Active Directory Basics

Vivek Pandit

1.What is Active Directory and How it Works ?

Active Directory (AD) is Microsoft's proprietary directory service. It runs on Windows Server and enables administrators to manage permissions and access to network resources.

Active Directory stores data as objects. An object is a single element, such as a user, group, application or device such as a printer. Objects are normally defined as either resources, such as printers or computers, or security principals, such as users or groups.

The main service in Active Directory is Domain Services (AD DS), which stores directory information and handles the interaction of the user with the domain. AD DS verifies access when a user signs into a device or attempts to connect to a server over a network. AD DS controls which users have access to each resource, as well as group policies. For example, an administrator typically has a different level of access to data than an end user.

3.Components Of Active Directory

1. Domain
2. Domain controller
3. Trees
4. Forest
5. Organizational Unit (OU)
6. Containers

3.Components Of Active Directory

1. Domain

A **domain** is a group of objects, such as users or devices, that share the same AD database.

It is used to group objects together and manage them. The domain provides an Authentication and Authorization boundary that provides a way to limit the scope of access to the resources of that domain. Consider **abc.com** as a domain.

3.Components Of Active Directory

2. Domain Controller

- Domain Controller is a server that processes requests and allows user logon, resource access and etc
- A server that is running **AD DS** is called **domain controller.**
- Domain controller host abd replicate the directory service database inside the forest.
- Domain Controller is a server computer that acts like a brain for windows server domain.

3.Components Of Active Directory

3. Trees

A **tree** is one or more domains grouped together. The tree structure uses a contiguous namespace to gather the collection of domains in a logical hierarchy. Trees can be viewed as trust relationships where a secure connection, or trust, is shared between two domains. Multiple domains can be trusted where one domain can trust a second, and the second domain can trust a third.

Trees can additionally have child domains. By default, Trees create Transitive trust with other domains.

3.Components Of Active Directory

4. Forest

Forest is said to be the collection of the Trees. Forest shares the common schema between its branches.

A forest consists of shared catalogs, directory schemas, application information and domain configurations. The schema defines an object's class and attributes in a forest. In addition, global catalog servers provide a listing of all the objects in a forest. According to Microsoft, the forest is Active Directory's security boundary.

3.Components Of Active Directory

5. Organizational Unit (OU)

Organizational Units (OUs) organize users, groups and devices. Each domain can contain its own OU. However, OUs cannot have separate namespaces, as each user or object in a domain must be unique.

3.Components Of Active Directory

6. Users

Users are one of the most common object type in Active Directory. Users are one of the objects known as **security principals**, meaning that they can be authenticated by The domain and can assigned privileges over over **resources** like files or printers.

Users can be used to represent two types of entities:

- **People:** users will generally represent persons in your organisation that need to access the network, like employees.
- **Services:** you can also define users to be used by services like IIS or MSSQL. Every single service requires a user to run, but service users are different from regular users as they will only have the privileges needed to run their specific service.

3.Components Of Active Directory

7. Machines

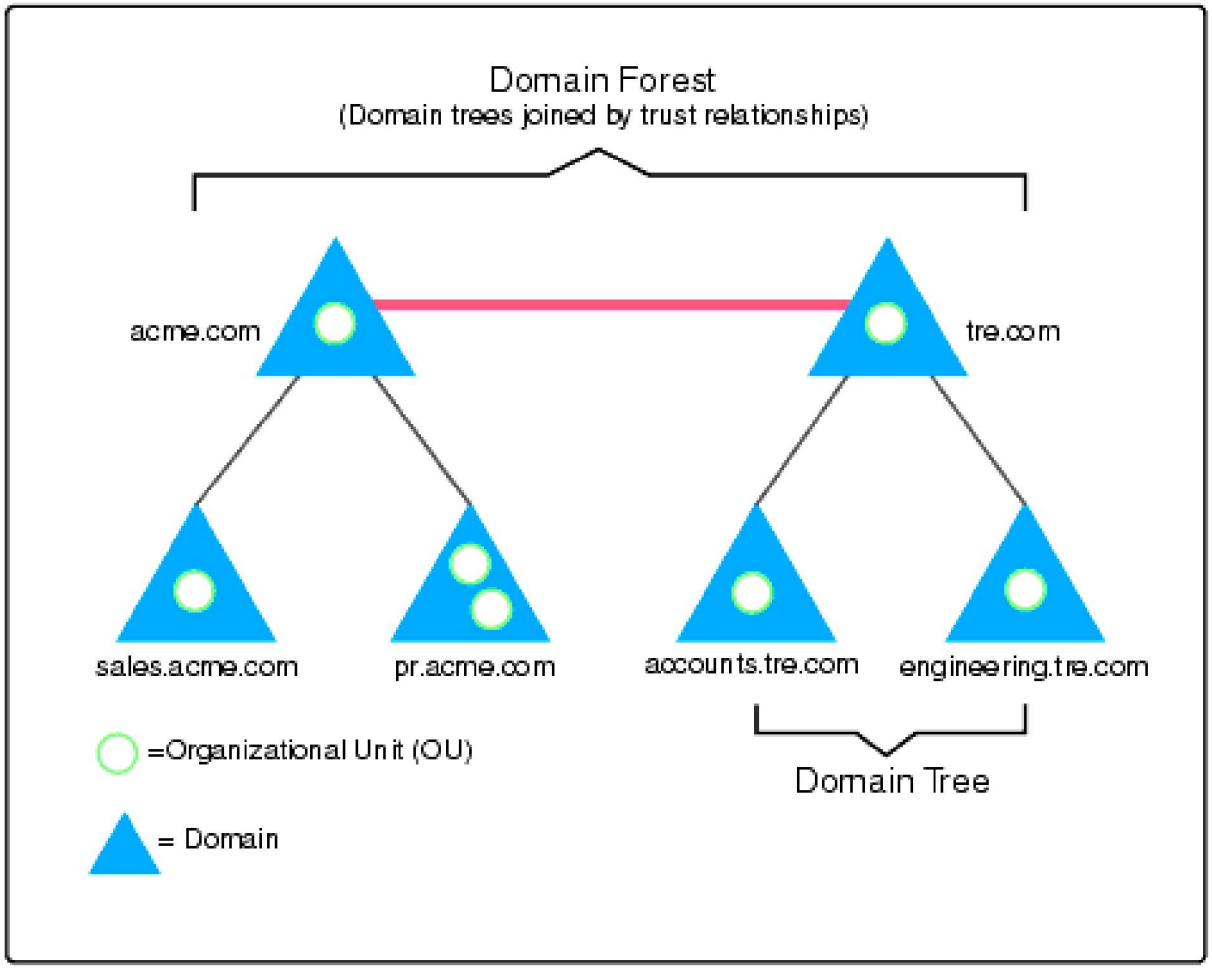
Machines are another type of object within Active Directory; for every computer that joins the Active Directory domain, a machine object will be created. Machines are also considered "security principals" and are assigned an account just as any regular user. This account has somewhat limited rights within the domain itself.

The machine accounts themselves are local administrators on the assigned computer, they are generally not supposed to be accessed by anyone except the computer itself, but as with any other account, if you have the password, you can use it to log in.

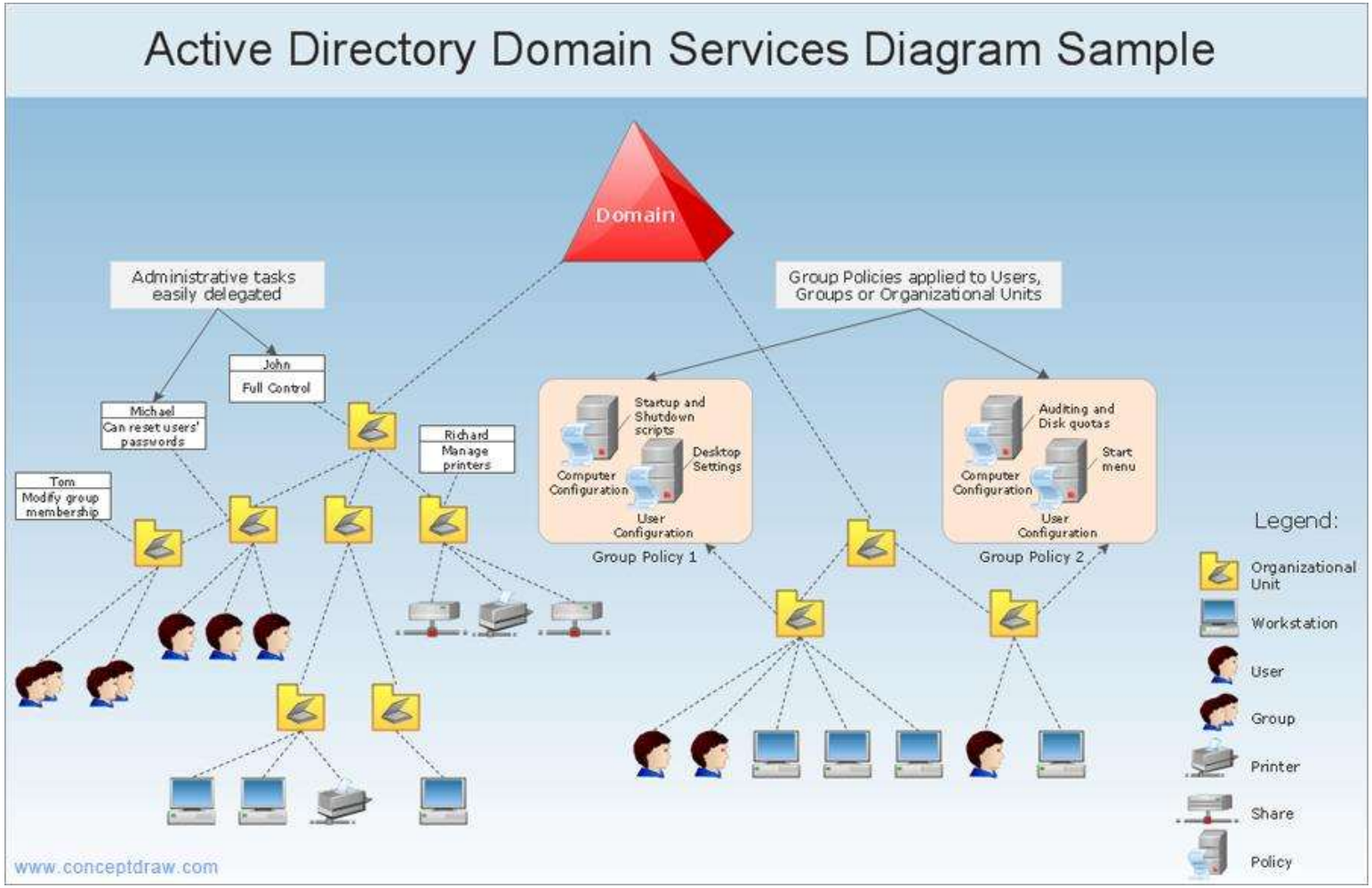
Note: Machine Account passwords are automatically rotated out and are generally comprised of 120 random characters.

Identifying machine accounts is relatively easy. They follow a specific naming scheme. The machine account name is the computer's name followed by a dollar sign. For example, a machine named DC01 will have a machine account called DC01$.

4.Active Directory Structure



4.Active Directory Structure



4.Active Directory Services

Several different services comprise Active Directory. The main service is Domain Services, but Active Directory also includes Lightweight Directory Services (AD LDS), Lightweight Directory Access Protocol (LDAP), Certificate Services, or AD CS, Federation Services (AD FS) and Rights Management Services (AD RMS). Each of these other services expands the product's directory management capabilities.

- **Lightweight Directory Services** has the same codebase as AD DS, sharing similar functionalities, such as the application program interface. AD LDS, however, can run in multiple instances on one server and holds directory data in a data store using Lightweight Directory Access Protocol.
- **Lightweight Directory Access Protocol** is an application protocol used to access and maintain directory services over a network. LDAP stores objects, such as usernames and passwords, in directory services, such as Active Directory, and shares that object data across the network.

- **Certificate Services** generates, manages and shares certificates. A certificate uses encryption to enable a user to exchange information over the internet securely with a public key.
- **Active Directory Federation Services** authenticates user access to multiple applications -- even on different networks -- using single sign-on (SSO). As the name indicates, SSO only requires the user to sign on once, rather than use multiple dedicated authentication keys for each service.
- **Rights Management Services** control information rights and management. AD RMS encrypts content, such as email or Microsoft Word documents, on a server to limit access.

Tasks

- Research more on active directory structure.