МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ

УНИВЕРСИТЕТ им. Р.Е.АЛЕКСЕЕВА

Институт радиоэлектроники и информационных технологий

Теория

по лабораторной работе №3

«Групповые политики, анализ и настройка безопасности Windows Server»

по дисциплине

«Программное обеспечение вычислительных сетей»

РУКОВОДИТЕЛЬ:

_____ __Кочешков А. А.__

(подпись) (фамилия, и.,о.)

СТУДЕНТ:

_____ __Сухоруков В.А.___

(подпись) (фамилия, и.,о.)

_____19-ВМ_____

(шифр группы)

Работа защищена «___»_____

С оценкой _____

Нижний Новгород 2022

12.Разделы AD, свойства системы репликации. Специализированные роли контроллеров домена FSMO

12.1. Разделы AD

Физически данные БД AD распределены и хранятся на контроллерах разных доменов.

Для управления размещением данных и процессами репликации в рамках всего каталога выделены ряд крупных контекстов имен. *Контекст имен* – связное законченное поддерево в общем пространстве имен.

Каждый раздел каталога используется для размещения отдельного вида информации.

- *Domain Partition* - доменный раздел каталога. В этом разделе содержатся данные обо всех объектах, принадлежащих к определенному домену. Реплицируется только в пределах своего домена. Индивидуален для каждого домена в лесу.
- *Schema Partition* – раздел схемы, данные обо всех типах объектов и их атрибутах (объявления классов), доступных в AD. Схема AD едина и общая для всех доменов. Реплицируется во всем лесу с владельца схемы.
- *Global Catalog Partition* – раздел глобального каталога. Управляется сервером глобального каталога. Реплицируется в лесу.

Сервер глобального каталога выполняет 3 главные функции:

- Поиск объекта в лесу доменов по одному или нескольким атрибутам. Например, атрибутами поиска объекта класса User могут быть Имя, Фамилия, Учетная запись, а результатом – DN объекта.
- Разрешение основного имени пользователя UPN. Обычный DC перенаправляет запрос на аутентификацию пользователя серверу ГК, а тот указывает DC, который может выполнить аутентификацию.
- Предоставление информации о членстве пользователя в группах с универсальной областью действия. Эта информация нужна для регистрации пользователя в системе.

В случае, если в процессе входа в систему пользователя, являющегося членом универсальной группы, сервер ГК окажется недоступным, система не получит данные, необходимые для его авторизации. Исключение: члены глобальной группы Администраторы домена могут входить в систему, даже когда ГК недоступен.

- *Configuration Partition* – раздел конфигурации, описывает топологию репликации между DC. Сам раздел реплицируется в лесу.
- *Application Partitions* – разделы приложений, в которых могут быть размещены данные самих сетевых приложений. Это возможность со стороны ADDS, а разработчики приложений могут ею воспользоваться для своих нужд.

Характерный пример – DNS сервер, интегрированный с AD, хранит свою базу данных записей DNS в выделенном разделе приложений AD.

В итоге, реплики раздела домена, раздела схемы и раздела конфигурации присутствуют в обязательном порядке на всех контроллерах доменов.

Доменный раздел индивидуален для каждого домена. Реплики разделов схемы и конфигурации одинаковы для всех контроллеров (read only).

12.2. Специализированные роли контроллеров домена.

Служба каталога Active Directory использует модель репликации с множеством равноправных участников. С точки зрения подсистемы репликации не имеет значения, какой из носителей осуществляет изменения в каталоге. Изменения могут быть произведены в любой из копий каталога. Однако существует определенный класс операций, которые должны выполняться только одним контроллером домена. Этот класс операций называется операциями с одним исполнителем (Flexible Single-Master Operations, FSMO). Если привлечь к выполнению подобных операций более одного контроллера домена, нельзя исключать возможность конфликтов. В определенных случаях подобные конфликты могут привести к нарушению целостности каталога. Имеется два типа операций с одним исполнителем, которые принято называть ролями контроллеров домена. От первого типа ролей требуется уникальность исполнителя в пределах всего леса доменов. Роль данного типа может быть возложена только на один контроллер в лесу доменов. К другому типу ролей предъявляется требование уникальности исполнителя только в пределах домена. В каждом домене может быть только один исполнитель роли. Таким образом, в рамках леса доменов исполнителей каждой из подобных ролей будет столько же, сколько и доменов, образующих лес. Рассмотрим пять существующих специализированных ролей.

- *Владелец схемы* (Schema Master). Контроллер домена, осуществляющий изменения в схеме каталога. Существование только одного владельца (хозяина) схемы в пределах леса доменов исключает возможность конфликтов, связанных с ее изменением. Отказ владельца схемы приводит к тому, что выполнение операции расширения схемы станет невозможным.
- *Владелец доменных имен* (Domain Naming Master). Контроллер домена, отслеживающий изменения в структуре леса доменов. Любое изменение пространства имен доменов Active Directory (добавление, удаление, а также переименование доменов) осуществляется исполнителем данной роли. Тем самым гарантируется целостность пространства имен и уникальность его компонентов. Отказ исполнителя этой роли приводит к

тому, что любое изменение пространства имен каталога станет невозможным.

- *Владелец идентификаторов* (Relative ID Master). Контроллер домена, осуществляющий генерацию идентификаторов (глобальные идентификаторы, идентификаторы безопасности и т. п.). От идентификатора в первую очередь требуется уникальность. Самый простой способ гарантировать уникальность генерируемых идентификаторов — возложить обязанность исполнителя данной роли на один контроллер в домене. Отказ исполнителя данной роли приводит к тому, что создание объектов в домене станет невозможным.
- *Эмулятор основного контроллера домена* (PDC Emulator). Если домен находится на функциональном уровне Windows 2000 mixed, эмулятор основного контроллера домена (PDC) используется для обеспечения репликации изменений между контроллерами домена Windows NT и Windows 2000/Server 2003. Исполнитель роли фактически эмулирует домен Windows NT. Поскольку в домене Windows NT допустимо наличие только одного основного контроллера, его эмулятор в домене Active Directory также может быть только один. На других функциональных уровнях эмулятор основного домена используется для изменения паролей учетных записей, а также играет ведущую роль в процессе синхронизации системных часов всех контроллеров домена. Эмулятор PDC по умолчанию выбирается оснасткой Group Policy Object Editor. Поэтому, если исполнитель данной роли недоступен, администратор может столкнуться с серьезными проблемами при редактировании объектов групповой политики.
- Владелец инфраструктуры (Infrastructure Master). Контроллер домена, отвечающий за структуру каталога. В процессе удаления или перемещения объектов один из контроллеров домена должен взять на себя обязанности по сохранению ссылки на данные объекты до тех пор, пока эти изменения не будут реплицированы на все остальные контроллеры домена. Если в домене имеются несколько контроллеров домена, желательно не совмещать функции исполнителя данной роли и сервера глобального каталога. Лучше разнести эти функции на разные контроллеры домена, которые обязательно должны быть соединены высокоскоростным каналом. Если в домене имеется только один контроллер, этим требованием можно пренебречь.

По умолчанию все специализированные роли возлагаются на первый контроллер домена, установленный в новом лесе доменов. Аналогичным образом, в процессе создания нового домена первый установленный контроллер будет выбран в качестве исполнителя ролей, уникальных в пределах домена. Понижение контроллера домена, выбранного в качестве исполнителя специализированной роли, до выделенного сервера приводит к тому, что роли передаются другому контроллеру домена.

При необходимости администратор может в любой момент передать обязанности исполнителя любой роли другому контроллеру домена. Это может потребоваться, например, в ситуации, когда планируется обновление аппаратного обеспечения сервера. В процессе нормальной передачи роли текущий исполнитель специализированной роли освобождается от исполнения специфических обязанностей и становится обычным контроллером домена. Одновременно с этим на другой контроллер домена, выбранного на роль нового исполнителя, возлагаются обязанности исполнителя специализированной роли. Если администратор не может обеспечить доступность сервера, являющегося исполнителем специализированной роли, либо восстановление его работоспособности не представляется возможным, он должен возложить обязанности исполнения данной роли на другой контроллер домена. Процесс принудительной передачи функций исполнителя специализированной роли другому контроллеру домена называется захватом роли.

12.3. Свойства системы репликации

Для обозначения односторонней передачи данных от одного партнера по репликации к другому в AD используется термин «соединение».

Инфраструктура соединений между DC называется топологией репликации.

Причем каждый раздел каталога строит свою топологию репликации с общими и собственными соединениями.

Формирование топологии репликации выполняет специальный системный процесс Knowledge Consistency Checker (KCC). KCC выполняется на всех контроллерах, периодически активируется и проверяет доступность существующих соединений.

Соединения генерируются автоматически с использованием информации о физической структуре AD (сайты и сети). Или определяются вручную администратором.

Свойства внутридоменных, внутрисайтовых, и межсайтовых соединений различаются.

- *Внутрисайтовая репликация.* KCC автоматически начинает создавать топологию репликации в виде кольца. Избыточность дает надежность. При увеличении числа контроллеров DC добавляются радиальные связи для уменьшения числа ретрансляции до трех
- *Межсайтовая репликация.* Соединения между сайтами должны устанавливаться с учетом свойств каналов связи, которые могут отличаться по пропускной способности, загрузке, стабильности. Поэтому система более сложная и динамичная. Один KCC в сайте назначается как генератор межсайтовой топологии ISTG. Сайты связаны между собой особыми связями, называемыми «site link», которые определяют стоимость

маршрутизации данных AD (элементы леса, домена, папка SYSVOL и т.д.) между различными сайтами. Кроме автоматически устанавливаемых соединений между сайтами часто требуется ручная настройка от администратора.