Основы Active Directory Domain Services

Тверской государственный технический университет
Прохныч А.Н.

Понятие каталога

- служба каталога существует очень давно
  - ✔ поиска объекта сети (файла, принтер)
  - ✔ аутентификации (учетные записи)
  - ✔ управление доступом к ресурсам
- начало 90-х
  - ✔ Novell Directory Services (NDS)
  - ✔ домен NT 4.0
    - линейная структура

Основные компоненты AD DS

Физические компоненты	Логические компоненты
Хранилище данных	Разделы
Контроллеры домена	Схема
Глобальный каталог	Домены
Read-only контроллеры домена (RODC)	Деревья
	Леса
	Сайты
	Организационные единицы (OU)

Хранилище данных AD DS

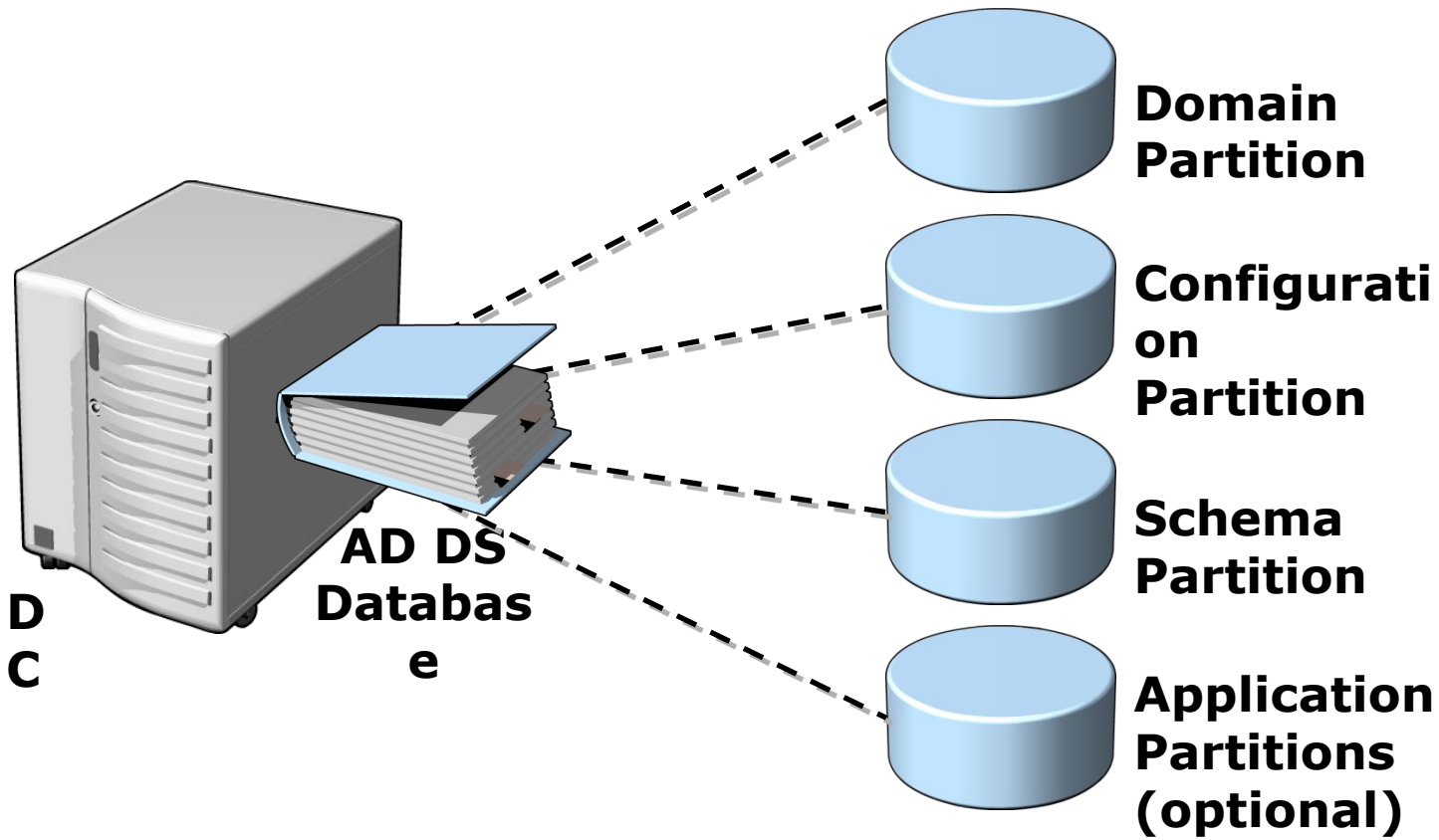
- содержит файлы базы данных
- процессы для хранения и управления информацией для пользователей, сервисов и приложений

- файл NTDS.dit
- %SystemRoot%\NTDS на всех контроллерах

Разделы AD DS

- необходимость хранения больших «кусков» определенной информации
- логическое понятие, объединение связанной информации
- основные разделы:
  - ✔ схема
  - ✔ конфигурация
  - ✔ домен

Разделы AD DS



Домен

- логический компонент каталога
- используется для группирования и управления объектами AD
  - ✔ пользователи, группы, все созданные объекты
  - ✔ уникальные учетные записи для объектов
- административная граница применения групповых политик
- репликационная граница для репликации данных между контроллерами
- аутентификационная и авторизационная граница
  - ✔ ограничение доступа к ресурсам

Аутентификация

- проверка «личности» пользователя, компьютера во время входа на компьютер или сетевой ресурс
- процедура проверки подлинности данных
  - ✔ проверки соответствия введённого пользователем пароля к учётной записи паролю в базе данных
  - ✔ проверка цифровой подписи письма по ключу шифрования
  - ✔ проверка контрольной суммы файла на соответствие заявленной автором этого файла

Авторизация

- предоставление определённому лицу или группе лиц прав на выполнение определённых действий
- процесс проверки (подтверждения) данных прав при попытке выполнения этих действий

Авторизация

- участники безопасности (security principal) получают уникальный идентификатор безопасности (SID) при создании учетной записи
- при аутентификации выдаются маркеры доступа (security token) включающий SID пользователя и SID все групп, членом которых он является
- ресурсы имеют список контроля доступа (ACL), которые определяют права на этом ресурсе
- сравнивается маркер безопасности со списком контроля доступа

Контроллер домена (DC)

- сервер с установленной ролью AD DS
  - ✔ располагается копия хранилища AD DS
  - ✔ обеспечивается репликация на другие контроллеры домена и леса
  - ✔ реализуются функции аутентификации и авторизации

Read-only контроллер домена (RODC)

- дополнительные контроллер домена
- содержит копию хранилища AD, доступную только на чтение
- однонаправленная репликация
  - ✔ только на себя
  - ✔ репликация с точностью до атрибута
    - выключаем копирование хешей паролей для критических учетных записей или сертификатов
- реализация контроллера домена в филиале

Прародитель AD DS

- домен Windows NT 4.0
  - ✔ единая центральная база безопасности
  - ✔ сетевой SAM (Security Account Manager)
  - ✔ добавили учетные записи для компьютеров (кто наши, а кто нет ☺)

Проблемы домена NT 4.0

- схема взаимодействия контроллеров домена
  - ✔ главные контроллер – PDC
    - запись и чтение
    - запись изменений в одну точку
    - он один – единственный и неповторимый
  - ✔ дополнительные – BDC
    - только чтение
    - репликация из одной точки
  - ✔ аналогично классическим DNS серверам

WINS сервера

- сервер имен WINS
  - ✔ NETBIOS имена
  - ✔ линейный список имен, а не отдельно по зонам, как DNS
  - ✔ список **реплицировался**
    - обмен измененными данными
    - timestamp для каждого объекта
    - двусторонний обмен в обе стороны
- модель взаимодействия –> Active Directory
- Windows Server 2000 (NT 5.0)
  - ✔ контроллеры равноправны
  - ✔ мультимастерная репликация

Замена WINS

- WINS использует короткие имена
  - ✔ 15 символов
- расширение функционала DNS
  - ✔ srv-записи (определение местоположения)
  - ✔ реализация механизма поиска ближайшего контроллера домена

Связь DNS и AD DS

- AD DS требует структуру DNS
- доменное имя AD DS должно быть DNS доменным именем
- записи контроллеров домена должны быть зарегистрированы в DNS
- DNS зоны можно интегрировать в базу Active Directory

Сайты AD DS

- проблема поиска ближайшего контроллера домена и обеспечение быстрой репликации
- домен NT – broadcast запрос
- **сайт** – представление сегмента сети
  - ✔ «географическое» подмножество
  - ✔ внутри быстрая и надежная связь
- по сути это LAN сеть – привязка к IP-подсетям
- используются для управления трафиком репликации
- назначение групповых политик всем компьютерам и пользователям определенного расположения

Хранение произвольных объектов

- домен NT4.0
  - ✔ фиксированный набор объектов и атрибутов
  - ✔ добавить новый нельзя
- **схема AD DS**

Схема AD DS

- это служебный раздел
- определяет каждый тип объекта в AD DS
- определяет набор атрибутов и их характеристик
- обеспечивает выполнение правил создания и конфигурации объекта

Схема AD DS

Тип объекта	Функции	Пример
Класс	Определяет, какие новые объекты могут быт созданы в каталоге	Класс пользователя Класс компьютера
Атрибут	Определяет какая информация может быть сохранена для каждого класса объектов	Display Name

Схема AD DS

- схема меняется редко
  - ✔ «тяжелый» софт (Exchange Server)
  - ✔ обновление с Windows Server 2003 или Windows Server 2008 AD до Windows Server 2012 AD DS
- идентичность схемы
  - – залог возможности обмена

Лес

- причины создания нескольких доменов
  - ✔ разделение базы безопасности
  - ✔ территориальное разделение филиалов
  - ✔ разделение репликации
- домен NT 4.0
  - ✔ трудно строить сложные структуры для больших организаций
  - ✔ доменной структуры не хватает
- термин **лес**

Лес

- экземпляр Active Directory
  - ✔ внутри несколько доменов
  - ✔ общая схема
  - ✔ общая база «лесных» настроек
  - ✔ конфигурация – служебный раздел с общими сведениями AD
  - ✔ **лес = организация (холдинг)**
- доверительные отношения между доменами
- общий глобальный каталог
  - ✔ для облегчения поиска

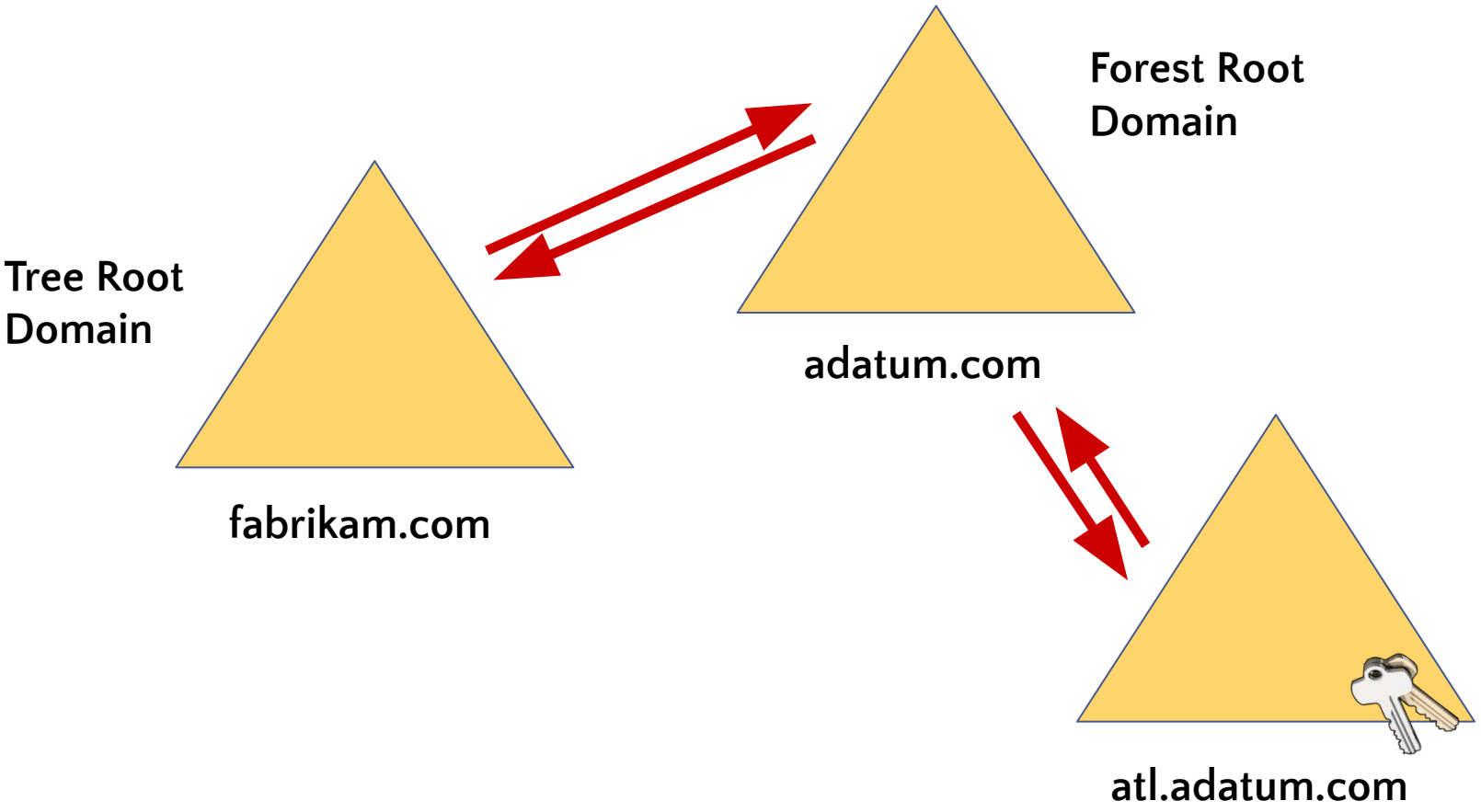
Деревья

- дерево – иерархия доменов в AD DS
- все домены в дереве:
  - ✔ содержат смежные пространства имен с родительским доменом
  - ✔ могут иметь дочерние домены
  - ✔ имеют двусторонние доверительные отношения с другими доменами в дереве

Деревья

- создание нового домена в лесу с т.з. DNS
  - ✔ новый домен находится в пространстве имен родителя
    - прописываем у родителя DNS делегирование – сведения о потомке
  - ✔ новый домен имеет отличное от «папиного» пространство имен
    - **Tree Root Domain**

Tree Root Domain



Организационные единицы (OUs)

- OU – более функциональный контейнер
- может содержать пользователей, группы, компьютеры и другие OU
- используются для:
  - ✔ структуризации – иерархического и логического представления объектов AD
  - ✔ управления коллекцией объектов
  - ✔ делегирование прав на администрирование группами объектов
  - ✔ применения политик