Лабораторная работа 4. Доменные службы Active Directory (AD DS). Установка и первоначальная настройка AD DS. Объекты AD. Групповые политики (GPO).

Теоретический материал.

Рабочие и домашние группы, домены

Домены, рабочие группы и домашние группы представляют разные методы организации компьютеров в сети. Основное их различие состоит в том, как осуществляется управление компьютерами и другими ресурсами.

Компьютеры под управлением Windows в сети должны быть частью рабочей группы или домена. Компьютеры под управлением Windows в домашней сети также могут быть частью домашней группы, но это не обязательно.

Компьютеры в домашних сетях обычно входят в состав рабочих групп и, возможно, домашней группы, а компьютеры в сетях на рабочих местах - в состав доменов.

Домены управляются централизованно одним или группой Windows серверов называемых контроллерами домена. Контроллер домена в компьютерных сетях - сервер, контролирующий область компьютерной сети (домен). Контроллеры домена хранят данные каталога и управляют взаимодействиями пользователя и домена, включая процессы входа пользователя в систему, проверку подлинности и поиски в каталоге. Контроллеры домена создаются при использовании мастера установки Active Directory.

В рабочей группе:

- Все компьютеры являются одноранговыми узлами сети; ни один компьютер не может контролировать другой.
- На каждом компьютере находится несколько учетных записей пользователя. Чтобы войти в систему любого компьютера, принадлежащего к рабочей группе, необходимо иметь на этом компьютере учетную запись.
- В составе рабочей группы обычно насчитывается не больше двадцати компьютеров.
- Рабочая группа не защищена паролем.

- Все компьютеры должны находиться в одной локальной сети или подсети.

В домашней группе:

- Компьютеры в домашней сети должны принадлежать рабочей группе, но они также могут состоять в домашней группе. С помощью домашней группы предоставлять доступ к рисункам, музыке, видео, документам и принтерам другим пользователям намного проще.
- Домашняя группа защищена паролем, но он вводится только один раз при добавлении компьютера в домашнюю группу.

Домашняя группа удалена из Windows 10 (версия 1803).

В домене:

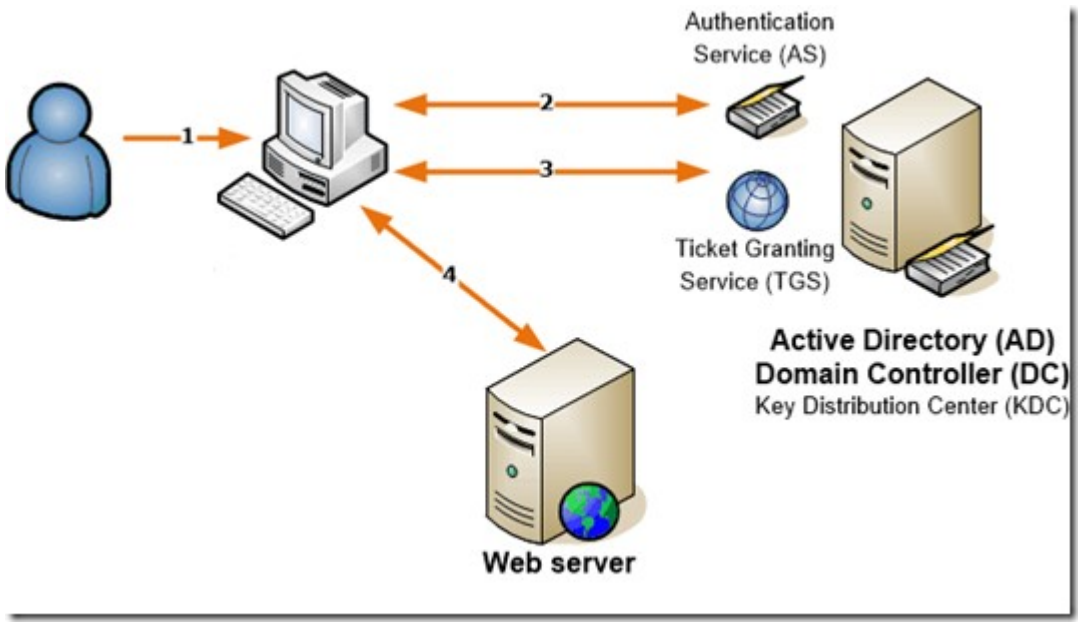
- Один или несколько компьютеров являются серверами. Администраторы сети используют серверы для контроля безопасности и разрешений для всех компьютеров домена. Это позволяет легко изменять настройки, так как изменения автоматически производятся для всех компьютеров. Пользователи домена должны указывать пароль или другие учетные данные при каждом доступе к домену.
- Если пользователь имеет учетную запись в домене, он может войти в систему на любом компьютере. Для этого не требуется иметь учетную запись на самом компьютере.
- Права изменения параметров компьютера могут быть ограничены, так как администраторы сети хотят быть уверены в единообразии настроек компьютеров.
- В домене могут быть тысячи компьютеров.
- Компьютеры могут принадлежать к различным локальным сетям.

Active Directory

Службы Active Directory (AD) - решение от компании Microsoft позволяющее объединить различные объекты сети (компьютеры, сервера, принтера, различные сервисы) в единую систему. В данном случае AD выступают в

роли каталога (базы данных), в котором хранится информация о пользователях, ПК, серверах, сетевых и периферийных устройствах.

Для реализации данного решения, необходим специальный сервер - контроллер домена. Именно он будет выполнять функции аутентификации пользователей и устройств в сети, а также выступать в качестве хранилища базы данных. При попытке использовать любой из объектов (ПК, сервер, принтер) сети, выполняется обращение к контроллеру домена, который либо разрешает это действие (есть необходимые права), либо блокирует его.



Единая точка аутентификации

Поскольку контроллер домена Active Directory хранит всю информацию об инфраструктуре и пользователях, вы легко можете использовать его для входа систему. Так, все данные пользователей (логины и пароли) хранятся в единой базе данных, что существенно упрощает работу с ними. При авторизации все компьютеры обращаются к этой базе данных, благодаря чему вносимые изменения будут применены ко всем компьютерам сети. Также с помощью AD реализуются политики безопасности, благодаря котором можно ограничить (либо разрешить) доступ к определенным серверам.

Удобное управление политиками

С помощью Active Directory можно поделить компьютеры на различные рабочие группы (организационные подразделения). Это существенно упрощает использование инфраструктуры в двух случаях:

1. Изменение существующих настроек группы. Поскольку настройки хранятся в единой базе данных, при их модификации, они будут применены для всех компьютеров, относящихся к этой группе.
2. Добавление нового пользователя. Он автоматически получает установленные для его группы настройки, что существенно ускоряет создание новой учетной записи.

В зависимости от пользователя (учетной записи, которая используется) и его группы можно ввести ограничение на использование функционала операционной системы. Например, вы можете ограничить установку приложений всем кроме администраторов.

Безопасность

Службы Active Directory существенно увеличивают защиту корпоративной сети. Так, все данные (учетные записи) хранятся на контроллерах доступа, которые защищены от внешнего доступа. Кроме того, для аутентификации в AD используется протокол Kerberos (протокол для взаимной аутентификации клиента и сервера перед установкой соединения, в нем учтена возможность перехвата и модификации пакетов, что повышает его надежность), который значительно безопаснее аналога в рабочих группах.

Удобный обмен файлами

С помощью AD достаточно легко реализуется технология Distributed File System (DFS), которая используется для управления файлами. Фактически, это распределенная сеть для хранения файлов - физически они располагаются на нескольких серверах, но логически находятся в одном месте.

Это удобная функция, позволяющая масштабировать существующую инфраструктуру, добавляя новые сервера, а не заменяя ими старые.

Интеграция сервисов и оборудования

Службы Active Directory позволяют организовать все оборудование и сервисы в единую систему. Например, присутствует поддержка стандарта LDAP (протокол для доступа к службе каталогов X.500), который позволяет работать с почтовыми и прокси серверами. Поддерживаются не только продукты Microsoft, но и сторонние решения:

- IP-телефония;
- 1C;
- шлюз удаленных рабочих столов (Remote Desktop Gateway).

Стоит отметить, возможность интеграции с Windows Server используя протокол RADIUS, благодаря которому можно использовать VPN подключение для работы вне офиса.

Наличие дублирующего контроллера доменов

Вся база данных хранится на контроллере доменов Active Directory, поэтому при его отказе, вся система будет недоступна. Для обеспечения отказоустойчивости следует развернуть 1 или более дублирующих контроллеров доменов и настроить автоматическую репликацию всех изменений. В данном случае, при выходе из строя одного из контроллеров работоспособность сети не нарушается, ведь оставшиеся продолжают работать.

Структура Active Directory

Объекты

Active Directory имеет иерархическую структуру, состоящую из объектов. Объекты разделяются на три основные категории: ресурсы (например,

принтеры), службы (например, электронная почта) и учётные записи пользователей и компьютеров. Служба предоставляет информацию об объектах, позволяет организовывать объекты, управлять доступом к ним, а также устанавливает правила безопасности.

Объекты могут быть хранилищами для других объектов (группы безопасности и распространения). Объект уникально определяется своим именем и имеет набор атрибутов — характеристик и данных, которые он может содержать; последние, в свою очередь, зависят от типа объекта. Атрибуты являются составляющей базой структуры объекта и определяются в схеме. Схема определяет, какие типы объектов могут существовать.

Сама схема состоит из двух типов объектов: объекты классов схемы и объекты атрибутов схемы. Один объект класса схемы определяет один тип объекта Active Directory (например, объект «Пользователь»), а один объект атрибута схемы определяет атрибут, который объект может иметь.

Каждый объект атрибута может быть использован в нескольких разных объектах классов схемы. Эти объекты называются объектами схемы (или метаданными) и позволяют изменять и дополнять схему, когда это необходимо и возможно. Однако каждый объект схемы является частью определений объектов, поэтому отключение или изменение этих объектов могут иметь серьёзные последствия, так как в результате этих действий будет изменена структура каталогов. Изменение объекта схемы автоматически распространяется в службе каталогов. Будучи однажды созданным, объект схемы не может быть удалён, он может быть только отключён. Обычно все изменения схемы тщательно планируются.

Контейнер аналогичен объекту в том смысле, что он также имеет атрибуты и принадлежит пространству имён, но, в отличие от объекта, контейнер не обозначает ничего конкретного: он может содержать группу объектов или другие контейнеры.

Иерархия объектов Active Directory

Структурные объекты:

- Сервер — компьютер, выполняющий определённые роли в домене.
- Контроллер домена — сервер, хранящий каталог и обслуживающий запросы пользователей к каталогу. Помимо хранения данных контроллер домена может выступать в качестве одной из FSMO-ролей.

- Домен — минимальная структурная единица организации Active Directory.
- Дерево доменов — иерархическая система доменов, имеющая единый корень (корневой домен).
- Лес доменов — множество деревьев доменов, находящихся в различных формах доверительных отношений.

Административные объекты:

- Организационная единица (OU) — объект-контейнер для хранения других объектов. Может выступать в качестве объекта применения политик, прав доступа, но не может выступать в качестве субъекта доступа (то есть возможно выдать права для всех пользователей из данной OU, но невозможно выдать права на доступ к каким-либо ресурсам самой OU).

Контролируемые объекты:

- Компьютер — рабочая станция или сервер, входящие в домен.
- Пользователь — учётная запись, от имени которой выполняются программы на компьютерах.
- Группа — объект-контейнер для других объектов. В отличие от организационной единицы, может быть самостоятельным субъектом доступа при проверке прав доступа к какому-либо объекту (иными словами, можно разрешить доступ к какому-нибудь ресурсу для всех пользователей, включенных в группу, путем предоставления прав к ресурсу непосредственно данной группе; в случае с организационной единицей права потребовалось бы предоставить всем пользователям, включенным в OU).
- Групповая политика — набор правил, применяемых к объектам. Групповая политика назначается группе (или, как частный случай любому объекту, который может быть включён в группу — пользователю, компьютеру), организационной единице или узлу.

Топологические объекты:

- Сайт (англ. site) — группа серверов, объединённая локальной сетью (высокоскоростными надёжными линиями).

Структура

Верхним уровнем структуры является лес — совокупность всех объектов, атрибутов и правил (синтаксиса атрибутов) в Active Directory. Лес содержит одно или несколько деревьев, связанных транзитивными отношениями доверия. Дерево содержит один или несколько доменов, также связанных в иерархию транзитивными отношениями доверия. Домены идентифицируются своими структурами имён DNS — пространствами имён.

Объекты в домене могут быть сгруппированы в контейнеры — подразделения. Подразделения позволяют создавать иерархию внутри домена, упрощают его администрирование и позволяют моделировать, например, организационную или географическую структуру организации в службе каталогов. Подразделения могут содержать другие подразделения. Microsoft рекомендует использовать как можно меньше доменов в службе каталогов, а для структурирования и политик использовать подразделения. Часто групповые политики применяются именно к подразделениям. Групповые политики сами являются объектами. Подразделение является самым низким уровнем, на котором могут делегироваться административные полномочия.

Другим способом деления являются сайты, которые являются способом физической (а не логической) группировки на основе сегментов сети. Сайты подразделяются на имеющие подключения по низко скоростным каналам (например, по каналам глобальных сетей, с помощью виртуальных частных сетей) и по высокоскоростным каналам (например, через локальную сеть). Сайт может содержать один или несколько доменов, а домен может содержать один или несколько сайтов. При проектировании службы каталогов важно учитывать сетевой трафик, создающийся при синхронизации данных между сайтами.

Ключевым решением при проектировании службы каталогов является решение о разделении информационной инфраструктуры на иерархические домены и подразделения верхнего уровня. Типичными моделями, используемыми для такого разделения, являются модели разделения по функциональным подразделениям компании, по географическому положению и по ролям в информационной инфраструктуре компании. Часто используются комбинации этих моделей.

Интеграция с UNIX

Различные уровни взаимодействия с Active Directory могут быть реализованы в большинстве UNIX-подобных операционных систем посредством LDAP-

клиентов, но такие системы, как правило, не воспринимают большую часть атрибутов, ассоциированных с компонентами Windows, например, групповые политики и поддержку односторонних доверенностей. Однако с выходом Samba 4 появилась возможность использовать групповые политики и инструменты администрирования Windows.

Альтернативным вариантом является использование других реализаций службы каталогов, выполняющих двухстороннюю синхронизацию с Active Directory, реализуя таким образом «отражённую» интеграцию, когда клиенты UNIX- и Linux-систем аутентифицируются на собственных серверах, а клиенты Windows — в Active Directory. Другим вариантом является использование OpenLDAP с возможностью полупрозрачного перекрытия, расширяющей элементы удалённого сервера LDAP дополнительными атрибутами, хранимыми в локальной базе данных.

Групповые политики

Групповая политика — это инструмент архитектуры Active Directory, который позволяет управлять настройками серверов и рабочих терминалов, подключенных к домену, централизованно. Также, с помощью групповых политик достаточно просто распространить программное обеспечение. Администратор может указать политики для группы в одном месте, а затем применить их к целевой группе пользователей.

Во многих компаниях, как правило, применяется деление на отделы: отдел кадров, бухгалтерия, юристы, отдел системного администрирования. Предположим, что каждому отделу необходим собственный минимальный набор программного обеспечения, а рабочие станции должны быть настроены для конкретных нужд и под конкретные задачи. Благодаря групповым политикам появляется возможность создать настройки для конкретных групп пользователей в домене. При помощи Active Directory GPO администратор может устанавливать и управлять стандартизированными наборами настроек, конкретно для бухгалтерии или отдела кадров.

Настройка рабочих мест пользователей становится проще и эффективнее, т. к. она производится централизованно и не требует дублирования на каждом ПК.

Компоненты GPO

Выделяют два компонента групповых политик — клиентский и серверный, т.е. формируется структура “клиент-сервер”.

Серверный компонент представляет оснастка MMC (Microsoft Management Console), предназначенная для настройки групповой политики. MMC можно использовать для создания политик, а также для контроля и управления административными шаблонами, настройками безопасности (установка ПО, скрипты и т.п.). Обобщенное название “возможностей” называется расширением. Каждое расширение может иметь дочернее расширение, которое разрешает добавление новых или удаление старых компонентов, а также их обновление.

Клиентский компонент получает и применяет настройки групповой политики. Клиентские расширения являются компонентами запускаемыми на клиентской ОС, которые отвечают за интерпретацию и обработку объектов групповой политики.

Для администрирования GPO используют оснастки MMC — Group Policy Management Console (GPMC) и Group Policy Management Editor.

Сценарии использования Active Directory GPO:

- Централизованная настройка пакета программ Microsoft Office.
- Централизованная настройка управлением питанием компьютеров.
- Настройка веб-браузеров и принтеров.
- Установка и обновление ПО.
- Применение определенных правил в зависимости от местоположения пользователя.
- Централизованные настройки безопасности.
- Перенаправление каталогов в пределах домена.
- Настройка прав доступа к приложениям и системным программам.

Список источников:

1. http://veeremaa.tpt.edu.ee/2013/ad.htm
2. https://www.it-lite.ru/blog/iaas/obzor-vozmozhnostey-active-directory/
3. https://ru.wikipedia.org/wiki/Active_Directory
4. https://ru.wikipedia.org/wiki/Иерархия_объектов_Active_Directory
5. https://serverspace.ru/support/help/active-directory-group-policies/