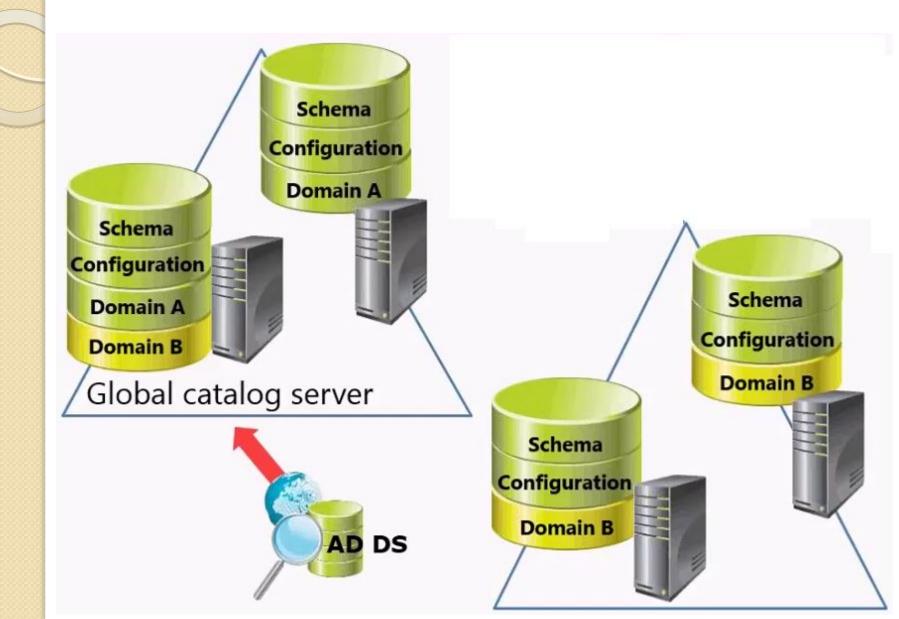


Глобальный каталог: История

- □ появился в Windows Server 2000
 - схемы не было
 - ✓ конфигурации не было
 - контроллер домена мог ответить
 на любой запрос относительно объектов
 Active Directory

Глобальный каталог



Глобальный каталог

- □ позволяет находить объекты в любом домене текущего леса
- хранит копии BCEX объектов Active
 Directory в лесу
 - ✓ полная копия всех объектов каталога своего домена
 - ✓ частичная копия всех объектов всех других доменов леса
- □ содержит основной, но не полный набор атрибутов объекта

Глобальный каталог

- □ копирование объектов в GC используется стандартная репликация
- ☐ значение параметра атрибутаisMemberOfPartialAttributeSet = true
 - ✓ оснастка «Схема Active Directory»
 - ✓ опция «Реплицировать этот атрибут в глобальный каталог»

Сервер Глобального каталога

- контроллеры домена, которые хранят копии глобального каталога
- □ создается автоматически на первом контроллере домена в лесу
- □ достаточно одного на сайт
- ☐ дополнительный контроллер домена можно назначить GC
 - ✓ оснастка «Сайты и службы Active Directory»
 - ✓ опция «Глобальный каталог»

Поиск объектов

- □ GC может ответить на любой запрос без перенаправления его контроллеру домена
- □ LDAР запросы через порт 3268
- □ параметр «Весь каталог» при поиске объекта
- □ GC содержит права доступа для объектов и атрибутов
 - ✓ нет прав объект не попадет в результат поиска по запросу

Проверка подлинности

- □ аутентификация пользователей из других доменов леса
- □ разрешает имя пользователя, если контроллер не знает «учетку»
 - ✓ «учетка» из одного домена, а компьютер из другого домена леса

Проверка членства в универсальных группах

- □ мультидоменная среда
- в универсальной группе могут быть члены из других доменов

Проверка ссылок на объекты внутри леса

- □ атрибут содержит ссылку на объект из другого домена
- для проверки ссылки контроллер домена использует GC

Поиск в адресной книге Exchange

- □ тесная интеграция Exchange и AD
- 🛮 поиск в Глобальной адресной книге
- 🛮 поиск пользователя по e-mail

Роли FSMO

Flexible single-master operations — «операции с одним исполнителем» определить «более равного» контроллера среди всех остальных равных разрешение конфликтных ситуаций «мастерская роль» — это просто признак в специальном объекте прописано, какой контроллер какими ролями владеет уникальные для леса уникальные для домена

Роли FSMO: уникальные для леса

- Domain Naming Master
 - ✔ Владелец доменных имён
- ☐ Schema Master
 - ✓ Владелец схемы

Роли FSMO: Domain Naming Master

- 🛮 добавление и удаление доменов
 - ✓ уникальность NETBIOS-имени
- □ создание и удаление разделов
 - ✓ собственные partitions
 - уникальность именования
- □ создание и удаление перекрестных ссылок
 - ✓ объекты класса crossRef
 - ✓ могут быть на домены вне леса
- □ одобрение переименования домена

Роли FSMO: Schema Master

□ «арбитр» при обнаружении конфликтов схем (к нему бегут два контроллера при обнаружении расхождения в схемах)
 □ может изменять схему (разрешена запись с схему)
 □ уведомляет остальных об изменении схемы
 □ при «падении» schema master просто не сможем менять схему и все ⊙, т.к. копия схемы у всех контроллеров леса

Роли FSMO: уникальные для домена

- ☐ RID Master
 - Владелец относительных идентификаторов
- ☐ Infrastructure Master
 - Владелец инфраструктуры домена
- ☐ PDC Emulator
 - Эмулятор основного контроллера домена

Роли FSMO: Infrastructure Master

- □ выполняет инспекцию всех «иностранцев» из другого домена
 - проверка изменения атрибутов пользователей из других доменов
 - ✓ поиск объектов неродного домена по GUID
- □ при одном домене не имеет смысла
- □ в многодоменной структуре IM не должен быть сервером GC

Роли FSMO: RID Master

- □ выделение последовательности уникальных RID`ов каждому контроллеру в домене
 - ✓ 500 номеров из общего пула
 - ссылки на идентификаторы
 - ✓ порог получения новой «пачки» 100
- □ обеспечивает корректность перемещения объектов между доменами

Роли FSMO: PDC Emulator

- до Windows 2000
 обеспечение совместимости с предыдущими версиями Windows
 - ✓ обработка операции «смена пароля»
 - ✓ репликация обновлений на ВDС
 - ✓ обозреватель сети (поиск сетевых ресурсов)

Роли FSMO: PDC Emulator

- ☐ c Windows Server 2000
 - сервер точного времени домене
 - изменение паролей и блокировка пользователей
 - «скоростная» репликация на PDC Emulator
 - «запасной» запрос на PDC Emulator
 - ✓ сохранение групповых политик в SYSVOL
 - ✓ изменения в пространстве имен Distributed File System (DFS)
 - управление «Встроенными участниками системы безопасности»
 - выполняется AdminSDHolder (владелец административных дескрипторов безопасности)