Служба каталогов Active Directory. Назначение службы каталогов. Логическая и физическая структура Active Directory.
http://www.intuit.ru/department/os/sysadmswin/6/

Современные сети часто состоят из множества различных программных платформ, большого разнообразия оборудования и программного обеспечения. Пользователи зачастую вынуждены запоминать большое количество паролей для доступа к различным сетевым ресурсам. Права доступа могут быть различными для одного и того же сотрудника в зависимости от того, с какими ресурсами он работает. Все это множество взаимосвязей требует от администратора и пользователя огромного количества времени на анализ, запоминание и обучение.

Решение проблемы управления такой разнородной сетью было найдено с разработкой службы каталога.

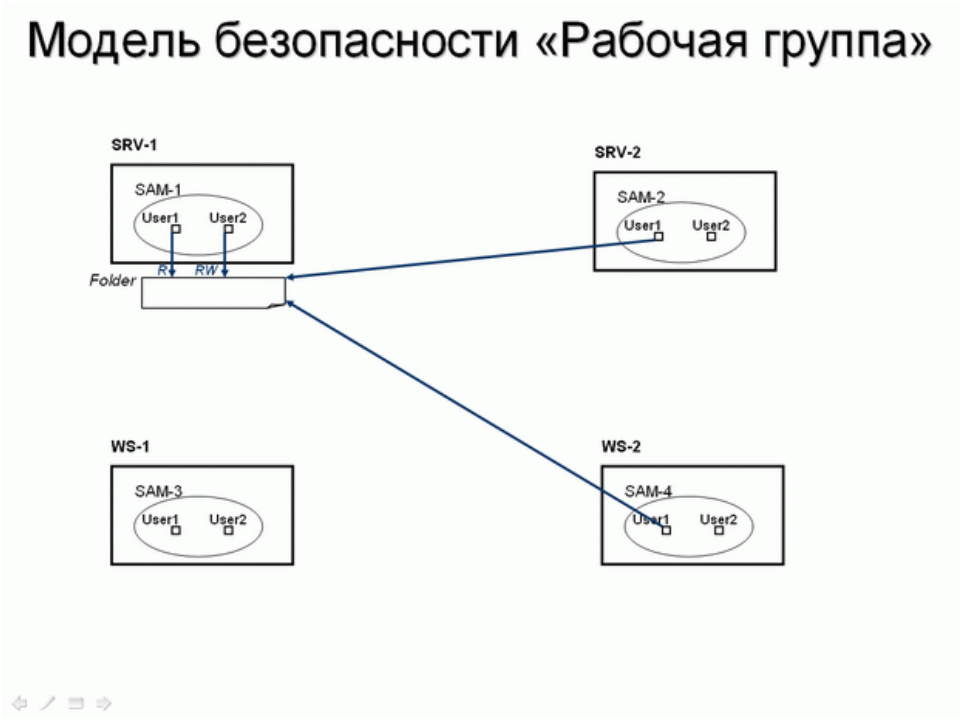
Информация о пользователе, заносится единожды в службу каталога, и после этого становится доступной в пределах всей сети. Любые изменения, занесенные в службу каталога администратором, сразу обновляются по всей сети.
Администраторам уже не нужно беспокоиться об уволенных сотрудниках — просто удалив учетную запись пользователя из службы каталога, он сможет гарантировать автоматическое удаление всех прав доступа на ресурсы сети, предоставленные ранее этому сотруднику.
Служба каталогов Active Directory является основой логической структуры корпоративных сетей, базирующихся на системе Windows. Служба каталогов Active Directory содержит в первую очередь объекты, на которых базируется система безопасности сетей Windows, — учетные записи пользователей, групп и компьютеров. Учетные записи организованы в логические структуры: домен, дерево, лес, организационные подразделения.

Модели управления безопасностью: модель "Рабочая группа" и централизованная доменная модель

Как уже говорилось выше, основное назначение служб каталогов — управление сетевой безопасностью. Основа сетевой безопасности — база данных учетных записей (accounts) пользователей, групп пользователей и компьютеров, с помощью которой осуществляется управление доступом к сетевым ресурсам. Прежде чем говорить о службе каталогов Active Directory, сравним две модели построения базы данных служб каталогов и управления доступом к ресурсам.

Модель "Рабочая группа"

Данная модель управления безопасностью корпоративной сети — самая примитивная. Она предназначена для использования в небольших одноранговых сетях (3–10 компьютеров) и основана на том, что каждый компьютер в сети с операционными системами Windows NT/2000/XP/2003 имеет свою собственную локальную базу данных учетных записей и с помощью этой локальной БД осуществляется управление доступом к ресурсам данного компьютера. Локальная БД учетных записей называется база данных SAM (Security Account Manager) и хранится в реестре операционной системы. Базы данных отдельных компьютеров полностью изолированы друг от друга и никак не связаны между собой.



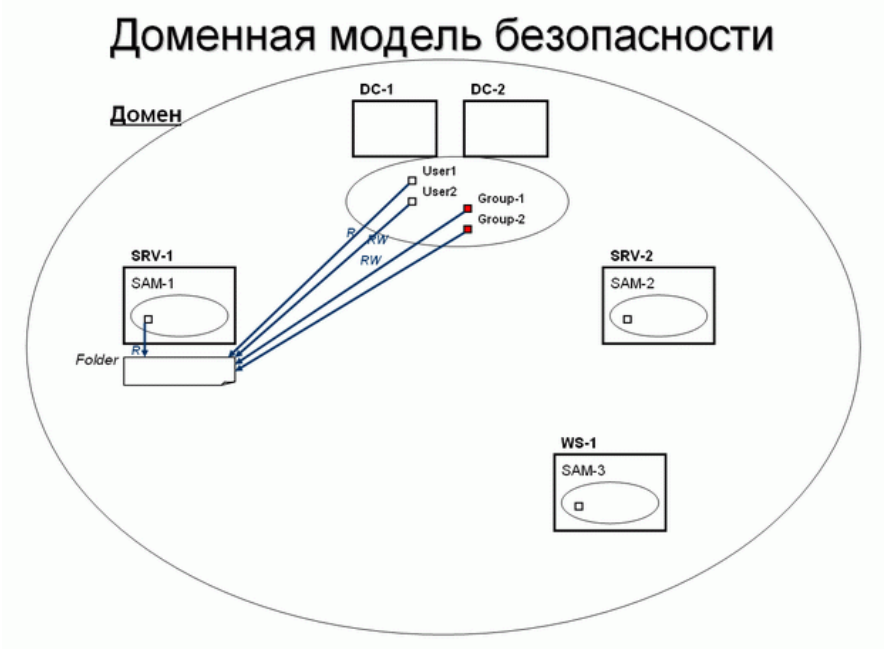
В данном примере изображены два сервера (SRV-1 и SRV-2) и две рабочие станции (WS-1 и WS-2). Их базы данных SAM обозначены соответственно SAM-1, SAM-2, SAM-3 и SAM-4 (на рисунке базы SAM изображены в виде овала). В каждой БД есть учетные записи пользователей User1 и User2. Полное имя пользователя User1 на сервере SRV-1 будет выглядеть как

"SRV-1\User1", а полное имя пользователя User1 на рабочей станции WS-1 будет выглядеть как "WS-1\User1". Представим, что на сервере SRV-1 создана папка Folder, к которой предоставлен доступ по сети пользователям User1 — на чтение (R), User2 — чтение и запись (RW). Главный момент в этой модели заключается в том, что компьютер SRV-1 ничего "не знает" об учетных записях компьютеров SRV-2, WS-1, WS-2, а также всех остальных компьютеров сети. Если пользователь с именем User1локально зарегистрируется в системе на компьютере, например, WS-2 (или, как еще говорят, "войдет в систему с локальным именем User1 на компьютере WS-2"), то при попытке получить доступ с этого компьютера по сети к папке Folder на сервере SRV-1 сервер запросит пользователя ввести имя и пароль (исключение составляет тот случай, если у пользователей с одинаковыми именами одинаковые пароли).

Модель "Рабочая группа" более проста для изучения, здесь нет необходимости изучать сложные понятия Active Directory. Но при использовании в сети с большим количеством компьютеров и сетевых ресурсов становится очень сложным управлять именами пользователей и их паролями — приходится на каждом компьютере (который предоставляет свои ресурсы для совместного использования в сети) вручную создавать одни и те же учетные записи с одинаковыми паролями, что очень трудоемко, либо делать одну учетную запись на всех пользователей с одним на всех паролем (или вообще без пароля), что сильно снижает уровень защиты информации. Поэтому модель "Рабочая группа" рекомендуется только для сетей с числом компьютеров от 3 до 10 (а еще лучше — не более 5), при условии что среди всех компьютеров нет ни одного с системой Windows Server.

Доменная модель

В доменной модели существует единая база данных служб каталогов, доступная всем компьютерам сети. Для этого в сети устанавливаются специализированные серверы, называемые контроллерами домена, которые хранят на своих жестких дисках эту базу. На рис. 6.2. изображена схема доменной модели. Серверы DC-1 и DC-2 — контроллеры домена, они хранят доменную базу данных учетных записей (каждый контроллер хранит у себя свою собственную копию БД, но все изменения, производимые в БД на одном из серверов, реплицируются на остальные контроллеры).



В такой модели, если, например, на сервере SRV-1, являющемся членом домена, предоставлен общий доступ к папке Folder, то права доступа к данному ресурсу можно назначать не только для учетных записей локальной базы SAM данного сервера, но, самое главное, учетным записям, хранящимся в доменной БД. На рисунке для доступа к папке Folder даны права доступа одной локальной учетной записи компьютера SRV-1 и нескольким учетным записям домена (пользователя и группам пользователей). В доменной модели управления безопасностью пользователь регистрируется на компьютере ("входит в систему") со своей доменной учетной записью и, независимо от компьютера, на котором была выполнена регистрация, получает доступ к необходимым сетевым ресурсам. И нет необходимости на каждом компьютере создавать большое количество локальных учетных записей, все записи созданы однократно в доменной БД. И с помощью доменной базы данных осуществляется централизованное управление доступом к сетевым ресурсам независимо от количества компьютеров в сети.

Назначение службы каталогов Active Directory

Каталог (справочник) может хранить различную информацию, относящуюся к пользователям, группам, компьютерам, сетевым принтерам, общим файловым ресурсам и так далее — будем называть все это объектами. Каталог хранит также информацию о самом объекте, или его свойства, называемые атрибутами. Например, атрибутами, хранимыми в каталоге о пользователе, может быть имя его руководителя, номер телефона, адрес, имя для входа в систему, пароль, группы, в которые он входит, и многое другое. Для того чтобы сделать хранилище каталога полезным для пользователей, должны

существовать службы, которые будут взаимодействовать с каталогом. Например, можно использовать каталог как хранилище информации, по которой можно аутентифицировать пользователя, или как место, куда можно послать запрос для того, чтобы найти информацию об объекте.

Служба каталогов Active Directory (сокращенно — AD) обеспечивает эффективную работу сложной корпоративной среды, предоставляя следующие возможности:

- Единая регистрация в сети; Пользователи могут регистрироваться в сети с одним именем и паролем и получать при этом доступ ко всем сетевым ресурсам и службам (службы сетевой инфраструктуры, службы файлов и печати, серверы приложений и баз данных и т. д.);
- Безопасность информации. Средства аутентификации и управления доступом к ресурсам, встроенные в службу Active Directory, обеспечивают централизованную защиту сети;
- Централизованное управление. Администраторы могут централизованно управлять всеми корпоративными ресурсами;
- Администрирование с использованием групповых политик. При загрузке компьютера или регистрации пользователя в системе выполняются требования групповых политик; их настройки хранятся в объектах групповых политик (GPO) и применяются ко всем учетным записям пользователей и компьютеров, расположенных в сайтах, доменах или организационных подразделениях;
- Интеграция с DNS. Функционирование служб каталогов полностью зависит от работы службы DNS. В свою очередь серверы DNS могут хранить информацию о зонах в базе данных Active Directory;
- Расширяемость каталога. Администраторы могут добавлять в схему каталога новые классы объектов или добавлять новые атрибуты к существующим классам;
- Масштабируемость. Служба Active Directory может охватывать как один домен, так и множество доменов, объединенных в дерево доменов, а из нескольких деревьев доменов может быть построен лес;
- Репликация информации. В службе Active Directory используется репликация служебной информации в схеме со многими ведущими (multi-master), что позволяет модифицировать БД Active Directory на любом контроллере домена. Наличие в домене нескольких контроллеров обеспечивает отказоустойчивость и возможность распределения сетевой нагрузки;
- Гибкость запросов к каталогу. БД Active Directory может использоваться для быстрого поиска любого объекта AD, используя его свойства (например, имя пользователя или адрес его электронной почты, тип принтера или его местоположение и т. п.);
- Стандартные интерфейсы программирования. Для разработчиков программного обеспечения служба каталогов предоставляет доступ ко всем возможностям (средствам) каталога и поддерживает принятые стандарты и интерфейсы программирования (API).

В Active Directory может быть создан широкий круг различных объектов. Объект представляет собой уникальную сущность внутри Каталога и обычно обладает многими атрибутами, которые помогают описывать и распознавать его. Учетная запись пользователя является примером объекта. Этот тип объекта может иметь множество атрибутов, таких как имя, фамилия, пароль, номер телефона, адрес и многие другие. Таким же образом общий принтер тоже может быть объектом в Active Directory и его атрибутами являются его имя, местоположение и т.д. Атрибуты объекта не только помогают определить объект, но также позволяют вам искать объекты внутри Каталога.

Домен

Основной единицей системы безопасности Active Directory является домен. Домен формирует область административной ответственности. База данных домена содержит учетные записи пользователей, групп и компьютеров. Большая часть функций по управлению службой каталогов работает на уровне домена (аутентификация пользователей, управление доступом к ресурсам, управление службами, управление репликацией, политики безопасности).

Имена доменов Active Directory формируются по той же схеме, что и имена в пространстве имен DNS. И это не случайно. Служба DNS является средством поиска компонент домена — в первую очередь контроллеров домена.

Контроллеры домена — специальные серверы, которые хранят соответствующую данному домену часть базы данных Active Directory. Основные функции контроллеров домена:

- **хранение БД Active Directory** (организация доступа к информации, содержащейся в каталоге, включая управление этой информацией и ее модификацию);
- **синхронизация изменений в AD** (изменения в базу данных AD могут быть внесены на любом из контроллеров домена, любые изменения, осуществляемые на одном из контроллеров, будут синхронизированы с копиями, хранящимися на других контроллерах);
- **аутентификация пользователей** (любой из контроллеров домена осуществляет проверку полномочий пользователей, регистрирующихся на клиентских системах).

Настоятельно рекомендуется в каждом домене устанавливать не менее двух контроллеров домена — во-первых, для защиты от потери БД Active Directory в случае выхода из строя какого-либо контроллера, во-вторых, для распределения нагрузки между контроллерами.

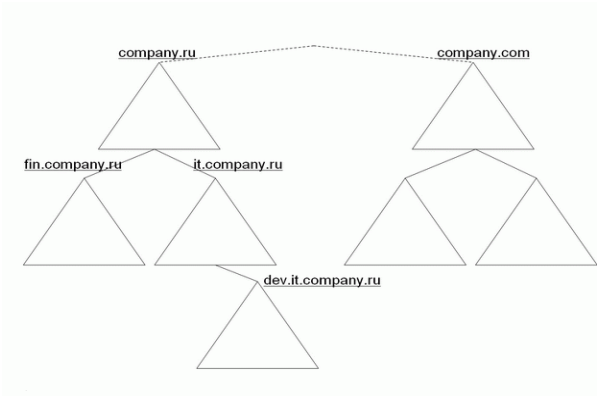
Дерево

Дерево является набором доменов, которые используют единое связанное пространство имен. В этом случае "дочерний" домен наследует свое имя от "родительского" домена. Дочерний домен автоматически устанавливает двухсторонние транзитивные доверительные отношения с родительским доменом. Доверительные отношения означают, что ресурсы одного из доменов могут быть доступны пользователям других доменов.

Пример дерева Active Directory изображен на рис. 6.3. В данном примере домен company.ru является доменом Active Directory верхнего уровня. От корневого домена отходят дочерние домены it.company.ru и fin.company.ru. Эти домены могут относиться соответственно к ИТ-службе компании и финансовой службе. У домена it.company.ru есть поддомен dev.it.company.ru, созданный для отдела разработчиков ПО ИТ-службы.

Корпорация Microsoft рекомендует строить Active Directory в виде одного домена. Построение дерева, состоящего из многих доменов необходимо в следующих случаях:

- для децентрализации администрирования служб каталогов (например, в случае, когда компания имеет филиалы, географически удаленные друг от друга, и централизованное управление затруднено по техническим причинам);
- для повышения производительности (для компаний с большим количеством пользователей и серверов актуален вопрос повышения производительности работы контроллеров домена);
- для более эффективного управления репликацией (если контроллеры доменов удалены друг от друга, то репликация в одном может потребовать больше времени и создавать проблемы с использованием несинхронизированных данных);
- для применения различных политик безопасности для различных подразделений компании;
- при большом количестве объектов в БД Active Directory.



Лес

Наиболее крупная структура в Active Directory. Лес объединяет деревья, которые поддерживают единую схему (схема Active Directory — набор определений типов, или классов, объектов в БД Active Directory). В лесу между всеми доменами установлены двухсторонние транзитивные доверительные отношения, что позволяет пользователям любого домена получать доступ к ресурсам всех остальных доменов, если они имеют соответствующие разрешения на доступ. По умолчанию, первый домен, создаваемый в лесу, считается его корневым доменом, в корневом домене хранится схема AD.

Новые деревья в лесу создаются в том случае, когда необходимо построить иерархию доменов с пространством имен, отличным от других пространств леса. В примере на рис. 6.3 российская компания могла открыть офис за рубежом и для своего зарубежного отделения создать дерево с доменом верхнего уровня company.com. При этом оба дерева являются частями одного леса с общим "виртуальным" корнем.

При управлении деревьями и лесами нужно помнить два очень важных момента:

- первое созданное в лесу доменов дерево является корневым деревом, первый созданный в дереве домен называется корневым доменом дерева (tree root domain);
- первый домен, созданный в лесу доменов, называется корневым доменом леса (forest root domain), данный домен не может быть удален (он хранит информацию о конфигурации леса и деревьях доменов, его образующих).

Организационные подразделения (ОП).

Организационные подразделения (Organizational Units, OU) — контейнеры внутри AD, которые создаются для объединения объектов в целях делегирования административных прав и применения групповых политик в домене. ОП существуют только внутри доменов и могут объединять только объекты из своего домена. ОП могут быть вложенными друг в друга, что позволяет строить внутри домена сложную древовидную иерархию из контейнеров и осуществлять более гибкий административный контроль. Кроме того, ОП могут создаваться для отражения административной иерархии и организационной структуры компании.

Глобальный каталог

Глобальный каталог является перечнем всех объектов, которые существуют в лесу Active Directory. По умолчанию, контроллеры домена содержат только информацию об объектах своего домена. Сервер Глобального каталога является контроллером домена, в котором содержится информация о каждом объекте (хотя и не обо всех атрибутах этих объектов), находящемся в данном лесу.

Логическая структура Active Directory

Служба каталогов Active Directory организована в виде иерархической структуры, построенной из различных компонентов, которые представляют элементы корпоративной сети. В этой структуре есть, например, пользовательские объекты, компьютерные объекты, и различные контейнеры. Способ организации этих элементов представляет собой логическую структуру Active Directory в корпоративной сети. Логическая структура Active Directory включает в себя леса, деревья, домены и Организационные подразделения (ОП). Каждый из элементов логической структуры описан ниже.

Домен — логическая группа пользователей и компьютеров, которая поддерживает централизованное администрирование и управление безопасностью. Домен является единицей безопасности – это означает, что администратор для одного домена, по умолчанию, не может управлять другим доменом. Домен также является основной единицей для репликации — все контроллеры одного домена должны участвовать в репликации друг с другом. Домены в одном лесу имеют автоматически настроенные доверительные отношения, что позволяет пользователям из одного домена получать доступ к ресурсам в другом. Необходимо также знать, что можно создавать доверительные отношения с внешними доменами, не входящими в лес.

Дерево является набором доменов, которые связаны отношениями "дочерний"/"родительский", а также используют связанные (смежные, или прилегающие) пространства имен. При этом дочерний домен получает имя от родительского. Например, можно создать дочерний домен, называемый it, в домене company.com, тогда его полное имя будет it.company.com (рис. 6.33). Между доменами автоматически устанавливаются двухсторонние транзитивные доверительные отношения (домен it.company.com доверяет своему "родительскому" домену, который в свою очередь "доверяет" домену sales.company.com – таким образом, домен it.company.com доверяет домену sales.company.com, и наоборот). Это означает, что доверительные отношения могут быть использованы всеми другими доменами данного леса для доступа к ресурсам данного домена. Заметим, что домен it.company.com продолжает оставаться самостоятельным доменом, в том смысле, что он остается единицей для управления системой безопасности и процессом репликации. Поэтому, например, администраторы из домена sales.company.com не могут администрировать домен it.company.com до тех пор, пока им явно не будет дано такое право.

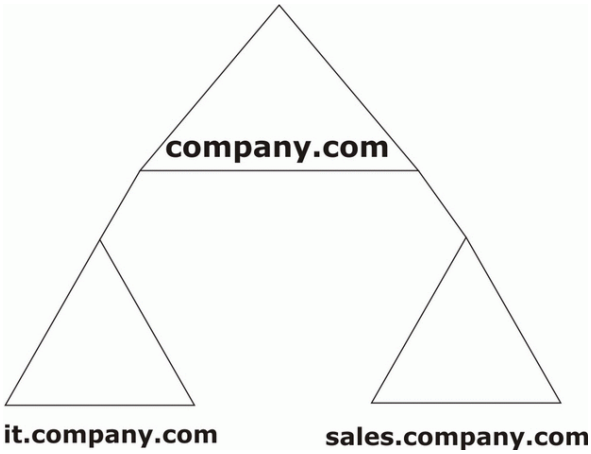


Рис. 6.33.

Лес — это одно или несколько деревьев, которые разделяют общую схему, серверы Глобального каталога и конфигурационную информацию. В лесу все домены объединены транзитивными двухсторонними доверительными отношениями.

Каждая конкретная инсталляция Active Directory является лесом, даже если состоит всего из одного домена.

Организационное подразделение (ОП) является контейнером, который помогает группировать объекты для целей администрирования или применения групповых политик. ОП могут быть созданы для организации объектов в соответствии с их функциями, местоположением, ресурсами и так далее. Примером объектов, которые могут быть объединены в ОП, могут служить учетные записи пользователей, компьютеров, групп и т.д. Напомним, что ОП может содержать только объекты из того домена, в котором они расположены.

Подводя итог, можно сказать, что логическая структура Active Directory позволяет организовать ресурсы корпоративной сети таким образом, чтобы они отражали структуру самой компании.

Физическая структура Active Directory

Физическая структура Active Directory служит для связи между логической структурой AD и топологией корпоративной сети.

Основные элементы физической структуры Active Directory — контроллеры домена и сайты.

Контроллеры домена были подробно описаны в предыдущем разделе.

Сайт — группа IP-сетей, соединенных быстрыми и надежными коммуникациями. Назначение сайтов — управление процессом репликации между контроллерами доменов и процессом аутентификации пользователей. Понятие "быстрые коммуникации" очень относительное, оно зависит не только от качества линий связи, но и от объема данных, передаваемых по этим линиям. Считается, что быстрый канал — это не менее 128 Кбит/с (хотя Microsoft рекомендует считать быстрыми каналы с пропускной способностью не менее 512 Кбит/с).

Структура сайтов никак не зависит от структуры доменов. Один домен может быть размещен в нескольких сайтах, и в одном сайте могут находиться несколько доменов (рис. 6.34).

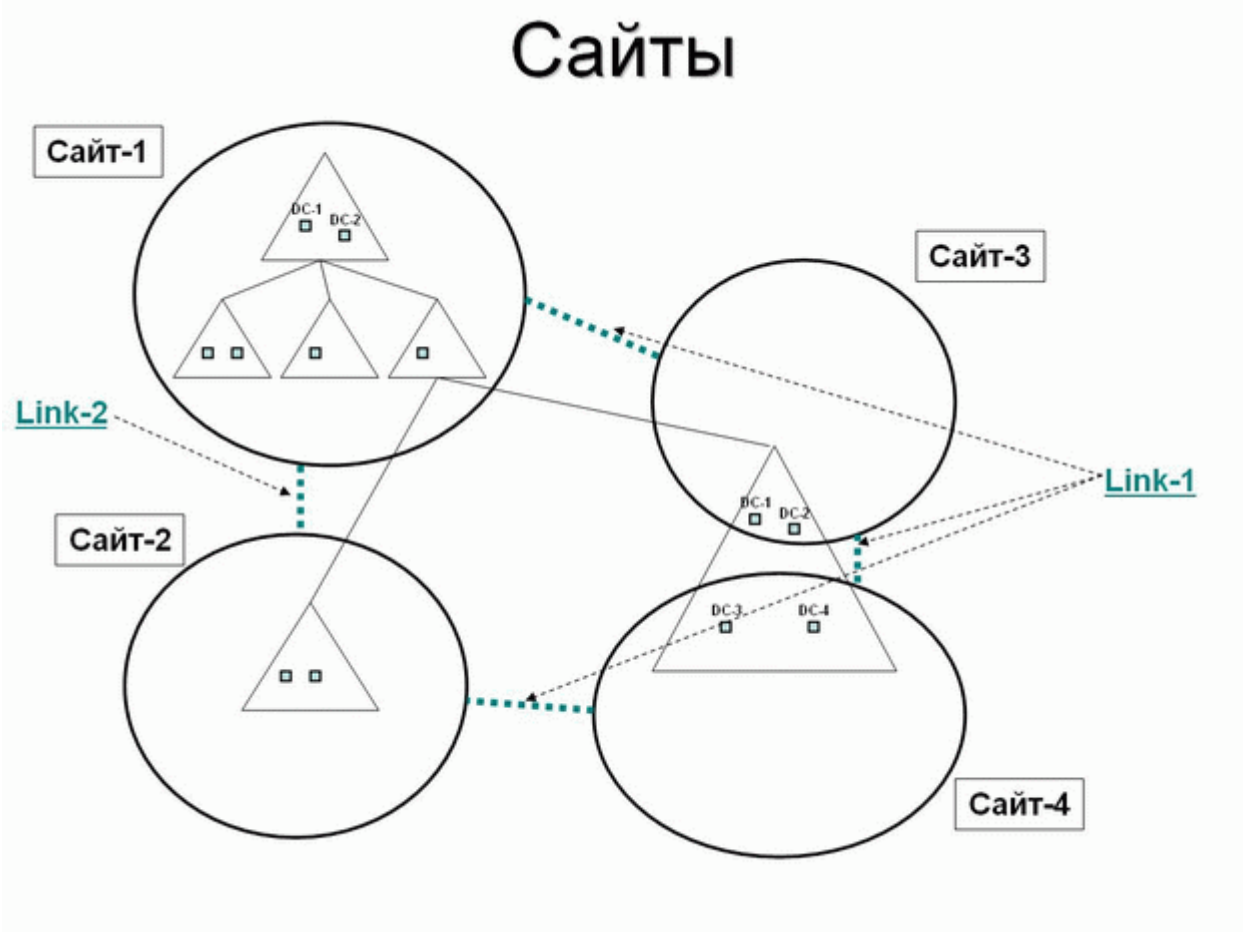


Рис. 6.34.