парка компьютеров;
- тестировать изменения конфигурации или параметры настройки системы посредством мониторинга результатов;
- диагностировать проблемы, а также компоненты или процессы, требующие оптимизации.

В Windows имеется несколько средств мониторинга производительности Active Directory. Основной является консоль Performance (Производительность), в которой можно настроить просмотр детальных числовых значений, отражающих функционирование Active Directory. Можно представить эти данные в графическом виде с заказанной периодичностью

обновления данных. Возможности этой консоли также позволяют регистрировать активность системы в файл или отсылать предупреждения.

Чтобы сохранить максимальную производительность службы каталога, необходимо также знать, что предпринимать в ответ на проведенный мониторинг, то есть что требуется для поддержания функционального состояния службы в пределах нормальных рабочих параметров, которые были установлены.

13.3.2 Мониторинг репликации

Один из критических компонентов Active Directory, за работой которого необходимо наблюдать, - это *репликация*.

Существуют два стандартных средства администрирования серверов для мониторинга и поиска неисправностей репликации. Первый инструмент - Event Viewer (Средство просмотра событий). Журнал событий Directory Service (Служба каталога) - это один из журналов регистрации событий, который добавляется ко всем *контроллерам домена*. Большая часть событий, связанных с репликацией каталога, записывается в него, и это первое место, которое необходимо просмотреть в случае возникновения сбоя при репликации.

Инструмент администрирования Performance (Производительность) полезен для контроля деятельности, связанной с репликацией, которая происходит на сервере. Когда сервер назначается *контроллером домена*, к списку счетчиков производительности добавляется объект NTDS Performance. Счетчики производительности можно использовать для контроля объема трафика репликации, а также другой деятельности, связанной с Active Directory.

Одно из наиболее полезных инструментальных средств, предназначенных для мониторинга и поиска неисправностей репликации, - это Replication Monitor (Монитор репликации). Монитор репликации

контролирует один или более серверов по создаваемому администратором списку серверов, предоставляя возможность управлять почти всеми аспектами репликации Active Directory - например, отслеживать текущее состояние репликации, последнюю успешную репликацию или любые отказы при репликации; вынуждать репликацию; вынуждать КСС к повторному вычислению топологии маршрутизации. Используя данный инструмент мониторинга, можно контролировать репликации на всех *контроллерах домена* корпоративной сети.

Второй полезный инструмент мониторинга репликаций - Repadmin, входящий в набор Windows Server 2003 Support Tools (Средства обслуживания Windows Server 2003) и обеспечивающий такие же функциональные возможности, как и Replication Monitor, но через интерфейс командной строки. Инструмент Repadmin дополнительно позволяет изменять топологию репликации, добавляя объекты связи, и сообщает об отказах репликационных связей между двумя партнерами по репликации.

Также в состав пакета Windows Server 2003 Support Tools входит инструмент командной строки Dcdiag, который может проверять DNS-регистрацию *контроллера домена*. Он отслеживает наличие идентификаторов защиты (SID) в заголовках контекста именования (naming context), соответствующие разрешения для репликации, анализирует состояние *контроллеров домена* в *лесе* или предприятии и многое другое.

13.3.3 Мониторинг службы DNS

В Windows предусмотрены два способа контроля работы сервера *DNS* [4]:

- **Запись событий по умолчанию в журнал сервера DNS**. Сообщения о событиях сервера *DNS* хранятся в журнале (log-файле) сервера отдельно от файлов событий, связанных с другими приложениями. Этот журнал можно просмотреть из оснастки Event Viewer. В него записывается ограниченный набор событий, выявляемых службой *DNS*, таких как запуск и остановка сервера. Event Viewer также позволяет наблюдать за событиями *DNS* на компьютерах клиентов: эти события заносятся в файл журнала на каждом компьютере.

- **Использование команд отладки для записи событий в текстовый файл**. Консоль *DNS* позволяет задавать дополнительные параметры для создания временного текстового файла журнала (DNS.log), хранящегося в папке %systemroot%\DNS. Серверы *DNS* в Windows поддерживают следующие отладочные команды:
    - Query - записывать запросы, полученные от клиентов;
    - Notify - записывать уведомления, полученные от других серверов *DNS*;
    - Update - записывать изменения зоны, полученные от других компьютеров;
    - Questions - записывать содержимое раздела вопроса для каждого запроса, обработанного сервером *DNS*;
    - Answers - записывать содержимое раздела ответа для каждого запроса, обработанного сервером *DNS*;
    - Send - подсчитывать запросы, посланные сервером *DNS*;
    - Received - подсчитывать запросы, полученные сервером *DNS*;
    - UDP - подсчитывать запросы, полученные по протоколу UDP;
    - TCP - подсчитывать запросы, полученные по протоколу TCP;
    - Full Packets - подсчитывать полные пакеты, полученные и записанные сервером *DNS*;
    - Write Through - подсчитывать пакеты, прошедшие через сервер *DNS* туда и обратно.

По умолчанию все эти дополнительные возможности отладки отключены. После активизации какой-либо из них служба *DNS* сможет контролировать дополнительные виды событий, что может пригодиться при отладке сервера. Такой мониторинг требует много ресурсов (в некоторых случаях замедляется работа сервера и требуется дополнительное место на диске), поэтому его следует использовать кратковременно, когда действительно нужна подробная информация о работе сервера.

13.4Автоматизация мониторинга Active Directory

Active Directory в процессе своей работы постоянно занимается самодиагностикой. Часть сбоев Active Directory умеет исправлять самостоятельно, но некоторые действия требуют участия квалифицированного персонала. Крайне важно своевременно заметить такой сбой и предпринять корректирующие действия.

Для этого рядом фирм разработано специальное программное обеспечение, позволяющее в реальном времени отслеживать работу Active Directory и предоставляющее администратору расширенный набор инструментов для диагностики и устранения проблем.

Компания Microsoft также выпустила на рынок свое решение под названием Microsoft Operations Manager (MOM 2005, MSCOM 2007). Возможности этого продукта позволяют контролировать абсолютное большинство ключевых параметров Active Directory [6]:

- AD DIT/Log Free Space.
- All Performance Data.
- Database and Log Overview.
- Database Size.
- DC OS Metrics Overview.
- DC Response Time.
- DC/GC Response.
- GC Response Time.
- Log File Size.
- LSASS Processor Time.
- Memory metrics.
- Intersite Replication Traffic.
- Replication Alerts last 7 days.
- Replication Inbound Bytes/sec.
- Replication Latency.
- Replication Performance Overview.

В MOM имеется встроенный механизм оповещения администраторов о возникших проблемах, а также возможность строить целевые отчеты для выявления узких мест системы и опасных тенденций, что позволяет предотвратить сбой еще до того, как он возникнет и ситуация станет критической. MOM включает управление событиями, мониторинг служб и предупреждений, генерацию отчетов и анализ тенденций. Это делается через центральный пульт: агенты, выполняющиеся на управляемых узлах (серверах, являющихся объектами мониторинга), посылают данные, которые будут проанализированы, отслежены и отображены на едином пульте управления. Эта централизация дает возможность сетевому администратору управлять большой совокупностью серверов из одного места с помощью мощных инструментов, предназначенных для удаленного управления серверами. Системы MOM используют пакеты управления для расширения базовой информации, касающейся определенных сетевых услуг, а также серверных приложений. Пакет управления Base Management Pack содержит характеристики всех служб сервера Windows Server 2003, включая Active Directory, службу доменных имен (*DNS*) и Интернет-службу Microsoft Internet

Information Services (IIS). Пакет управления Application Management Pack включает характеристики серверов Microsoft .NET Enterprise Servers, таких как Microsoft Exchange 2000 Server и Microsoft SQL Server 2000.

В крупных компаниях, имеющих соответствующие достаточные ресурсы, рекомендуется внедрять данный комплекс мониторинга (или аналогичные системы) уже на ранних стадиях развертывания Active Directory.

13.5Краткие итоги

14 ЛЕКЦИЯ: УСТРАНЕНИЕ НЕПОЛАДОК С ACTIVE DIRECTORY

Описаны типичные проблемы при функционировании Active Directory, включая ошибки репликации, неполадки с DNS и схемой, проблемы при задании разрешений и сведений о доверии. Приведены возможные варианты решения перечисленных проблем.

Цель лекции: Дать представление о возможных неполадках с Active Directory и способах их устранения.

При возникновении неполадок в работе Active Directory необходимо в первую очередь проверить журнал событий службы каталогов. Кроме того, существуют и другие специализированные средства отслеживания проблем. Также для решения возникающих вопросов с Active Directory возможно обращение в сертифицированные службы поддержки вендоров и к информации, размещенной на официальном сайте производителя.

14.1 Типичные проблемы с Active Directory

Перечислим некоторые типичные проблемы с Active Directory, с которыми можно столкнуться, и их возможные решения [4], [5].

- **Невозможно добавить или удалить домен**. Возможная причина: *хозяин именования доменов* недоступен, что может быть вызвано проблемами с сетевым соединением или отказом компьютера, играющего роль *хозяина именования доменов*. Предлагаемое решение: решить проблему с сетевым соединением, или починить/заменить компьютер, играющий роль *хозяина именования доменов*, или переназначить роль *хозяина именования доменов*.
- **Невозможно создать объекты в Active Directory**. Возможная причина: недоступен мастер относительных идентификаторов, что может быть вызвано проблемами с сетевым соединением или отказом компьютера, играющего роль мастера относительных идентификаторов. Предлагаемое решение: решить проблему с сетевым соединением, или починить/заменить компьютер, играющий роль мастера относительных идентификаторов, или переназначить роль мастера относительных идентификаторов.
- **Изменения членства в группе не вступают в силу**. Возможная причина: недоступен *хозяин инфраструктуры*, что может быть вызвано проблемами с сетевым соединением или отказом компьютера, играющего роль *хозяина инфраструктуры*. Предлагаемое решение: решить проблему с сетевым соединением, или починить/заменить компьютер, играющий роль *хозяина инфраструктуры*, или переназначить роль *хозяина инфраструктуры*.
- **Пользователи без программного обеспечения Active Directory не могут войти в систему**. Возможная причина: недоступен *эмулятор основного контроллера домена*, что может быть вызвано проблемами с сетевым соединением или отказом компьютера, играющего роль эмулятора основного контроллера домена. Предлагаемое решение: решить проблему с сетевым соединением, или починить/заменить компьютер, играющий роль эмулятора

основного контроллера домена, или переназначить роль эмулятора основного контроллера домена.

- **Пользователю не удается локально войти в систему на контроллере домена**. Вероятная причина: возможность локального входа в систему контроллера домена управляется политиками безопасности, которые устанавливаются в параметрах групповой политики. Предлагаемое решение: в используемом по умолчанию *объекте* "Политика контроллера домена" назначить определенному пользователю или группе право "Локальный вход в систему".
- **Не удается подключиться к контроллеру домена, работающему под управлением Windows 2000**. Возможная причина: на контроллере домена под управлением Windows 2000, к которому производится подключение, не установлен пакет обновления версии 3 или более поздней. Предлагаемое решение: установить на *контроллер домена* под управлением Windows 2000 пакет обновления версии 3 или более поздней.
- **Сообщения об ошибках "Домен не найден", "Сервер недоступен" или "Сервер RPC недоступен"**. Возможная причина: ошибка регистрации или разрешения имени. Предлагаемое решение: проверить доступность и правильность работы службы *DNS* (в том числе регистрацию NetBIOS) на соответствующем сервере.

14.2Ошибки репликации

Неэффективная *репликация* вызывает падение производительности службы Active Directory, например, могут не распознаваться новые пользователи. В большинстве случаев в результате неэффективной обработки запросов и неэффективной репликации информация каталога устаревает, а контроллеры домена становятся недоступными.

Журнал службы каталога сообщает об ошибках репликации, которые происходят после установления репликационной связи. Нужно просматривать журнал регистрации событий службы каталога в поисках событий репликации, имеющих тип Error (Ошибка) или Warning (Предупреждение).

Далее приводится два примера типичных ошибок репликации в том виде, как они отображены в журнале регистрации событий службы каталога [13].

- **Событие с ID 1311**. Информация о конфигурации репликации, имеющаяся в инструменте Active Directory Sites And Services (*Сайты* и службы Active Directory), не отражает точно физическую топологию сети. Эта ошибка указывает на то, что один или более контроллеров домена или сервер-плацдарм находятся в автономном режиме (либо отключены), или что серверы-плацдармы подключены, но не содержат нужных контекстов именования (NC), либо при репликации требуемого контекста наименования между *сайтами* Active Directory возникают ошибки. Также возможная причина данной ошибки заключается в том, что один или несколько узлов не включены в *связи сайтов* либо *связи*

сайтов содержат все *сайты*, но не все взаимодействующие между собой *связи сайтов*.

- **Событие с ID 1265** (Access denied - Доступ запрещен). Эта ошибка может возникать в том случае, если локальный *контроллер домена* не сумел подтвердить подлинность своего партнера по репликации при создании репликационной связи или при попытке реплицировать по существующей связи. Ошибка возникает тогда, когда *контроллер домена* был отсоединен от остальной части сети в течение долгого времени и его пароль учетной записи компьютера не синхронизирован с паролем учетной записи компьютера, хранящимся в каталоге его партнера по репликации.

Если получено сообщение о событии с ID 1265 и ошибке "Ошибка поиска в *DNS*" или об ошибке "RPC-сервер недоступен" в журнале службы каталогов, то возможная причина свидетельствует о неполадках *DNS*.

Репликация Active Directory зависит от следующих факторов:

- Записи должны реплицироваться на DNS-серверы, используемые партнерами репликации.
- Каждая зона *DNS* должна иметь необходимое делегирование дочерних зон.
- В IP-конфигурации контроллеров доменов должны быть правильно заданы основные и альтернативные DNS-серверы.

Как правило, проблемы, которые можно устранить средствами консоли Active Directory Sites and Services, таковы [4]:

- новая информация каталога не распространяется своевременно;
- запросы на обслуживание не обрабатываются вовремя.

Далее приведены некоторые типичные ошибки репликации и способы их устранения [4], [5], [6].

- **Любой отказ в репликации между контроллерами домена**. Возможная причина: неправильное функционирование инфраструктуры *DNS*. Предлагаемое решение: настроить DNS-сервер и правильно сконфигурировать службу *DNS*.
- **Репликация информации каталога прекратилась**. Возможная причина: *сайты*, включающие клиентов и контроллеры домена, не имеют связей с контроллерами доменов другого *сайта* сети, что вызывает сбои в обмене информацией каталога между *сайтами*. Предлагаемое решение: создать связь между текущим *сайтом* и *сайтом*, подключенным к остальным *сайтам* сети.
- **Репликация информации каталога замедлилась, но не остановилась**. Возможные причины и предлагаемые решения приведены в таблице 14.1.

Таблица 14.1. Причины и решения при замедлении репликации

Возможная причина	Предлагаемое решение
Хотя все *сайты* соединены связями, существующая структура межсайтовой репликации недостаточно полна.	Необходимо убедиться, что служба Active Directory настроена правильно. Для объединения нескольких *связей сайтов*,

Информация каталога реплицируется на все контроллеры домена, если они объединены связями, однако это не оптимальное решение. При наличии *связей сайтов* и отсутствии мостов распространение изменений с одних контроллеров доменов на другие, с которыми отсутствуют прямые связи, выполняется слишком долго	требующих более эффективной репликации, рекомендуется создать мост или объединить в мост все *связи сайтов*
Текущих сетевых ресурсов недостаточно для обслуживания суммарного трафика репликации. Такая ситуация может повлиять на службы, не имеющие отношения к Active Directory, поскольку обмен информацией каталога требует значительных сетевых ресурсов	Увеличить долю свободных сетевых ресурсов, выделяемых трафику каталога. Уменьшить частоту репликации в расписании. Настроить стоимость *связей сайтов*. Создать *связи сайтов* или мосты связей сайтов, чтобы получить сетевые подключения с повышенной пропускной способностью
Информация каталога, изменившаяся на контроллерах домена в одном *сайте*, своевременно не обновилась на контроллерах домена в других *сайтах*, поскольку заданная в расписании частота межсайтовой репликации слишком низка	Увеличить частоту репликации. Если *репликация* выполняется через мост, проверить, какая *связь сайтов* сдерживает репликацию. Увеличить интервал времени, отведенный для репликации, или частоту репликации в заданный интервал времени для проблемной *связи сайтов*.
Клиенты пытаются запросить аутентификацию, информацию и службы у контроллера домена по подключению с низкой пропускной способностью. Это может замедлить отклик на запросы клиентов.	Проверить, имеется ли *сайт*, который способен лучше обслуживать подсеть клиента. Если медленно обслуживаемый клиент изолирован от контроллера домена, попробовать создать другой *сайт* с собственным контроллером домена, к которому затем присоединить клиента. Создать подключение с большей пропускной способностью.

- **При попытке репликации вручную получено сообщение "Отказано в доступе" от оснастки Active Directory Sites And Services (Сайты и службы Active Directory)**. Возможная причина: принудительная *репликация*, выполняемая пользователем вручную, влечет за собой репликацию не всех общих каталогов приложений партнеров репликации, а возможна только для тех контейнеров, для которых разрешена синхронизация репликации, при этом *репликация* остальных каталогов приложений даст сбой. Предлагаемое решение: для принудительной репликации вручную указанного каталога приложений

использовать средства командной строки Repadmin из набора инструментов поддержки Windows.

- **Не удается подключиться к контроллеру домена под управлением Windows 2000 при помощи оснастки Active Directory Sites And Services (Сайты и службы Active Directory)**. Возможная причина: на контроллере домена, который работает под управлением Windows 2000 и к которому требуется подключиться, не установлен пакет обновления версии 3 или более поздний. Предлагаемое решение: установить на *контроллер домена* под управлением Windows 2000 пакет обновления версии 3 или более поздний.

Проверка топологии репликации заключается в том, что Active Directory запускает процесс, который определяет стоимость межсайтовых подключений, проверяет доступность известных контроллеров домена и факт добавления новых. На основе полученных сведений Active Directory добавляет или удаляет объекты-подключения для формирования эффективной топологии репликации. Этот процесс не затрагивает объекты-подключения, созданные вручную с помощью инструмента Active Directory Sites and Services.

14.3Устранение неполадок DNS

Приведем некоторые возможные неполадки *DNS* и способы их решения [4], [6].

- **Прерывание делегирования зоны**. Возможная причина: делегирование зоны неправильно сконфигурировано. Предлагаемое решение: проверить параметры делегирования зоны и исправить конфигурацию, если это необходимо.
- **Неполадки, связанные с зонной передачей**. Возможные причины и предлагаемые решения приведены в таблице 14.2.

Таблица 14.2. Причины и решения при неполадках, связанных с зонной передачей

Возможная причина	Предлагаемое решение
Приостановка службы DNS на сервере	Необходимо убедиться, что все серверы, используемые в процессе передачи, доступны и службы *DNS* на них не приостановлены
Разрыв связи по сети между серверами *DNS*, используемыми в процессе зонной передачи	Проверить (используя команду PING) с двух сторон наличие сетевого канала между двумя серверами *DNS*. В случае неудачи одного из двух тестов необходимо искать причину непосредственно в сети
Серийные номера зоны	Увеличить серийный номер (используя консоль

на сервере-получателе и сервере-источнике совпадают, что препятствует передаче	*DNS*) для сервера-источника, чтобы он превысил серийный номер сервера-получателя, после чего инициировать передачу зоны на сервере-получателе
Возникают проблемы при взаимодействии сервера-источника и сервера-получателя	Проверить, не установлена ли на одном из серверов старая версия *DNS* (например, версия BIND)
Зона содержит записи ресурсов и другие данные, которые сервер *DNS* не может правильно интерпретировать	Необходимо убедиться, что зона не содержит несовместимых типов данных (например, записей ресурсов неподдерживаемых типов) и ошибок. Указать в конфигурации сервера приостановку загрузки некорректных данных и определить метод проверки имен (эти параметры задаются в консоли *DNS*)
Данные полномочной зоны некорректны	Если при передаче зоны постоянно происходят ошибки, то необходимо убедиться, что зона не содержит нестандартных данных. Чтобы определить вероятный источник ошибок, нужно просмотреть сообщения в журнале сервера *DNS*

- Неполадки динамического обновления. Возможные причины и предлагаемые решения приведены в таблице 14.3.

Таблица 14.3. Причины и решения при неполадках динамического обновления

Возможная причина	Предлагаемое решение
Клиент (или его сервер DHCP) не поддерживает протокол динамического обновления *DNS*	Необходимо убедиться, что пользователи поддерживают протокол динамического обновления и включены опции динамической поддержки. Чтобы зарегистрировать компьютеры клиентов для динамического обновления, рекомендуется установить на них Windows 2000 либо установить в сети сервер DHCP для обслуживания клиентов
Клиент не смог зарегистрироваться на сервере *DNS* для динамического обновления из-за неполной конфигурации *DNS*	Необходимо убедиться, что клиент правильно сконфигурирован, и при необходимости обновить конфигурацию. Для обновления конфигурации клиентов требуется задать первичный суффикс "*DNS*" на компьютере клиента с постоянным IP-адресом или задать зависящий от соединения суффикс "*DNS*" на

	одном из сетевых подключений клиента
Клиент *DNS* не смог обновить информацию с сервера *DNS* из-за проблем на сервере	Если клиент может обращаться к своему основному и альтернативным серверам *DNS*, указанным в его конфигурации, значит, источник проблемы не в компьютере клиента. На клиентах под управлением Windows 2000 рекомендуется использовать Event Viewer для просмотра системного log-файла и определения причин неудач при обновлениях записей ресурсов узлов и указателей
Сервер *DNS* не поддерживает динамические обновления	Необходимо убедиться, что сервер *DNS*, к которому обращается клиент, способен поддерживать протокол динамического обновления
Сервер *DNS* способен поддерживать динамическое обновление, но не делает этого	Необходимо убедиться, что основная зона, откуда клиенты получают изменения, настроена на их поддержку. По умолчанию, сервер *DNS* с Windows 2000 для основной зоны не поддерживает динамические обновления. Требуется отредактировать свойства зоны на основном сервере *DNS*, если это необходимо
База данных зоны недоступна	Необходимо убедиться, что зона существует и доступна для изменений. Для основных серверов *DNS* нужно проверить, что файл зоны на сервере существует и зона не приостановлена. Дополнительные серверы не поддерживают динамическое обновление. Для зоны, интегрированной в Active Directory, сервер *DNS* должен являться контроллером домена и иметь доступ к базе данных Active Directory, где хранится файл зоны

14.4Устранение неполадок схемы

Далее приведены некоторые типичные неполадки схемы Active Directory и способы их устранения [5].

- **Невозможно изменить или расширить схему**. Возможные причины и предлагаемые решения приведены в таблице 14.4.

Таблица 14.4. Причины и решения при невозможности изменить схему

Возможная причина	Предлагаемое решение
Хозяин схемы недоступен, что может быть вызвано проблемами с сетевым соединением или отказом компьютера, играющего роль хозяина схемы	Решить проблему с сетевым соединением, или починить/заменить компьютер, играющий роль хозяина схемы, или переназначить роль хозяина схемы
Пользователь, пытающийся изменить схему, не входит в группу "Администраторы схемы"	Добавить соответствующую учетную запись пользователя в группу "Администраторы схемы"
Контроллер домена, являющийся хозяином схемы, работает под управлением Windows 2000, и на нем не разрешено изменение схемы	Разрешить изменение схемы на этом контроллере домена

- **Невозможно добавить атрибуты в класс**. Возможные причины и предлагаемые решения приведены в таблице 14.5.

Таблица 14.5. Причины и решения при невозможности добавить атрибуты в класс

Возможная причина	Предлагаемое решение
Атрибуты не удается связать с классом, поскольку не обновлен кэш схемы	После добавления атрибута и до добавления этого атрибута в класс необходимо убедиться, что кэш схемы обновлен
Предпринята попытка определения класса на контроллере домена, который не является хозяином схемы и на который еще не реплицирован новый атрибут	Требуется всегда выполнять обновление схемы на хозяине схемы

- **Не удается найти или запустить оснастку "Схема Active Directory"**. Возможная причина: оснастка "Схема Active Directory" не установлена или не зарегистрирована. Предлагаемое решение: установить и/или зарегистрировать оснастку "Схема Active Directory" [6].
- **Не удается подключиться к контроллеру домена, работающему под управлением Windows 2000, при помощи оснастки "Схема Active Directory"**. Возможная причина: на контроллере домена под управлением Windows 2000, к которому производится подключение, не установлен пакет обновлений версии 3 или более поздней. Предлагаемое решение: установить на *контроллер домена* под управлением Windows 2000 пакет обновлений версии 3 или более поздней.

14.5Устранение неполадок в сведениях о доверии

Далее приведены некоторые типичные неполадки в сведениях о доверии Active Directory и способы их устранения [5].

- **Клиенты не могут обратиться к ресурсам в другом домене**. Возможная причина: произошел разрыв доверительных отношений между *доменами*. Предлагаемое решение: восстановить и проверить *доверительные отношения* между *доменами*; для успешного восстановления доверия потребуется *эмулятор основного контроллера домена* (эмулятор PDC), который должен быть доступен.
- **Клиентам не удается получить доступ к ресурсам домена вне леса**. Возможная причина: произошел сбой внешнего доверия между *доменами*. Предлагаемое решение: восстановить и проверить *доверительные отношения* между *доменами*; для успешного восстановления доверия потребуется *эмулятор основного контроллера домена* (эмулятор PDC), который должен быть доступен.
- **Ошибки доверия между серверами или рабочими станциями**. Возможная причина: время синхронизации между контроллерами домена или рабочими станциями неверно, сервер находится в нерабочем состоянии либо нарушено доверительное отношение. Предлагаемое решение: осуществить проверку и установку доверительных отношений между компьютерами, при необходимости в режиме пакетного управления довериями, а также обеспечить защиту каналов между компьютерами.

14.6Проблемы при задании разрешений

При назначении или изменении разрешений NTFS на доступ к файлам/папкам иногда возникают проблемы, которые важно вовремя устранить. Далее описаны некоторые типичные проблемы с разрешениями, а также способы их устранения [4].

- **Пользователь не может получить доступ к файлу или папке**. Если файл или папка были скопированы или перемещены на другой том NTFS, разрешения могли измениться. Необходимо проверить разрешения, назначенные учетной записи пользователя и группам, членом которых он является. Например, иногда пользователь не имеет разрешение или доступ для него запрещен в индивидуальном порядке или как члену группы.
- **Учетная запись пользователя добавлена в группу, чтобы предоставить этому пользователю доступ к файлу или папке, но он не может получить доступ**. Чтобы войти в новую группу, в которую добавлена *учетная запись*, пользователь должен или выйти из системы и затем войти в нее повторно, или закрыть все сетевые подключения к компьютеру, на котором размещен файл или папка, и затем создать новое подключение.
- **Пользователь с разрешением Full Control для папки удаляет файл в папке, хотя не имеет разрешения удалять этот файл**. Необходимо предотвратить дальнейшее удаление пользователем файлов. Необходимо отменить специальное разрешение для папки, чтобы лишить пользователя с разрешением Full Control права удалять файлы в этой папке.

Далее приведены рекомендации по внедрению разрешений NTFS, которые помогут избежать возможных проблем [4].

- Рекомендуется назначать наиболее строгие разрешения NTFS, позволяющие пользователям и группам выполнять только необходимые задачи.
- Рекомендуется назначать все разрешения на уровне папок, а не на уровне файлов. Необходимо сгруппировать файлы, доступ к которым требуется ограничить, в отдельную папку и ограничить к ней доступ.
- Для всех исполняемых файлов приложений рекомендуется назначить группе Administrators (Администраторы) разрешения Read & Execute и Change Permissions, а группе Users (Пользователи) - разрешение Read & Execute. Повреждение файлов приложений обычно является результатом деятельности вирусов и несанкционированных действий. Назначив указанные разрешения, можно предотвратить изменение или удаление исполняемых файлов.
- Рекомендуется назначить группе CREATOR OWNER (Создатель-владелец) разрешение Full Control для общих папок данных, чтобы пользователи могли удалять и изменять созданные ими файлы/папки. Данное разрешение предоставляет пользователю, создавшему файл/папку, полный доступ в общей папке данных только к тем файлам/папкам, которые созданы непосредственно им.
- Для общих папок группе CREATOR OWNER рекомендуется назначить разрешение Full Control, а группе Everyone - разрешение Read and Write. Пользователи получат полный доступ к созданным ими файлам, однако члены группы Everyone (Все) смогут лишь считывать и добавлять файлы в каталог.
- Если к ресурсу не будут обращаться по сети, рекомендуется использовать длинные и подробные имена. Если планируется открыть к папке совместный доступ, имена папок/файлов должны поддерживаться всеми клиентскими компьютерами.
- Рекомендуется назначать, но не аннулировать разрешения. Если надо, чтобы пользователь или группа не имели доступа к конкретной папке или файлу, рекомендуется не назначать им соответствующее разрешение. Отмена разрешений должна быть исключением, а не обычной практикой.

14.7 Краткие итоги

15 ЛЕКЦИЯ: ВОССТАНОВЛЕНИЕ ACTIVE DIRECTORY

Дан краткий обзор процесса восстановления Active Directory, в том числе описаны предварительные действия при подготовке к отказам

Цель лекции: Указать необходимость спланировать подготовку к отказам для возможности восстановления Active Directory.

Служба каталога Active Directory - это наиболее критическая сетевая служба, которая развернута в сети. Если инфраструктура Active Directory будет неудачной, пользователи сети будут чрезвычайно ограничены в своей работе в сети. Почти все сетевые службы в Microsoft Windows Server 2003 выполняют аутентификацию пользователей в Active Directory, прежде чем они получат доступ к какому-либо сетевому ресурсу. Поэтому надо заранее приготовиться к предотвращению отказов и восстановлению службы.

15.1 Подготовка к отказам

Первые шаги в восстановлении системы после отказа выполняются намного раньше, чем случится сам отказ.

Подготовка включает просмотр всех элементов, составляющих нормальную сетевую инфраструктуру, а также некоторые специфичные для Active Directory вещи.

Перечисленные ниже процедуры являются критически важными [13].

- **Разработать последовательное создание резервной копии и восстановить управление контроллеров домена**. Первый шаг в любом плане восстановления состоит в установке соответствующих аппаратных средств и программного обеспечения для поддержки создания резервных копий контроллеров домена; после этого рекомендуется создать и протестировать план резервирования и восстановления.
- **Развернуть контроллеры домена Active Directory с аппаратной избыточностью**. Большинство серверов можно заказывать с некоторым уровнем аппаратной избыточности при небольшой дополнительной стоимости. Например, сервер с двойным источником питания, избыточными сетевыми картами и избыточной аппаратной системой жесткого диска должен быть стандартным оборудованием для контроллеров домена. Во многих больших компаниях аппаратная избыточность поднята на такой уровень, когда все контроллеры домена связаны с различными цепями питания и подключены к различным коммутаторам Ethernet или сетевым сегментам.

15.2Хранение данных в Active Directory

База данных Active Directory хранится в файле по имени Ntds.dit, который по умолчанию расположен в папке %systemroot%\NTDS, содержащей также следующие файлы [13]:

- Edb.chk - файл контрольных точек, который указывает, какие транзакции из журналов регистрации были записаны в базу данных Active Directory;
- Edb.log - журнал регистрации текущих транзакций, имеющий фиксированную длину в 10 Мб;
- Edbxxxxx.log. После того как Active Directory проработала некоторое время, могут появиться один или более журналов, у которых часть имени файла, обозначенная как xxxxx, представляет собой увеличивающийся шестнадцатеричный порядковый номер. Эти журналы являются предшествующими журналами; всякий раз, когда текущий журнал заполнен, он переименовывается в следующий предшествующий журнал, и создается новый журнал Edb.log. Старые журналы автоматически удаляются по мере того, как изменения, представленные в журналах, переносятся в базу данных Active Directory. Каждый из этих журналов занимает 10 Мб;
- Edbtemp.log - временный журнал, который используется тогда, когда заполнен текущий журнал (Edb.log). Новый журнал создается под именем Edbtemp.log, в нем хранятся все транзакции, а затем журнал Edb.log переименовывается в следующий предшествующий журнал. Далее журнал Edbtemp.log переименовывается в журнал Edb.log;
- Res1.log и Res2.log - резервные журналы, которые используются только в ситуации, когда на жестком диске заканчивается свободное пространство. Если текущий журнал заполнен, а сервер не может создать новый журнал, потому что на жестком диске нет свободного пространства, сервер подавит любые транзакции Active Directory, находящиеся в настоящее время в памяти, использует место для резервных журналов, а затем завершит работу Active Directory. Размер каждого из этих журналов - 10 Мб.

Каждая модификация в базе данных Active Directory называется транзакцией. Транзакция может состоять из нескольких шагов. Например, когда пользователь перемещается из одной *организационной единицы* (OU) в другую, в OU-адресате должен быть создан новый объект, а в OU-источнике удален старый объект. Чтобы транзакция была закончена, оба шага должны быть выполнены; если один из шагов потерпит неудачу, вся транзакция должна получить откат, чтобы никакой шаг не был засчитан. Когда все шаги в транзакции выполнены, транзакция считается законченной. Используя модель транзакций, система Windows Server 2003 гарантирует, что база данных всегда остается в согласованном состоянии.

Всякий раз, когда в базе данных Active Directory делается какое- либо изменение (например, изменяется номер телефона пользователя), оно сначала

записывается в журнал транзакций. Поскольку журнал транзакций является текстовым файлом, в котором изменения записываются последовательно, то запись в журнал происходит намного быстрее, чем запись в базу данных. Поэтому использование журналов транзакций улучшает работу контроллера домена.

Как только транзакция была записана в журнал транзакций, контроллер домена загружает страницу базы данных, содержащую пользовательский объект, в память (если она еще не находится в памяти). Все изменения в базе данных Active Directory делаются в памяти контроллера домена. *Контроллер домена* использует максимально доступный объем памяти и хранит в памяти максимально большую часть базы данных Active Directory. *Контроллер домена* удаляет страницы базы данных из памяти только тогда, когда свободная память становится ограниченной или когда *контроллер домена* выключается. Изменения, сделанные к страницам базы данных, переписываются в базу данных только тогда, когда сервер мало используется или при его выключении.

Журналы транзакций не только улучшают работу контроллера домена, обеспечивая место для быстрой записи изменений, но и обеспечивают возможность восстановления данных в случае отказа сервера. Например, если было сделано изменение, относящееся к Active Directory, то оно записывается в журнал транзакций, а затем на страницу базы данных, находящуюся в памяти сервера. Если в этот момент сервер неожиданно выключается, то изменения не будут переданы из памяти сервера в базу данных. Когда *контроллер домена* будет перезапущен, он найдет в журнале все транзакции, которые еще не были переданы в базу данных. Затем эти изменения применятся к базе данных при запуске служб контроллера домена. В процессе этого восстановления используется файл контрольной точки. Файл контрольной точки является указателем на то, какие транзакции из имеющихся в журнале были переписаны в базу данных. В процессе восстановления *контроллер домена* читает файл контрольной точки,

определяя, какие транзакции были переданы базе данных, а затем он добавляет в базу данных изменения, которые еще не были переданы. Использование журналов транзакций улучшает работу контроллеров домена и увеличивает возможность восстановления данных в случае неожиданного выключения сервера. Эти преимущества максимальны, если журнал транзакций и база данных расположены на отдельных жестких дисках.

Служба Active Directory Windows Server 2003 сконфигурирована для циркулярной (circular) регистрации, и эта конфигурация не может быть изменена. При циркулярной регистрации сохраняются только те предшествующие журналы, содержащие транзакции, которые не были переписаны в базу данных. По мере передачи информации из предшествующего журнала в базу данных журнал удаляется. Циркулярная регистрация предотвращает потерю данных в случае сбоя на жестком диске контроллера домена, когда будет восстанавливаться база данных из резервной копии. Предположим, что выполняется *резервное копирование* Active Directory каждую ночь, но жесткий диск контроллера домена сломался в 17:00, после того как было сделано несколько сотен изменений в базе данных в течение дня. По мере выполнения изменений предшествующие журналы транзакций удалялись, поскольку информация из них передавалась в базу данных Active Directory. Когда будет восстановлена база данных к состоянию, соответствующему резервной копии предыдущей ночи, все изменения, которые были сделаны в течение дня, будут потеряны. Единственный способ предотвратить эту потерю данных состоит в развертывании по крайней мере двух контроллеров домена, которые реплицируют информацию друг другу в течение дня. Если произойдет сбой на одном из контроллеров домена, то можно будет восстановить на нем базу данных из резервной копии, а все изменения, сделанные в течение дня, будут скопированы на восстановленный сервер.

15.3Создание резервной копии Active Directory

Наиболее важное из ограничений, накладываемых на создание резервной копии службы каталога, состоит в том, что Active Directory может копироваться только как часть данных системного состояния контроллера домена.

Данные системного состояния контроллера домена включают [13]:

- базу данных Active Directory и журналы транзакций;
- системные файлы и файлы запуска, находящиеся под защитой Windows;
- системный реестр контроллера домена;
- всю зонную информацию DNS, интегрированную с Active Directory;
- папку Sysvol;
- базу данных регистрации классов COM+;
- базу данных службы сертификатов (если *контроллер домена* является также сервером службы сертификатов);
- информацию кластерной службы;
- метакаталоги информационной Интернет-службы Microsoft (IIS) (если служба IIS установлена на компьютере).

Все эти компоненты должны копироваться и восстанавливаться целиком из-за их тесной интеграции. Например, если на сервере службы сертификатов был создан сертификат, который был назначен на объект Active Directory, то база данных службы сертификатов (содержащая запись о создании объекта) и объект Active Directory (содержащий запись о том, что сертификат назначен на объект) должны быть сохранены.

Программы резервного копирования (backup) могут делать различные типы резервных копий, включая нормальные, добавочные, дифференцированные и т. д. *Резервное копирование* системного состояния контроллера домена всегда является нормальным копированием, когда все файлы, относящиеся к System State (Состояние системы), копируются и отмечаются как копируемые.

Общая практика состоит в том, что все контроллеры домена должны участвовать в цикле регулярного резервного копирования. Одно исключение к этому правилу можно сделать, если имеется несколько контроллеров домена, расположенных в одном офисе. В этом случае можно осуществлять такую процедуру восстановления контроллеров домена, в которой вначале

будет устанавливаться новый *контроллер домена*, а затем заполняться его каталог путем *репликации*. Однако даже в этом сценарии следует создавать резервные копии по крайней мере некоторых контроллеров домена на случай такой аварии, при которой будут выведены из строя все контроллеры домена в офисе. В любом случае необходимо создать резервные копии хозяина операций.

Другая проблема, которую нужно рассмотреть в связи с резервным копированием контроллера домена? - это частота создания резервной копии. Служба Active Directory предполагает, что давность резервной копии не может превышать время жизни объектов-памятников. По умолчанию время жизни объекта-памятника составляет 60 дней. Причина этого ограничения связана с тем способом, которым Active Directory использует объекты-памятники. Когда объект удален, он фактически не удаляется из каталога до тех пор, пока не истечет время жизни объекта-памятника. Вместо этого объект маркируется как объект-памятник, и большинство его атрибутов удаляются. Затем объект-памятник копируется на все другие контроллеры домена. По истечении времени жизни объекта-памятника он наконец удаляется из каталога на каждом контроллере домена. Если восстановить *контроллер домена* из резервной копии, давность которой превышает время жизни объекта-памятника, то в каталоге можно обнаружить информацию, несогласованную между контроллерами домена. Допустим, что пользователь был удален из каталога через день после создания резервной копии, а соответствующий объект-памятник оставался в каталоге 60 дней. Если бы резервная копия была восстановлена на контроллере домена более чем через 60 дней, после того как объект стал объектом-памятником, то на восстановленном контроллере домена был бы этот пользовательский объект, и поскольку объект-памятник более не существует, то *контроллер домена* не стал бы его удалять. В таком сценарии восстановленный *контроллер домена* имел бы копию объекта, который не существует ни в каком другом каталоге. По этой причине система резервирования и программа восстановления

предотвращают попытки восстановления каталога из резервной копии, хранящейся дольше, чем период удаления объектов-памятников.

Хотя время жизни объектов-памятников накладывает жесткое ограничение на частоту резервного копирования, очевидно, что создавать резервные копии контроллеров домена лучше гораздо чаще, чем каждые 60 дней. Возникнет много проблем, если восстанавливать *контроллер домена* из резервной копии, более давней, чем пара дней. Поскольку восстановление Active Directory включает восстановление всей информации о состоянии системы, эта информация будет восстановлена до предыдущего состояния. Если сервер является также сервером службы сертификатов, то все удостоверения, выпущенные до того, как была создана резервная копия, не будут включены в базу данных службы сертификатов. Если были обновлены драйверы или установлены какие-либо новые приложения, они не смогут работать, потому что будет сделан откат системного реестра к предыдущему состоянию. Почти все компании поддерживают такой режим резервного копирования, в котором некоторые серверы копируются каждую ночь. Контроллеры домена должны включаться в такой режим резервирования.

15.4Процесс восстановления

Существуют две причины, из-за которых, возможно, придется восстанавливать Active Directory [13].

- Первая причина возникнет, когда база данных станет непригодной для использования, потому что на одном из контроллеров домена произошел отказ в работе жесткого диска или база данных испорчена до такой степени, что ее больше не удается загрузить.
- Вторая причина возникнет, когда в результате ошибки кто-то удалил *организационную единицу*, содержащую несколько сотен учетных записей пользователей и групп. В этом случае желательнее восстановить информацию, чем вводить ее повторно.

Если планируется восстанавливать Active Directory, потому что базу данных на одном из контроллеров домена больше нельзя использовать, то имеются следующие два варианта процесса [13].

- Первый вариант состоит в том, чтобы вообще не восстанавливать Active Directory на отказавшем сервере, а создать еще один *контроллер домена*, назначив другой сервер, на котором выполняется система Windows Server 2003, контроллером домена. Таким способом будут восстановлены функциональные возможности контроллера домена, а не служба Active Directory на определенном контроллере домена.
- Второй вариант состоит в восстановлении отказавшего сервера и последующем восстановлении базы данных Active Directory на этом сервере. В этом случае будет выполнено восстановление при отсутствии полномочий (non-authoritative). При таком восстановлении база данных Active Directory восстанавливается на контроллере домена, а затем все изменения, сделанные к Active Directory после создания резервной копии, реплицируются на восстановленный *контроллер домена*.

Если планируется восстанавливать Active Directory, потому что кто-то удалил большое количество объектов из каталога, то необходимо восстановить базу данных Active Directory на одном из контроллеров домена, используя резервную копию, которая содержит удаленные объекты. Затем требуется сделать восстановление при наличии полномочий (authoritative), в процессе которого все восстановленные данные отмечаются так, чтобы они реплицировались на все другие контроллеры домена, перезаписывая удаленную информацию.

Для восстановления Active Directory необходимо архивировать данные состояния службы [4], [6]: реестр, базу данных регистрации COM+, системные загрузочные файлы и базу данных служб сертификации (если это сервер служб сертификации). При перезагрузке компьютера в режиме восстановления служб каталогов необходимо войти в систему с администраторскими правами, используя правильные имя и пароль учетной записи Security Accounts Manager. При этом нельзя использовать учетную запись администратора Active Directory, так как службы Active Directory отключены и нельзя их средствами проверить подлинность учетной записи. Для этого применяется база данных учетных записей SAM: пароль учетной записи SAM задается в процессе установки Active Directory.

15.5Краткие итоги

16 ДОПОЛНИТЕЛЬНЫЕ МАТЕРИАЛЫ: ГЛОССАРИЙ

- **Active Directory (AD)** - служба каталогов, поставляемая с Microsoft Windows начиная с Windows 2000 Server.
- **DNS (Domain Name Service)** - служба разрешения доменных имен, использующая иерархическое пространство имен для поиска компьютеров.
- **Knowledge Consistency Checker (KCC)** - отдельный контрольный процесс Active Directory, обеспечивающий целостность топологии (ни один контроллер домена не может быть исключен из процесса тиражирования) и исполняемый на всех контроллерах домена.
- **Lightweight Directory Access Protocol (LDAP)** - стандартный протокол для поиска информации в каталоге, используемый для осуществления запросов и обновления Active Directory и выполняющийся на всех контроллерах домена.
- **Группа** - набор пользователей, компьютеров или других групп, для которого можно задать разрешения.
- **Групповая политика** - средство, позволяющее задать параметры сразу для нескольких пользователей и компьютеров.
- **Дерево** - иерархия объектов и контейнеров, отражающая взаимосвязь между объектами или указывающая путь от одного объекта к другому.
- **Доверительные отношения (trust relationships)** - специальный механизм, позволяющий объектам в одном (доверяемом (trusted domain)) домене обращаться к ресурсам в другом (доверяющем (trusting domain)) домене.
- **Домен** - единая область, в пределах которой обеспечивается безопасность данных в компьютерной сети под управлением ОС Windows.
- **Доменное дерево** - иерархия доменов, которые имеют общую логическую структуру и конфигурацию и образуют непрерывное пространство имен.
- **Имя объекта** - наименование объекта, используемое для его идентификации.
- **Каталог (directory)** - информационный ресурс, используемый для хранения информации о каком-либо объекте.
- **Контейнер** - сущность, имеющая (как и объект) атрибуты, но (в отличие от объекта) не обозначающая ничего конкретного.
- **Контексты имен (сегменты, разделы)** - разделы Active Directory, содержащие следующие сегменты: раздел домена каталога, раздел конфигурации каталога, раздел схемы каталога, раздел глобального каталога, разделы приложений каталога.
- **Контроллер домена** - компьютер-сервер, управляющий доменом и хранящий реплику каталога домена (локальную БД домена).

- **Лес** - одно или несколько доменных деревьев, которые не образуют непрерывного пространства имен.
- **Логическая структура** - модель службы каталога (модель данных), которая определяет каждого участника безопасности на предприятии, а также организацию этих участников в Active Directory.
- **Модель данных** - модель, построенная на основе модели данных спецификации X.500, которая определяет логическую структуру Active Directory.
- **Область действия (scope)** - область действия Active Directory, которая может включать отдельные сетевые объекты (принтеры, файлы, имена пользователей), серверы и домены в отдельной глобальной сети, а также охватывать несколько объединенных сетей.
- **Объект** - непустой именованный набор атрибутов, обозначающий нечто конкретное, например, пользователя, принтер или приложение.
- **Объект групповой политики (Group Policy Object, GPO)** - объект, связанный с доменом, сайтом или OU и содержащий параметры конфигурации, которые требуется применить.
- **Объекты участников системы безопасности** - объекты Active Directory, которым назначены идентификаторы защиты и которые указываются при входе в сеть и предоставлении доступа к ресурсам домена.
- **Организационные единицы (подразделения)** - единицы управления внутри домена, позволяющие разделять домен на зоны административного управления.
- **Пространство имен** - ограниченная область, в которой может быть распознано данное имя путем его сопоставления с некоторым объектом или объемом информации, которому это имя соответствует.
- **Резервное копирование** - процесс, предназначенный для сохранения данных и, в случае неудачной попытки миграции, их повторного использования для совершения перехода к Active Directory.
- **Репликация** - операция в Active Directory, позволяющая синхронизировать данные в каталоге между различными контроллерами доменов.
- **Сайт (узел)** - элемент сети (одна или несколько подсетей), который содержит серверы Active Directory, поддерживает протокол TCP/IP и характеризуется хорошим качеством связи, подразумевающим высокую надежность и скорость передачи данных.
- **Связь сайта (site link)** - сущность, сконфигурированная для соединения данного сайта с остальными и состоящая из двух частей: физического соединения между сайтами (обычно WAN-канала) и объекта связи сайта (site link object), который создан в Active Directory и определяет протокол передачи трафика репликации (IP или SMTP).
- **Сегменты (разделы)** - см. Контексты имен (сегменты, разделы).
- **Сервер глобального каталога (Global Catalog, GC)** - роль, которую может выполнять любой отдельный контроллер домена в домене,

обеспечивающая пользователям возможность входить в сеть (участие в процессе аутентификации) и находить объекты в любой части леса.

- **Служба каталогов (directory service)** - сетевая служба, которая идентифицирует все ресурсы сети и делает их доступными пользователям.
- **Соглашение об уровне сервиса (Service-Level Agreement, SLA)** - соглашение между ИТ-отделом и сообществом пользователей, которое может содержать такие параметры, как максимально приемлемый уровень времени простоя системы, время входа в систему и время получения ответа на справочный запрос.
- **Учетная запись** - список атрибутов, определяющих участника системы безопасности (security principal), например, пользователя или группу пользователей.
- **Физическая структура** - структура Active Directory, которая отражает физическую структуру сети организации и состоит из компонентов (сайты и контроллеры доменов), применяемых для разработки структуры каталога.
- **Функциональная структура** - структура функционирования Active Directory, представленная в виде многоуровневой архитектуры, в которой уровни являются процессами, предоставляющими клиентским приложениям доступ к службе каталога.
- **Хозяин RID (Relative Identifier (RID) Master)** - роль (общедоменная) хозяина операций, которая может быть назначена одному из контроллеров в каждом домене и отвечает за выделение диапазонов относительных идентификаторов (RID) всем контроллерам в домене.
- **Хозяин именования доменов (Domain Naming Master)** - роль хозяина операций, которая может быть назначена контроллеру домена; действует в границах леса и отвечает за поддержание целостности доменов (протоколирование добавления и удаления доменов в лесу).
- **Хозяин инфраструктуры (Infrastructure Master)** - роль (общедоменная) хозяина операций, которая может быть назначена одному из контроллеров в каждом домене и отвечает за регистрацию изменений, вносимых в контролируемые объекты в домене.
- **Хозяин схемы (Schema Master)** - роль хозяина операций, которая может быть назначена первому контроллеру домена, действует в границах леса и отвечает за поддержку и распространение схемы на остальную часть леса.
- **Эмулятор основного контроллера домена (Primary Domain Controller (PDC) Emulator)** - роль (общедоменная) хозяина операций, которая может быть назначена одному из контроллеров в каждом домене и отвечает за эмуляцию Windows NT 4.0 PDC для клиентских машин, которые еще не переведены на Windows 2000, Windows Server 2003 или Windows XP и на которых не установлен клиент службы каталогов.

Первые шаги в восстановлении системы после отказа выполняются намного раньше, чем случится сам отказ. Подготовка включает просмотр всех элементов, составляющих нормальную сетевую инфраструктуру, а также некоторые специфичные для Active Directory вещи. Перечисленные ниже процедуры являются критически важными.

- Разработать последовательное создание резервной копии и восстановить управление контроллеров домена.
- Развернуть контроллеры домена Active Directory с аппаратной избыточностью.

Наиболее важное из ограничений, накладываемых на создание резервной копии службы каталога, состоит в том, что Active Directory может копироваться только как часть данных системного состояния контроллера домена.

Данные системного состояния контроллера домена включают:

- базу данных Active Directory и журналы транзакций;
- системные файлы и файлы запуска, находящиеся под защитой Windows;
- системный реестр контроллера домена;
- всю зонную информацию DNS, интегрированную с Active Directory;
- папку Sysvol;
- базу данных регистрации классов COM+;
- базу данных службы сертификатов (если *контроллер домена* является также сервером службы сертификатов);
- информацию кластерной службы;
- метакаталоги информационной Интернет-службы Microsoft (IIS) (если служба IIS установлена на компьютере).

Все эти компоненты должны копироваться и восстанавливаться целиком из-за их тесной интеграции.

Причины, из-за которых, возможно, придется восстанавливать Active Directory:

- База данных станет непригодной для использования.
- Удаление *организационной единицы*, содержащей несколько сотен учетных записей пользователей и групп.

Для восстановления Active Directory необходимо архивировать данные состояния службы: реестр, базу данных регистрации COM+, системные загрузочные файлы и базу данных служб сертификации (если это сервер служб сертификации).

Некоторые типичные проблемы с Active Directory, с которыми можно столкнуться:

- Невозможно добавить или удалить *домен*.
- Невозможно создать *объекты* в Active Directory.
- Изменения членства в группе не вступают в силу.
- Пользователи без программного обеспечения Active Directory не могут войти в систему.
- Пользователю не удается локально войти в систему на контроллере домена.
- Не удается подключиться к контроллеру домена, работающему под управлением Windows 2000.
- Сообщение об ошибке "*Домен* не найден", "Сервер недоступен" или "Сервер RPC недоступен".

Некоторые типичные ошибки репликации:

- Любой отказ в репликации между контроллерами домена.
- *Репликация* информации каталога прекратилась.
- *Репликация* информации каталога замедлилась, но не остановилась.
- При попытке репликации вручную получено сообщение "Отказано в доступе".
- Не удается подключиться к контроллеру домена под управлением Windows 2000 при помощи оснастки Active Directory Sites And Services (Сайты и службы Active Directory).

Некоторые возможные неполадки DNS:

- Прерывание делегирования зоны.
- Неполадки, связанные с зонной передачей.
- Неполадки динамического обновления.

Некоторые типичные неполадки схемы Active Directory:

- Невозможно изменить или расширить схему.
- Невозможно добавить атрибуты в класс.
- Не удается найти или запустить оснастку "Схема Active Directory".
- Не удается подключиться к контроллеру домена, работающему под управлением Windows 2000, при помощи оснастки "Схема Active Directory".

Некоторые типичные неполадки в сведениях о доверии Active Directory:

- Клиенты не могут обратиться к ресурсам в другом *домене*.
- Клиентам не удается получить доступ к ресурсам *домена* вне *леса*.
- Ошибки доверия между серверами или рабочими станциями.

Некоторые типичные проблемы с разрешениями:

- Пользователь не может получить доступ к файлу или папке.

- *Учетная запись* пользователя добавлена в группу, чтобы предоставить этому пользователю доступ к файлу или папке, но он не может получить доступ.
- Пользователь с разрешением Full Control для папки удаляет файл в папке, хотя не имеет разрешения удалять этот файл.

Мониторинг службы каталога является комбинацией задач, имеющих общую цель - измерение текущей характеристики некоторого ключевого индикатора (занимаемый объем диска, степень использования процессора, период работоспособного состояния службы и т. д.) по сравнению с известным состоянием (отправная точка).

Причины проведения мониторинга:

- Мониторинг идентифицирует потенциальные проблемы прежде, чем они проявятся и закончатся длительными периодами простоя службы.
- Мониторинг дает возможность поддерживать *соглашение об уровне сервиса* с пользователем сети.
- Необходимо отслеживать изменения инфраструктуры.

Преимущества, которые можно получать от проведения мониторинга Active Directory:

- Способность поддерживать SLA-соглашение с пользователями, избегая простоя службы.
- Достижение высокой производительности службы путем устранения "узких мест" в работе, которые иначе нельзя обнаружить.
- Снижение административных затрат с помощью профилактических мер в обслуживании системы.
- Повышенная компетентность при масштабировании и планировании будущих изменений инфраструктуры в результате глубокого знания компонентов службы, их функциональных возможностей и текущего уровня использования.
- Увеличение доброжелательности в отношении ИТ-отдела в результате удовлетворения клиентов.

При всех указанных преимуществах мониторинг Active Directory связан с затратами, которые необходимы для его эффективной реализации:

- Для проектирования, развертывания и управления системой мониторинга нужны соответствующие людские ресурсы (человеко-часы), требующие оплаты.
- На приобретение необходимых средств управления, на обучение и на аппаратные средства, которые предназначены для реализации мониторинга, требуются определенные фонды.
- Часть пропускной способности сети будет задействована для мониторинга Active Directory на всех *контроллерах домена* предприятия.
- Для выполнения приложений-агентов на целевых серверах и на компьютере, являющемся центральным пультом мониторинга, используются память и ресурсы процессора.

Схема процесса мониторинга службы Active Directory высокого уровня:

1. Определить, какой из индикаторов функционирования службы необходимо отслеживать.
2. Выполнить мониторинг индикаторов функционирования службы, чтобы установить и задокументировать базовый (нормальный) уровень.
3. Определить пороги для этих индикаторов функционирования,
4. Спроектировать необходимую аварийную систему, предназначенную для обработки событий при достижении порогового уровня.
5. Спроектировать систему создания отчета, фиксирующую историю состояния Active Directory.
6. Реализовать решение, которое будет измерять выбранные ключевые индикаторы в соответствии с расписанием, отражающим изменения данных индикаторов и их воздействие на состояние Active Directory.

При проектировании мониторинга рекомендуется планировать наблюдение за следующими элементами:

- Производительность служб Active Directory.
- *Репликация* Active Directory.
- Функционирование службы *DNS* и состояние DNS-сервера.
- Хранилище Active Directory.
- Служба репликации файлов.
- "Здоровье" системы *контроллера домена*.
- "Здоровье" *леса*.
- *Хозяева операций*.

Автоматизация мониторинга Active Directory возможна с помощью комплекса Microsoft Operations Manager (MOM 2005, MSCOM 2007) и его аналогов

Для возможности функционирования в компании различных приложений, используемых в бизнес-процессах до внедрения службы Active Directory, необходимо осуществить корректный перенос этих приложений и их настроек в новую спроектированную структуру.

В процессе миграции данных обеспечивается непрерывность работы пользователей и минимальное время простоя информационных систем компании.

При проведении миграции необходимо выполнить следующие задачи:

- перевести существующие домены ресурсов в организационные единицы новых доменов, что позволит упростить управление сетевыми ресурсами;

- "имитировать" ход миграции, при этом реального переноса данных не происходит;
- отменить сделанные действия, связанные с миграцией;
- переместить *учетные записи* служб;
- восстановить доверительные отношения между исходным и целевым доменами;
- преобразовать множество доменов в один или несколько крупных доменов в уже созданной среде Active Directory;
- реструктуризировать существующие группы или объединить несколько групп в одну в целевом домене;
- провести анализ процесса переноса данных с помощью журнализации миграционных событий.

Определение порядка модернизации доменов

- Определение домена, который должен быть модернизирован первым.
- Определение последовательности модернизации доменов *учетных записей*.
- Определение последовательности модернизации ресурсных доменов.
- Определение момента переключения для каждого домена из Mixed mode в Native mode Windows.
- Тестирование имеющихся критичных приложений в окружении Active Directory в смешанном режиме работы контроллеров доменов.

Существует три основных варианта модернизации доменной инфраструктуры.

- Обновление доменов.
- Реструктуризация доменов.
- Обновление доменов с их последующей реструктуризацией.

Основные критерии, которые используются при выборе наиболее подходящего варианта:

- Удовлетворенность имеющейся моделью существующего домена.
- Степень риска при переходе к новой модели домена.
- Время выполнения перехода.
- Рабочее время службы каталога, которое необходимо затратить на процесс перехода.
- Наличие ресурсов для выполнения перехода.
- Бюджет проекта перехода.

Подготовка перехода к Active Directory происходит в три этапа.

1. Планирование перехода.
2. Испытание плана перехода.
3. Проведение экспериментального перехода.

Миграцию данных при переходе к Active Directory необходимо сопровождать их *резервным копированием*.

При установке Active Directory выполняются следующие функции:

- Добавление контроллера домена к существующему домену.
- Создание первого контроллера домена в новом домене.
- Создание нового дочернего домена.
- Создание нового дерева домена.
- Установка DNS-сервера.
- Создание БД и журналов БД.
- Создание общего системного тома.

Существуют два режима домена - смешанный и основной. Изменение режима домена возможно лишь в одном направлении - из смешанного режима в основной режим, но не наоборот. При изменении режима со смешанного на основной происходит следующее:

- прекращается поддержка репликации нижнего уровня, после чего в этом домене запрещается иметь контроллеры, не работающие под управлением Windows 2000/2003 Server;
- запрещается добавление новых контроллеров нижнего уровня в данный *домен*;
- сервер, исполнявший роль основного контроллера домена, перестает быть таковым, поэтому все контроллеры становятся равноправными.

Согласно плану проведения развертывания, все решения должны предварительно тестироваться на стенде, развернутом на оборудовании в тестовой среде. В тестовой среде компании создается модель, идентичная модели промышленной среды либо ее фрагментам.

Тестирование проводится в соответствии с процедурами и сценариями тестирования (осуществляется функциональное и нагрузочное тестирование), одной из его целей является проверка отказоустойчивости решения с высоким показателем надежности.

На следующих этапах создания стенда необходимо протестировать:

- Распределение ролей между серверами.
- Работу сервиса *DNS*, установленного на серверах.
- Прохождение репликации между контроллерами доменов.
- Настройку соединения между контроллерами доменов.
- Добавление контроллера домена в Internet VLAN.
- Перенос баз WINS и DHCP.
- Аутентификацию пользователей на контроллере.

Далее процесс тестирования можно описать следующим образом:

- Тестирование реструктуризации домена.
- Тестирование переноса баз DHCP, WINS.

- Тестирование многосайтовой конфигурации физической топологии Active Directory.

После завершения тестовой эксплуатации осуществляется перенос данных из существующей структуры промышленной среды компании в спроектированную структуру Active Directory.

Модель репликации, используемая в Active Directory, представляет модель с нежестким согласованием, обладающую сходимостью.

- *Репликация* не является жестко согласованной, так как контроллеры домена, содержащие реплику раздела, не всегда имеют идентичную информацию.
- Процесс репликации всегда сходится, то есть если система поддерживается в стационарном состоянии, без внесения новых изменений к каталогу в течение некоторого времени, то все контроллеры домена достигнут единообразного состояния и будут иметь идентичную информацию.

Виды репликации: внутрисайтовая (между контроллерами домена одного сайта) и межсайтовая (между контроллерами домена, относящимися к разным сайтам).

Хранимая в каталоге информация делится на три категории, которые называются разделами каталога, и служит объектом репликации:

- информация о схеме;
- информация о конфигурации;
- данные домена.

Схема и конфигурация реплицируются на все контроллеры домена в дереве или лесе.

Все данные определенного домена реплицируются на каждый контроллер именно этого домена. Все объекты каждого домена, а также часть свойств всех объектов в лесе реплицируются в глобальный каталог.

Контроллер домена хранит и реплицирует:

- информацию о схеме дерева доменов или леса;
- информацию о конфигурации всех доменов в дереве или лесе;
- все объекты и их свойства для своего домена.

Глобальный каталог хранит и реплицирует:

- информацию о схеме в лесе;
- информацию о конфигурации всех доменов в лесе;
- часть свойств всех объектов каталога в лесе (реплицируется только между серверами глобального каталога);
- все объекты каталога и все их свойства для того домена, в котором расположен глобальный каталог.

Обмен данными из каталога производится с помощью разных сетевых протоколов, таких как IP или SMTP.

- **IP-репликация**. Использует удаленный вызов процедур (Remote Procedure Call, RPC) для репликации через связи сайтов (межсайтовой) и внутри сайта (внутрисайтовой).
- **SMTP-репликация**. Производится только через связи сайтов (межсайтовая), но не в пределах сайта.

Существуют два типа обновлений информации Active Directory, касающейся определенного контроллера домена - исходное обновление (originating update) и реплицируемое обновление (replicated update).

При планировании сайтов должны быть решены две задачи:

- оптимизация трафика регистрации рабочей станции;
- оптимизация репликации каталогов.

Основные этапы настройки сайта:

- Создание сайта.
- Сопоставление подсети сайту.
- Подключение сайта с использованием связей сайта.
- Выбор лицензирующего компьютера для сайта.

Основные этапы настройки репликации между сайтами:

- Создание связи сайта.
- Настройка атрибутов связей сайта.
- Создание мостов связей сайта.

Выбор структуры сайтов определяется следующей информацией:

- информация о *физической структуре* сети;
- информация о логической архитектуре Active Directory.

Основные принципы, которых рекомендуется придерживаться при планировании структуры сайтов:

- Создавать сайт для LAN или группы LAN.
- Создавать сайт для каждого территориального участка с контроллером домена.
- Создавать сайт для участков с сервером, на котором выполняется приложение, работающее с данными о сайтах.

Ответственный за топологию сайтов выполняет следующие обязанности:

- Изменяет топологию сайтов в соответствии с изменениями в физической топологии сети.
- Отслеживает сведения о подсетях в сети: IP-адреса, маски подсетей и местонахождения подсетей.
- Наблюдает за сетевыми соединениями и задает цены связей между сайтами.

Поскольку проектирование сайта сильно зависит от организационной инфраструктуры сети, то необходимо осуществить документирование этой инфраструктуры:

- схемы топологии глобальной (WAN) и локальной сетей (LAN);
- список всех офисов компании, в которых компьютеры связаны через высокоскоростные сетевые соединения;
- количество пользователей, компьютеров, серверов и локальных подсетей IP для каждого офиса компании.

При проектировании структуры каждого сайта для организации можно следовать правилам, перечисленным далее.

1. Выяснить особенности физической среды.
2. Определить физические сети, формирующие домены.
3. Определить, какие участки сети планируется назначить сайтами.
4. Определить физические соединения сайтов.
5. Для каждого объекта межсайтовой связи задать расписание (график и интервал репликации) и стоимость.
6. Обеспечить избыточность конфигурированием моста связей сайтов.
7. Если назначены серверы-плацдармы для репликации каждого сайта, то должны быть идентифицированы все разделы Active Directory, которые будут расположены в сайте, и назначен сервер-плацдарм для каждого раздела.

В проектирование сайта входит определение мест размещения серверов, необходимых для обеспечения нужных служб каталога Active Directory:

- Размещение DNS-серверов.
- Размещение контроллеров домена.
- Размещение *серверов глобального каталога*.
- Размещение серверов хозяев операций.

В Active Directory можно создать пять типов учетных записей:

- Компьютер;
- Пользователь;
- Группа;
- InetOrgPerson;
- Контакт.

В Windows Server 2003 существует два основных типа учетных записей пользователей:

- локальные;
- доменные.

И на локальных компьютерах, и в доменах создается две ключевые учетные записи:

- Администратор (Administrator);
- Гость (Guest).

Есть несколько правил, которые нужно соблюдать при планировании стратегии именования пользователей. При планировании стратегии аутентификации (в том числе, управления паролями) рекомендуется соблюдать ряд правил.

При планировании групп могут использоваться следующие их типы групп и области действия:

- группы безопасности;
- группы распространения;
- глобальные группы;
- локальные группы домена;
- универсальные группы:

Группы пользователей помогают достичь наибольших успехов в стратегии управления учетными записями при выполнении следующих правил:

- избегать выдачи разрешений учетным записям;
- создавать локальные группы домена;
- для упорядочивания пользователей использовать глобальные группы;
- помещать глобальные группы в локальные группы домена;
- не включать пользователей в универсальные группы.

При планировании групповой политики существует два основных ее типа:

- конфигурация компьютера;
- конфигурация пользователя.

Вне зависимости от типа групповой политики имеется три следующие категории:

- параметры программ (Software Settings);
- параметры Windows (Windows Settings);
- административные шаблоны (Administrative Templates).

Поскольку GPO, применяемые к пользователю или компьютеру, могут поступать из нескольких источников, нужен способ определения того, в каком порядке эти GPO обрабатываются.

- Локальный GPO.
- GPO сайта.
- GPO домена.
- GPO OU.

В этой лекции было продолжено рассмотрение вопроса, как планировать службу Active Directory перед ее развертыванием.

В службе Active Directory домены имеют DNS-имена. При исследовании существующей инфраструктуры *DNS* необходимо выполнить следующие действия.

- Задокументировать все DNS-имена доменов, используемые в настоящее время в пределах компании.
- Задокументировать все дополнительные имена, которые компания зарегистрировала для возможности использования в Интернете.
- Задокументировать существующую конфигурацию серверов *DNS*.

Для внедрения Active Directory существуют два вида пространств имен (внутреннее и внешнее), при этом пространство имен Active Directory совпадает с заданным зарегистрированным пространством имен *DNS* или отличается от него.

После определения структуры домена организации и планирования доменного пространства имен необходимо разработать структуру организационных единиц (OU или подразделений - ОП). Организационное подразделение позволяет:

- отразить структуру компании и организации внутри домена;
- делегировать управление сетевыми ресурсами, но сохранить способность управлять ими;
- изменять организационную структуру компании;
- группировать объекты так, чтобы администраторы легко отыскивали сетевые ресурсы.

OU используются в определенных целях:

- Делегирование административного управления объектами.
- Ограничение видимости объектов.
- Управление применением групповой политики.

Можно использовать следующую классификацию для моделей структуры OU:

- Модель структуры OU на основе местоположения.
- Модель структуры OU на основе структуры организации.
- Модель структуры OU на основе функций.
- Смешанная модель структуры OU - сначала по местоположению, затем по структуре организации.
- Смешанная модель структуры OU - сначала по структуре, затем по местоположению.

17 СПИСОК ЛИТЕРАТУРЫ

1. **Active Directory Overview**
   Microsoft, 1999
2. **Technical Overview of Windows Server 2000 Active Directory**
   Microsoft, 1999
3. **Курс "Основы построения операционных систем промышленного назначения. Управление распределенными ресурсами".Active Directory ОС Windows Server 2003**
   IBM,2004
4. **Microsoft Windows 2000 Active Directory Services. Учебный курс MCSE** М.: ИТД "Русская Редакция", 2004
5. **Windows Server 2003: справка к продукту**
   Microsoft, 2005
6. Аллен Р
   Active Directory: сборник рецептов для профессионалов Windows Server 2003 и Windows 2000 СПб.: ИД "ПИТЕР", 2004
7. Гленн У., Симпсон М.Т
   Проектирование инфраструктуры Active Directory и сети на основе Microsoft Windows Server 2003 СПб.: ИД "ПИТЕР", 2005
8. Гусева А
   Сети и межсетевые коммуникации Windows 2000 М.: Издво "Диалог-МИФИ", 2002
9. Зубанов Ф
   Active Directory: миграция на платформу Microsoft Windows Server 2003 М.: ИТД "Русская Редакция", 2004
10. Зубанов Ф
    Active Directory: подход профессионала М.: ИТД "Русская Редакция", 2002
11. Корбин В
    Планирование, внедрение и поддержка инфраструктуры Microsoft Windows Server 2003 Active Directory М.:ЭКОМ, 2007
12. Крафт М., Спилман Дж., Хадсон К
    Планирование, внедрение и поддержка инфраструктуры Active Directory Windows Server 2003 СПб.: ИД "ПИТЕР", 2007
13. Малкер М., Реймер С
    Active Directory для Windows Server 2003 Справочник администратора М.: ЭКОМ, 2004
14. Олсен Г.Л
    Служба Active Directory Windows 2000: разработка и внедрение М.: Изд-во "Вильямс", 2001
15. Чекмарев А
    Windows 2000 Active Directory СПб.: Изд-во "BHV",2004