Основы Active Directory: 1 Часть.

telegra.ph/Osnovy-Active-Directory-1-CHast-07-30

Life-Hack - Linux/Хакинг/Хакер/ИБ/Osint July 30, 2024

Active Directory (AD) – это служба каталогов для сетевых сред Windows, которая используется для организации и централизованного управления различными типами объектов: компьютерами, пользователями, серверами, принтерами и т.д.. AD является центральным элементом управления и аутентификации в сетях Windows. Active Directory тесно связана и интегрирована о множеством служб и приложений Microsoft, таких как DNS, DHCP, почтовая служба Exchange Server, и т.д. Благодаря тому, что все учетные записи хранятся в единой базе AD, пользователь может войти под своей учетной записью и паролем на любой компьютер в домене AD (в отличии от workgroup, где на каждом компьютере хранится собственная база пользователей).

Рассмотрим базовые понятия и элементы AD:

- **Объект** можно определить как любой ресурс, присутствующий в среде Active Directory, например подразделения, принтеры, пользователи, контроллеры домена и т. д.
- **Атрибуты**. Каждый объект в Active Directory имеет связанный набор атрибутов, используемых для определения характеристик данного объекта. Объект компьютера содержит такие атрибуты, как имя хоста и DNS-имя. Все атрибуты в AD имеют связанное имя LDAP, которое можно использовать при выполнении LDAP запросов, например displayName.

- **Схема** Active Directory по сути является основой любой корпоративной среды. Она определяет, какие типы объектов могут существовать в базе данных AD и связанные с ними атрибуты. В ней содержится информация о каждом объекте. Каждый объект имеет свою собственную информацию (часть необходимо установить, а часть является необязательной), хранящуюся в атрибутах. Когда объект создается из класса, это называется созданием экземпляра этого класса. Например, если мы возьмем компьютер RDS01. Этот объект-компьютер является экземпляром класса «компьютер» в Active Directory.
- **Домен** — это логическая группа объектов, таких как компьютеры, пользователи, подразделения, группы и т. д. Мы можем рассматривать каждый домен как отдельный город в пределах штата или страны. Домены могут работать полностью независимо друг от друга или соединяться доверительными отношениями.
- **Лес** — это совокупность доменов Active Directory. Это самый верхний контейнер, содержащий все объекты AD, представленные ниже, включая, помимо прочего, домены, пользователей, группы, компьютеры и объекты групповой политики. Лес может содержать один или несколько доменов и рассматриваться как штат в США или страна в ЕС. Каждый лес работает независимо, но может иметь различные доверительные отношения с другими лесами.
- **Дерево** — это совокупность доменов Active Directory, которая начинается с одного корневого домена. Лес — это совокупность деревьев AD. Каждый домен в дереве имеет общую границу с другими доменами. Доверительные отношения родитель-потомок формируются, когда домен добавляется в другой домен в дереве. Два дерева в одном лесу не могут иметь одно имя. Все домены в дереве имеют общий стандартный глобальный каталог, который содержит всю информацию об объектах, принадлежащих дереву.
- Для установки домена Active Directory нужно установить роль Active Directory Domain Services (ADDS) на компьютере с Windows Server. Такой сервер называется **контроллер домена Active Directory (DC)**. В домене может быть один или несколько контроллеров домена, в зависимости от потребностей и размера домена. Контроллеры домена выполняют аутентификацию пользователей и обслуживают запросы на доступ к ресурсам сети (используется как logon server).
- **Global Catalog (GC)** – эта роль может быть назначена любому контроллеру домена. Такой DC будет хранить краткую информацию о всем лесе и использоваться для выполнения поиска и аутентификации в разных доменах.
- На контроллере домена **хранится база Active Directory (NTDS.DIT)**. Каждый контроллер домена хранит свою копию базы AD и реплицирует новые/измененные данный с другим DC.
- **Контейнер** — содержат другие объекты и имеют определенное место в иерархии поддерева каталогов.
- **Организационная единица (OU)** – контейнеры внутри домена для логической группировки объектов (аналог – папки на диске). Например, OU является точками назначения GPO и делегирования полномочий.

- **GUID (Global Unique Identifier)** — это уникальное 128-битное значение, присваиваемое при создании пользователя или группы домена. Это значение GUID уникально для всего предприятия, аналогично MAC-адресу. Каждому отдельному объекту, созданному Active Directory, присваивается GUID. GUID хранится в атрибуте ObjectGUID. При запросе объекта AD (например, пользователя, группы, компьютера, домена, контроллера домена и т. д.) мы можем запросить значение его objectGUID с помощью PowerShell или выполнить поиск, указав его отличительное имя, GUID, SID или SAM. GUID используются AD для внутренней идентификации объектов. Поиск по значению GUID, является наиболее точным и надежным способом найти именно тот объект, который вы ищете, особенно если глобальный каталог может содержать совпадения для имени объекта. Свойство ObjectGUID никогда не изменяется и связано с объектом до тех пор, пока этот объект существует в домене.
- **Субъекты безопасности (Security principals)** — это все, что операционная система может аутентифицировать, включая пользователей, учетные записи компьютеров или даже потоки/процессы, которые выполняются в контексте учетной записи пользователя или компьютера (т. е. приложение, такое как Tomcat, работающее в контексте учетной записи службы внутри домен).