Администрирование информационных систем

Домены Windows
Active Directory

Службы каталогов

- Основная цель объединения компьютеров в вычислительную сеть – обеспечение совместного использования ресурсов.
- Одна из основных решаемых задач – реализация оптимального метода организации общих ресурсов.
- В крупной организации речь идет о множестве ресурсов и множестве потребителей данных ресурсов. Для эффективного управления такими списками применяются разные методы. Один из методов – развертывание *службы каталогов*.
- Служба каталогов – сетевая служба позволяющая пользователям получить доступ к ресурсу без знания точного месторасположения ресурса.
- При использовании службы каталогов вся информация об объектах сети объединяется в каталог (directory).
- Внутри каталога объекты организуются в соответствии с физической или логической структурой сети.

Службы каталогов

- Службы каталогов решают следующие задачи:
  - **Управление сетевыми ресурсами**. Служба каталогов облегчает пользователям поиск необходимых ресурсов, скрывая подробности реализации механизма поиска.
  - **Управление пользователями**. Каждый пользователь в сети идентифицируется набором реквизитов. Это позволяет осуществлять управление доступом к сетевым ресурсам.
  - **Управление приложениями**. В крупных вычислительных сетях возникает задача централизованного управления программным обеспечением, включая развертывание новых приложений и обновление существующих.
  - **Обеспечение функционирования сети**. Использование службы каталогов позволяет решить вопросы выделения IP-адресов, других параметров сети.
- **Сети Microsoft организуются с использованием службы каталогов Active Directory.**

Пространство имен X.500 и протокол LDAP

- Пространство имен (в соответствии со стандартом X.500) представляет собой иерархическую структуру имен, которая идентифицирует уникальный путь к контейнеру службы каталога.
- Это пространство имен определяется в числовой (точечной) нотации или в строковой.
- В строковой нотации пользовательский объект представляемый как:
  - cn=Dmitry, cn=Users, dc=Rosnou, dc=ru
  - Для удовлетворения требованию уникальности в пространстве имен X.500 в домене Rosnou.ru в контейнере Users может быть единственное имя Dmitry.

Протокол LDAP

- Протокол LDAP (облегченный протокол службы каталогов) является протоколом доступа. В данном протоколе для именования объектов используется система *характерных имен (Distinguish Name)*, предоставляющая информацию обо всех узлах дерева каталогов.
- Представление иерархии имен LDAP имеет вид:
  - LDAP: // cn=Dmitry, cn=Users, ou=faculty, dc=Rosnou, dc=ru
  - При записи характерного имени используются специальные ключевые слова:
    - DC – составная часть доменного имени;
    - OU – организационная единица;
    - CN – общее имя.
  - Имя, идентифицирующее сам объект, согласно терминологии LDAP, выступает в качестве относительного характерного имени. Относительное имя может быть не уникальным в рамках всего дерево, но должно быть уникальным в пределах контейнера.
  - *Каноническое имя* подобно характерному имени, за исключением того, что опускаются сокращения, обозначающие тип контейнера:
    - Rosnou.ru/faculty/Users/Dmitry

Использование имен объектов системы

- Другой способ именования объектов – использование *основных имен* субъектов системы безопасности.
- Основное имя субъекта системы безопасности имеет вид:
  - <имя субъекта>@<суффикс основного имени>
  - В качестве суффикса основного имени выступает имя домена, которому принадлежит данный субъект
  - Пример основного имени пользователя:
    - dmitry@rosnou.ru
- Глобальные идентификаторы. Для обеспечения уникальности объектов и облегчения поиска, каждому объекту ставится в соответствие 128-разрядное число – *глобальный уникальный идентификатор.*
- Данный идентификатор является обязательным атрибутом любого объекта, который не изменяется ни при каких обстоятельствах.

Доменная модель службы каталогов

- В рамках каталога Active Directory одним из основных понятий является понятие **домена** – совокупность компьютеров, характеризующихся наличием общей базы учетных записей пользователей и единой политики безопасности.
- Использование доменов позволяет разделить пространство имен на несколько фрагментов. Каждый объект может принадлежать **только** одному домену.
- Цели создания доменов:
  - **Разграничение административных полномочий.**
  - **Создание единой политики безопасности.**
  - **Разделение доменного контекста имен.**
- Центральным компонентом домена выступают серверы, хранящие фрагменты каталогов. Такие серверы называются **контроллерами домена**.

Иерархия доменов

- Windows позволяет организовать разные типа иерархии доменов.
  - Отношение между доменами по схеме «родитель-потомок». Имя дочернего домена включает в себя имя родительского домена.
  - Отношения, включающие несколько связанных деревьев – лес доменов (forest).

Доверительные отношения

- Для объединения объектов, хранящихся в разных доменов должны существовать определенные связи – *доверительные отношения*.
- Механизм установленных доверительных отношений позволяет организовать процесс аутентификации объектов и субъектов системы.
- Выделяют два типа доверительных отношений:
  - **Односторонние доверительные отношения**
  - **Двусторонние доверительные отношения**

Контроллеры домена

- Контроллеры домена в доменах Windows отвечают за аутентификацию пользователей и содержат фрагмент каталога.
- Некоторые операции могут выполняться только одним контроллером. Эти операции называются *операции с одним исполнителем (flexible single-master operations – FSMO).*
- Контроллеры доменов могут выполнять специализированные роли:
  - **Роли, требующие уникальности в пределах всего леса доменов:**
    - **Исполнитель роли владельца доменных имен**
    - **Исполнитель роли владельца схемы**
  - **Роли, требующие уникальности в пределах домена:**
    - **Исполнитель роли владельца идентификаторов**
    - **Исполнитель роли эмулятора основного контроллера домена**
    - **Исполнитель роли владельца инфраструктуры каталога.**
- По умолчанию все данные роли возлагаются на первый контроллер домена, установленный в лесе.
- Процесс принудительной передачи функций специализированной роли другому контроллеру называется *захватом роли*.

Разделы каталога

- В рамках каталога Active Directory выделяется несколько крупных фрагментов каталога – *разделов каталога*, представляющих законченные непрерывные поддеревья (контексты имен):
  - **Доменный раздел каталога**
  - **Раздел схемы каталога**
  - **Раздел конфигурации**
  - **Разделы приложений**
  - **Раздел глобального каталога**

Схема каталога

- Любой объект каталога принадлежит к некоторому классу объектов со своей структурой атрибутов.
- Определения всех классов объектов и совокупности правил, позволяющих управлять структурой каталога, хранится в специальной иерархической структуре – *схеме каталога*.
- Все данные схемы хранятся в виде двух классов объектов:
  - *Class Schema* – класс, определяющий типы объектов
  - *Attribute Schema* – класс, определяющий атрибут объекта. Каждый атрибут определяется в схеме один раз и может использоваться при описании множества классов объектов.
- Схема каталога хранится в отдельном разделе и допускает возможность расширения.

Раздел глобального каталога

- *Глобальный каталог* – специализированная база данных, содержащая фрагменты всех доменных контекстов имен.
- Для исключения чрезмерного разрастания базы данных в нее включены значения только наиболее часто используемых атрибутов.
- Контроллер домена, выступающий в качестве носителя такой базы данных, называется *сервером глобального каталога*. Он выполняется следующие функции:
  - *Предоставление пользователям возможности поиска объектов в лесу доменов по атрибутам*
  - *Разрешение основного имени пользователя*
  - *Предоставление информации о членстве пользователя в различных группах с универсальной областью действия.*
- В лесу доменов присутствует по крайней мере один сервер глобального каталога. По умолчанию это первый контроллер созданный в домене.

Другие разделы

- **Раздел конфигурации** – используется для размещения сведений о структуре системы: список всех доменов и деревьев леса, перечень существующих контроллеров домена и серверов глобального каталога.
- **Доменный раздел** – используется для размещения объектов, являющихся непосредственно частью домена. Здесь хранятся объекты, ассоциированные с пользователями, компьютерами, общими ресурсами. Данный раздел передается в рамках домена.
- **Разделы приложений** – могут быть созданы для различных сетевых приложений. Разделы могут быть созданы администратором вручную или самими приложениями при помощи интерфейса программирования ADSI (Active Directory Service Interfaces). Создание таких разделов позволяет обращаться к приложениям используя общий подход доменных имен.

Организационные единицы

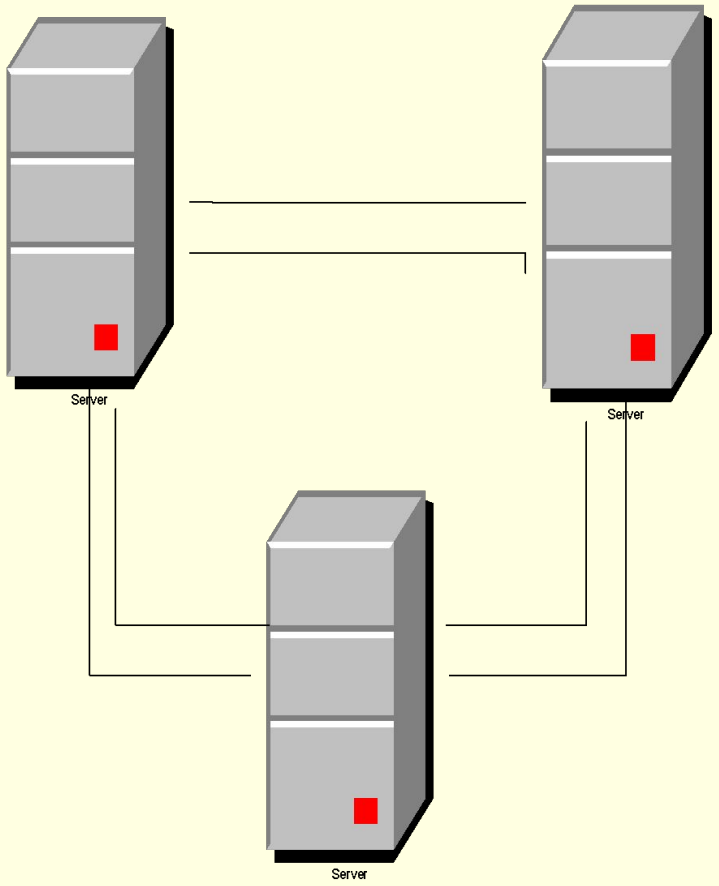
- В структуре службы каталога можно использовать специальные объекты контейнерного типа, позволяющие группировать объекты. Такими объектами являются *организационные единицы*, позволяющие объединять объекты в логическую структуру. Используются для упрощения управления входящими в них объектами.
- Иерархия организационных единиц образуется только в пределах домена. Организационные единицы принадлежащие разным доменам леса не связаны друг сдругом.

Физическая структура каталога. Репликация данных.

- Корпоративная сеть – совокупность подсетей, соединенных между собой линиями связи.
- Под узлом (site) в сетях Windows понимается совокупность подсетей объединенных высокоскоростными линиями связи.
- В структуре каталога существует специальный класс объектов, описывающий связи между узлами, - *соединение узлов.*
- Каждое соединение как объект каталога имеет следующие атрибуты:
  - Стоимость соединения
  - Расписание доступности соединения
  - Интервал репликации
  - Транспорт репликации
    - В качестве транспорта используются протоколы RPC и SMTP

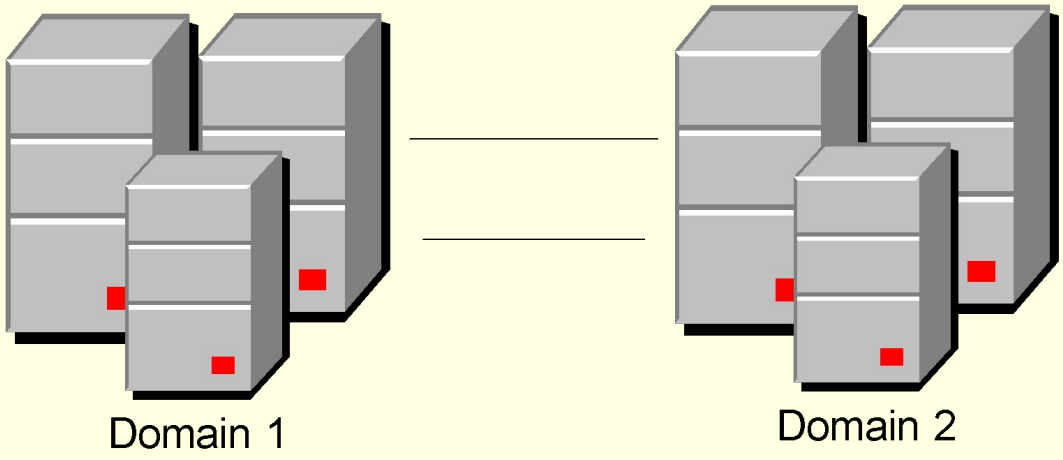
Репликация внутри узла

- При репликации баз данных каталога внутри узла осуществляется автоматически. В процессе репликации используется кольцевая топология (двунаправленное кольцо).
- В процессе репликации применяется протокол RPC. Используется *синхронное взаимодействие* – принимающий партнер, отправляя запрос, ожидает ответа от передающего партнера.



Репликации между узлами

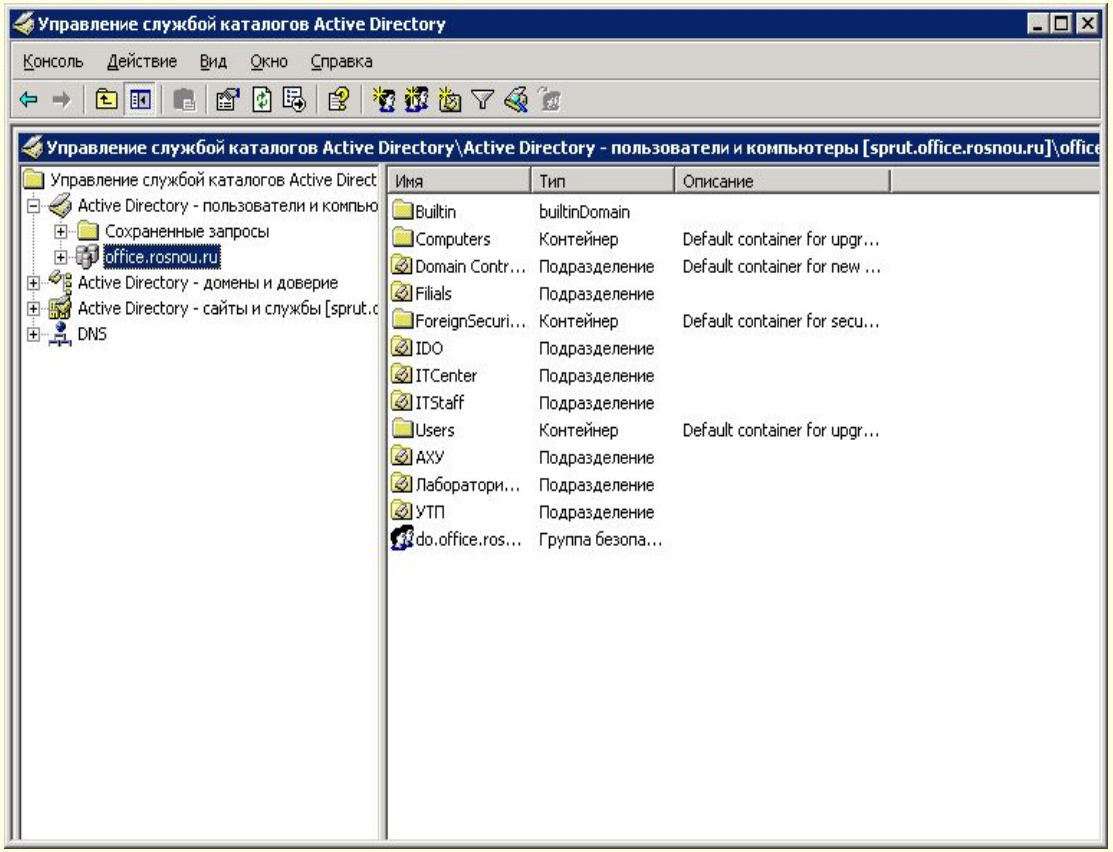
- Одной из причин объединения подсетей в узлы – необходимость управления процессом репликации между контроллерами домена на медленных линиях связи.
- В процессе репликации между узлами передается только информация об изменениях в схеме и данных конфигурации. Для серверов глобального каталога – данные о подмножестве объектов всех доменов, образующих лес.
- При передаче используются два протоколы: RPC и SMTP – для асинхронного взаимодействия.
- При репликации между узлами существенную роль играют *мостовые серверы*.



Управление службой Active Directory

- Для управления службой каталогов Active Directory используются специальные средства администрирования.

- Утилиты администрирования службы каталогов:
  - . Active Directory – пользователи и компьютеры
  - Active Directory – домены и доверие
  - Active Directory – сайты и службы



Управление службой Active Directory

- Оснастка «Active Directory — сайты и службы» является консолью управления Microsoft Management Console, которую можно использовать для администрирования репликации данных каталога.
- Другими средствами управления Active Directory являются программы командной строки.
- Программа **Ntdsutil** используется для обслуживания базы данных Active Directory, управления действиями одиночного хозяина операций и удаления метаданных, оставленных контроллерами домена, которые были удалены из сети без выполнения соответствующих операций