Проектирование Active Directory

Администрирование АИС

Цель лекции: Ввести используемые в курсе понятия службы каталогов, дать представление об этапах проектирования службы Active Directory.

Планирование является важным подготовительным этапом при реализации проекта по созданию единой инфраструктуры Active Directory в компании.

На этом этапе определяется последовательность осуществляемых работ, необходимых для проектирования предлагаемого решения:

- *сбор информации,*
- *ее анализ,*
- *разработка структуры и архитектуры решения,*
- *а также вариантов развертывания системы при миграции данных.*

Основные понятия службы каталогов

Прежде чем перейти к **обзору процесса проектирования**, включающего сбор и анализ данных о существующей структуре предприятия и подготавливающего реализацию Active Directory, необходимо **ввести и определить ряд терминов**, используемых в контексте службы каталогов Active Directory.

Область действия

Область действия (scope) Active Directory достаточно обширна.

Она может включать отдельные сетевые объекты (принтеры, файлы, имена пользователей), серверы и домены в отдельной глобальной сети.

Она может также охватывать несколько объединенных сетей. Некоторые из рассматриваемых ниже терминов относятся к группе сетей, поэтому важно помнить, что Active Directory может быть настроена на управление как отдельным компьютером, так и компьютерной сетью или группой сетей.

Пространство имен

Active Directory, как и любая другая служба каталогов, является прежде всего пространством имен.

Пространство имен - это такая ограниченная область, в которой может быть распознано данное имя.

Распознавание имени заключается в его сопоставлении с некоторым объектом или объемом информации, которому это имя соответствует.

Например, телефонный справочник представляет собой пространство имен, в котором именам телефонных абонентов могут быть поставлены в соответствие телефонные номера.

Файловая система Windows образует пространство имен, в котором имя файла может быть поставлено в соответствие конкретному файлу.

Active Directory образует пространство имен, в котором имя объекта в каталоге может быть поставлено в соответствие самому этому объекту.

Объект - это непустой, именованный набор атрибутов, обозначающий нечто конкретное, *например пользователя, принтер или приложение*.

Атрибуты содержат информацию, однозначно описывающую данный объект.

Атрибуты пользователя могут включать имя пользователя, его фамилию и адрес электронной почты.

Контейнер аналогичен объекту в том смысле, что он также имеет атрибуты и принадлежит пространству имен.

Однако, в отличие от объекта, контейнер не обозначает ничего конкретного: **он может содержать группу объектов или другие контейнеры**.

Термин " дерево " используется в данном документе для описания иерархии объектов и контейнеров.

- Как правило, конечными элементами дерева являются объекты.
- В узлах (точках ветвления) дерева располагаются контейнеры.
- Дерево отражает взаимосвязь между объектами или указывает путь от одного объекта к другому.
- Простой каталог представляет собой контейнер.
- Компьютерная сеть или домен тоже являются контейнерами.
- Непрерывным поддеревом называют любую непрерывную часть дерева, включающую все элементы каждого входящего в нее контейнера.

Имя

Служба Active Directory допускает существование **двух типов имен, используемых для идентификации объектов**:

- **Уникальное имя**.

Каждый объект в Active Directory имеет уникальное имя (Distinguished Name, DN). Это имя содержит указание на домен, в котором находится объект, и полный путь в иерархической структуре контейнеров, который приводит к данному объекту.

Типичным уникальным именем (DN) является имя: */O=Internet/DC=COM/DC=Microsoft/CN=Users/CN=James Smith.*

Это имя обозначает объект типа "пользователь"с именем "James Smith", находящийся в домене Microsoft.com.

- **Относительное имя**.

Относительное уникальное имя объекта (Relative Distinguished Name, RDN) - это та часть имени, которая сама является частью атрибута объекта.

В приведенном выше примере *RDN-именем объекта "James Smith"служит групповое имя (CN) CN=James Smith.*

RDN-именем родительского объекта является имя CN=Users.

Контексты имен (сегменты, разделы)

Active Directory может состоять из одного или нескольких контекстов имен или сегментов (разделов).

Контекстом имен может быть любое непрерывное поддерево каталога.

Контексты имен являются единицами репликации.

В Active Directory каждый сервер всегда содержит не менее трех контекстов имен:

- логическую структуру;
- конфигурацию (топологию репликации и соответствующие метаданные);
- один или несколько пользовательских контекстов имен (поддеревья, содержащие объединенные в каталог объекты).

Домены

Домен - это единая область, в пределах которой обеспечивается безопасность данных в компьютерной сети под управлением ОС Windows.

- Active Directory состоит из *одного или нескольких доменов*.
- *Применительно к отдельной рабочей станции доменом является сама станция.*
- *Границы одного домена могут охватывать более чем одно физическое устройство.*
- Каждый домен может иметь *свои правила защиты информации и правила взаимодействия* с другими доменами.
- Если несколько доменов связаны друг с другом **доверительными отношениями** и имеют единую логическую структуру, конфигурацию и глобальный каталог, то говорят о **дереве доменов**.

Доверительные отношения

Поскольку домены разграничивают зоны безопасности, специальный механизм, называемый *доверительными отношениями* (*trust relationships*), позволяет объектам в одном домене [доверяемом (*trusted domain*)] обращаться к ресурсам в другом [доверяющем (*trusting domain*)].

Windows Server 2003 поддерживает шесть типов доверительных отношений:

- **Доверие к родительскому и дочернему доменам**.

Active Directory автоматически выстраивает транзитивные двусторонние *доверительные отношения* между родительскими и дочерними доменами в дереве доменов.

При создании дочернего домена *доверительные отношения* автоматически формируются между дочерним доменом и его родителем.

Эти отношения двусторонние.

Доверие также является транзитивным, т. е. контроллеры доверяемого домена пересылают запросы на аутентификацию контроллерам доверяющих доменов.

- **Доверие к корневому домену дерева**.

Двусторонние транзитивные *доверительные отношения* автоматически создаются и между корневыми *доменами деревьев* в одном лесу.

Это резко упрощает управление доменами по сравнению с тем, что было в версиях Windows, предшествовавших Windows 2000.

Больше не нужно конфигурировать отдельные односторонние *доверительные отношения* между доменами.

- **Доверие к внешнему домену**.

Внешнее доверие используется, когда нужно создать *доверительные отношения* между доменом Windows Server 2003 и доменом Windows NT 4.0.

Поскольку ограниченные домены (down-level domains) (домены, не поддерживающие Active Directory) не могут участвовать в двусторонних транзитивных доверительных отношениях, следует использовать *внешнее доверие, которое является односторонним*.

- **Доверие к сокращению**.

Доверие к сокращению - это способ создания прямых *доверительных отношений* между двумя доменами, которые могут быть уже связаны цепочкой транзитивных доверий, но нуждаются в более оперативном реагировании на запросы друг от друга.

- **Доверие к сфере**.

Доверие к сфере служит для подключения домена Windows Server 2003 к сфере *Kerberos*, которая не поддерживает Windows и использует протокол защиты *Kerberos* V5.

Доверие к сфере может быть транзитивным или нетранзитивным, одно- или двусторонним.

- **Доверие к лесу**.

Доверие к лесу упрощает управление несколькими лесами и обеспечивает более эффективное защищенное взаимодействие между ними.

Этот тип доверия позволяет обращаться к ресурсам в другом лесу по той же идентификации пользователя (user IDentification, ID), что и в его собственном лесу.

Доменное дерево

Дерево доменов состоит из нескольких доменов, которые имеют общую логическую структуру и конфигурацию и образуют непрерывное *пространство имен*.

Домены в дереве связаны между собой *доверительными отношениями*.

Active Directory является множеством, которому принадлежат одно или несколько деревьев доменов.

Дерево доменов графически можно представить двумя способами:

- **Представление доменного дерева через доверительные отношения между доменами.**

Доверительные отношения между доменами в ОС Windows 2000 устанавливаются на основе протокола безопасности *Kerberos*.

Отношения, созданные с помощью этого протокола, обладают свойствами транзитивности и иерархичности: *если домен А доверяет домену В и домен В доверяет домену С, то домен А доверяет и домену С.*

- **Представление доменного дерева через пространство имен доменного дерева.**

Доменное дерево можно также представить с помощью пространства имен.

Уникальное *имя объекта* можно определить, двигаясь вверх по доменному дереву начиная с объекта.

Такой метод оказывается удобным при объединении объектов в логическую иерархическую структуру.

Главное достоинство непрерывного пространства имен состоит в том, что глубокий поиск, проводимый от корня дерева, позволяет просмотреть все иерархические уровни пространства имен.

Несколько доменных деревьев могут быть объединены в лес.

Лес

Лесом называется одно или несколько деревьев, которые не образуют непрерывного пространства имен.

Все деревья одного леса *имеют общие логическую структуру, конфигурацию и глобальный каталог*.

Все деревья данного леса *поддерживают друг с другом транзитивные иерархические доверительные отношения*, устанавливаемые на основе протокола Kerberos.

В отличие от дерева, *лес может не иметь какого-то определенного имени*.

Лес существует в виде совокупности объектов с перекрестными ссылками и доверительных отношений на основе протокола Kerberos, установленных для входящих в лес деревьев.

Поддержка протокола Kerberos требует, чтобы деревья одного леса составляли иерархическую структуру: имя дерева, располагающегося в корне этой структуры, может использоваться для обозначения всего данного леса деревьев.

Организационные единицы (подразделения)

Организационные единицы (Organizational Units, OU) или организационные подразделения (ОП) позволяют *разделять домен на зоны административного управления*, т. е. создавать единицы административного управления внутри домена.

В основном это дает *возможность делегировать административные задачи в домене*.

До появления Active Directory домен был наименьшим контейнером, которому могли быть назначены административные разрешения.

Сайт (узел)

Узлом (сайтом) называется такой элемент сети, который содержит серверы Active Directory.

Узел обычно *определяется как одна или несколько подсетей, поддерживающих протокол TCP/IP* и характеризующихся хорошим качеством связи, которое подразумевает высокую надежность и скорость передачи данных.

Определение узла как совокупности подсетей *позволяет администратору быстро и без больших затрат настроить топологию доступа и репликации в Active Directory* и полнее использовать достоинства физического расположения устройств в сети.

Когда пользователь входит в систему, клиент Active Directory ищет серверы Active Directory, расположенные в узле пользователя.

Поскольку компьютеры, принадлежащие к одному узлу, в масштабах сети можно считать расположенными близко друг к другу, *связь между ними должна быть быстрой, надежной и эффективной*.

Распознавание локального узла в момент входа в систему не составляет труда, так как рабочая станция пользователя уже знает, в какой из подсетей TCP/IP она находится, а подсети напрямую соответствуют узлам Active Directory.

Сбор и анализ информации

На данном этапе предпроектного исследования **собираются основные сведения по существующей инфраструктуре в компании.**

- **Для планирования структуры Active Directory** - *информация о доменной структуре и ее типе, структуре групп пользователей и распределении их по доменам, количестве существующих контроллеров доменов внутри каждого домена.*

Определение

- существующих *доверительных отношений* между доменами,
- односторонних и двухсторонних *доверительных отношений* и доменов, которые не должны включаться в леса Active Directory,
- пространства имен DNS, существующих в организации,
- и перечня существующих доменных имен организации, зарегистрированных в сети Интернет.

- **Для планирования сайтов Active Directory** - информация о существующей структуре сайтов, о топологии сети, о каналах связи и их пропускной способности.

- **Для планирования переноса текущей структуры сетевых сервисов на платформу Active Directory** - информация о топологии используемых сетевых сервисов DHCP, WINS, DNS.

- **Для обеспечения возможности резервного восстановления данных во время миграции** - схема резервного копирования информации.

- **Для определения возможной расширяемости решения** - исследование возможных вариантов изменения схемы при росте организации или ее реорганизации, определение области Active Directory (исследование подразделений, включая удаленные филиалы организации, необходимых для включения в Active Directory).

- **Для планирования миграции приложений, использующих Active Directory** - список приложений, связанных с Active Directory, и возможных ограничений, накладываемых ими на структуру Active Directory, определение механизмов идентификации пользователей.

План проектирования структуры Active Directory

Проектирование структуры Active Directory **начинается с компонентов высшего уровня, а затем проектируются компоненты низших уровней.**

Это означает, что

- первый шаг состоит в создании проекта леса,
- затем следует проект доменов,
- проект *DNS*
- и, наконец, проект организационной единицы (OU).

Проектирование структуры *Active Directory* должно включать следующие основные вехи.

1. **Планирование структуры лесов:**
   - Определение типовых лесов для основных типов региональных представительств.
   - Определение основных типов доверительных отношений между разными лесами.
   - Разработка политики контроля изменений леса.
   - Политика изменения схемы.
   - Политика изменения конфигурации.
   - Разработка структуры DNS для типовых лесов.

2. Планирование доменов для каждого леса:

- Реструктуризация существующих доменов на домены в зависимости от административных потребностей.
- Разбиение на домены в зависимости от физического месторасположения для оптимизации трафика репликации и запросов.
- Выбор корневого домена для каждого леса.
- Оптимизация аутентификации укороченными доверительными отношениями.

3. Планирование использования сайтов для каждого леса:

- Определение сайтов на основании физической топологии сети.
- Создание связей между сайтами.
- План размещения серверов глобального каталога в сайтах.
- План размещения серверов DNS в сайтах.

4. Планирование структуры организационных единиц для каждого домена:

- Планирование реорганизации существующих доменов в организационных единицах.
- Планирование организационных единиц для делегирования административных полномочий.
- Планирование организационных единиц для скрытия объектов.
- Создание организационных единиц для применения групповых политик.

5. **Планирование реорганизации существующих доменов и их перевод на новую платформу Active Directory:**
   - Планирование перемещения пользователей, компьютеров и групп.
   - Планирование модификации или удаления из структуры реструктуризируемых доменов.
   - Планирование изменения существующих доверительных отношений.
   - Планирование клонирования объектов безопасности.

6. Тестирование внедряемых решений и установка стенда:

- Определение возможностей и целей тестирования.
- Разработка сценариев тестирования:

цель тестирования;

тестируемые возможности и функции;

требования к оборудованию, программному обеспечению и его конфигурации;

описание проведения тестирования;

ожидаемые результаты или критерии успеха теста;

график тестирования.

При планировании новых учетных записей для предотвращения возможных проблем следует обратить внимание на **решение следующих вопросов:**

1) правила именования, которые обеспечат уникальные, но понятные имена учетных записей;
2) специалист, ответственный за определение паролей;
3) временные периоды, в которые пользователю разрешено и запрещено входить в сеть;
4) возможность блокировки учетной записи;
5) тип профиля пользователя;
6) хранение документов пользователя: в локальной папке или в домашней папке на сервере.

Краткие итоги

В этой лекции были **приведены термины для понимания предметной области *Active Directory***, а также **упомянуто об этапе предпроектного исследования, предназначенного для сбора и анализа информации**.

Основные сведения по существующей инфраструктуре в компании:

- *Информация о доменной структуре и ее типе, структуре групп пользователей и распределении их по доменам, о количестве существующих контроллеров доменов внутри каждого домена.*
- *Информация о существующей структуре сайтов, о топологии сети, о каналах связи и их пропускной способности.*
- *Информация о топологии используемых сетевых сервисов DHCP, WINS, DNS.*
- *Схема резервного копирования информации.*
- *Определение области Active Directory.*
- *Список приложений, связанных с Active Directory, и возможных ограничений, накладываемых ими на структуру Active Directory.*

Краткие итоги

Помимо этого **представлен типовой план проектирования структуры Active Directory**, который без детализации выглядит следующим образом.

- *Планирование структуры лесов.*
- *Планирование доменов для каждого леса.*
- *Планирование использования сайтов для каждого леса.*
- *Планирование структуры организационных единиц для каждого домена.*
- *Планирование реорганизации существующих доменов и их перевод на новую платформу Active Directory.*
- *Тестирование внедряемых решений и установка стенда.*