


Domain, Active Directory, Domain creation and system joining task.

Date: 20-07-2023

Task:

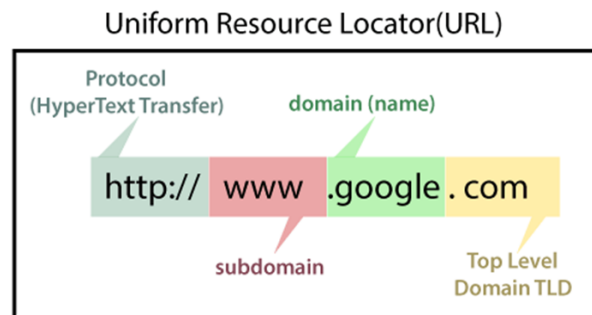
Domain:

A domain is a group of computers and devices that shares data and resources within the same network.

A domain name is the identity of one or more IP addresses; for example, the domain name  points to the IP address "74.125.127.147". Domain names are invented as it is easy to remember a name rather than a long string of numbers. It would be easy to enter a domain name in the search bar than a long sequence of numbers.

So, it is the web address of your website that people need to type in the browser URL bar to visit your website. In simple words, suppose your website is a house, then the domain name is its address.

A domain name cannot have more than sixty-three characters excluding .com, .net, .org, .edu, etc. The minimum length of a domain is one character excluding the extensions. It is entered in the URL after the protocol and subdomain as shown in the following example and the image:



Active Directory:

Active directory is a database of everything on the network -Computers, user accounts, file share, printers, groups and more.

Active Directory is a directory service and authentication framework developed by Microsoft. It is used to manage and organize resources in a Windows network environment, including user accounts, computers, servers, printers, and more.

Active Directory consists of several key components, including:

- **Domain:** A logical grouping of network objects with a common security policy.
- **Domain Controller:** Servers that store a copy of the Active Directory database and authenticate users.
- **Organizational Units (OUs):** Containers for organizing objects within a domain.
- **Groups:** Collections of users, computers, or other objects.
- **Users and Computers:** Representing people and devices in the network.

Commonly used by the help desk-Reset passwords, Add, and remove accounts.

Security in Active Directory is managed through **access control lists (ACLs) and security policies.**

A forest in Active Directory is a **collection of one or more domains that share a common schema and global catalog.** A forest represents the highest level of organizational structure within Active Directory.

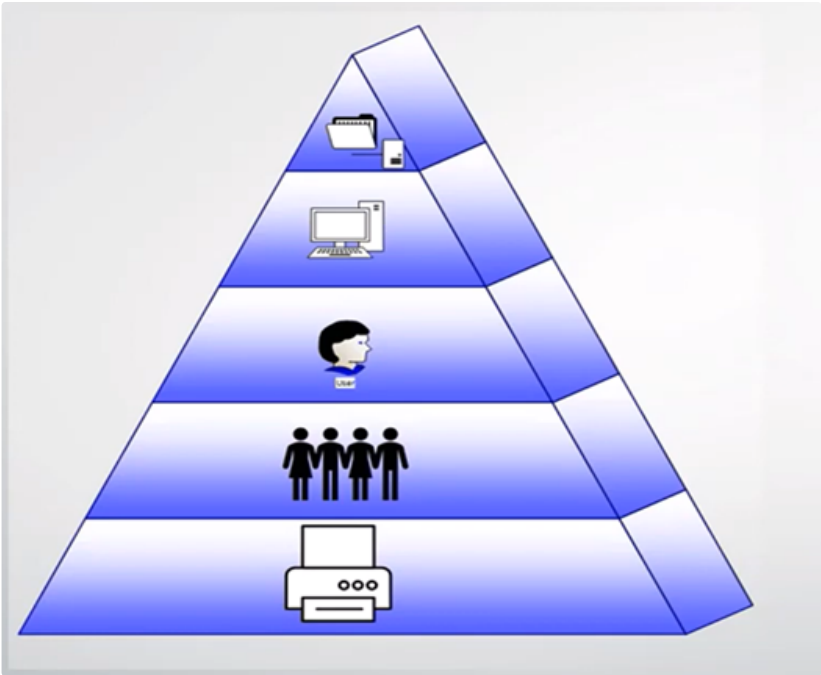
Trust relationships allow domains in an Active Directory forest to share resources. Trusts can be either one-way or two-way and are established to grant permissions and access between domains.

ADFS is a service that allows single sign-on (SSO) and identity federation between organizations or between different applications. It enables users to access multiple systems with a single set of credentials.

Active Directory Domain Services:

It contains NTFS.DIT (directory information tree) which is the important of AD and contains physical components and logical components in it.

Physical Components	Logical Components
Data store	Partitions
Domain Controllers	Schema
Global Catalog	Sites
RODC	Domain
	Domain Trees
	Sites
	Organizational Units



Active Directory Representation

A domain is a logical grouping of resources, and it creates a boundary. A group of objects, such as users or groups of devices, that share the same AD database makes up a [domain](#).

Resources include Users, Groups, Computers, Printers and more.

Each domain has its own database (NTFS.DIT)

Each domain can have multiple child domains which means in an organization any user has an issue we create a child domain and information of that user will be kept in that to solve the issue within organizational boundary.

All domains in a forest share the same Schema, schema is the blueprint. Which is same across the organization all the features and attributes contained by organizational domain will also be applied to the child domain. From root domain we create multiple child domains, and these child domains can be accessed with permissions only. Parent and child domains share the same namespace. The combination of root domain and child domain is known as Tree domain.

If we acquire a company named training.com, we will have different namespaces, trees, domain. We need to create trust between the trees. Different companies with different domains, blueprints, namespaces combining both are known as forest. By combining them we had the advantage that we could make a single blueprint/schema for both the forests.

The first tree contains a company named ELP aviation. It has 1Domain, 1tree, 1forest and Hr. ELP aviation 2domain, 1 tree, 1 forest and IT.ELP aviation 3domain, 1 tree, 1 forest all of this have the same schema/blueprint, emails, and attributes. By combining with others, the company will have 4 domains, 2 trees and 2 forests.

Difference Between Forest, Domain and Domain Controller:

1. Forest:

- **Definition:** A forest is the top-level container in the AD hierarchy. It represents the highest level of organizational structure in AD.
- **Function:** A forest is a collection of one or more domains with a common schema, global catalog, and directory configuration. It forms a security boundary, and objects within a forest share a common AD database, directory schema, and global catalog.
- **Trust Relationships:** Trust relationships can be established between domains within the same forest and between domains in different forests.

2. Domain:

- **Definition:** A domain is a logical grouping of network resources, including user accounts, computers, servers, and other objects. Domains are organized within a forest.
- **Function:** A domain serves as a security boundary where administrators can manage users, groups, and resources efficiently. Each domain has its own security policies, accounts, and permissions.
- **Trust Relationships:** Trust relationships are typically established between domains within the same forest, allowing users and resources to be shared.

3. Domain Controller:

- **Definition:** A domain controller (DC) is a server within a domain that stores a writable copy of the Active Directory database for that domain.
- **Function:** Domain controllers are responsible for authenticating users and computers, enforcing security policies, and maintaining the directory database for their domain. They replicate changes with other domain controllers to ensure consistency.
- **Role in a Forest:** In a forest, domain controllers exist for each domain, and at least one domain controller in each domain holds the Global Catalog (GC) role, which stores a partial copy of all objects in the forest.

Organizational Units serve two main purposes:

- **Delegated administration:**

Organizational units allow administrators to assign admin rights to users that are only valid within a specific OU. This helps restrict the control of individual admins in accordance with the principle of least privilege.

- **Managing Group Policy:**

Group policy objects (GPOs) let admins manage a variety of settings for users and devices in Windows networks.

- **Group Policy:**

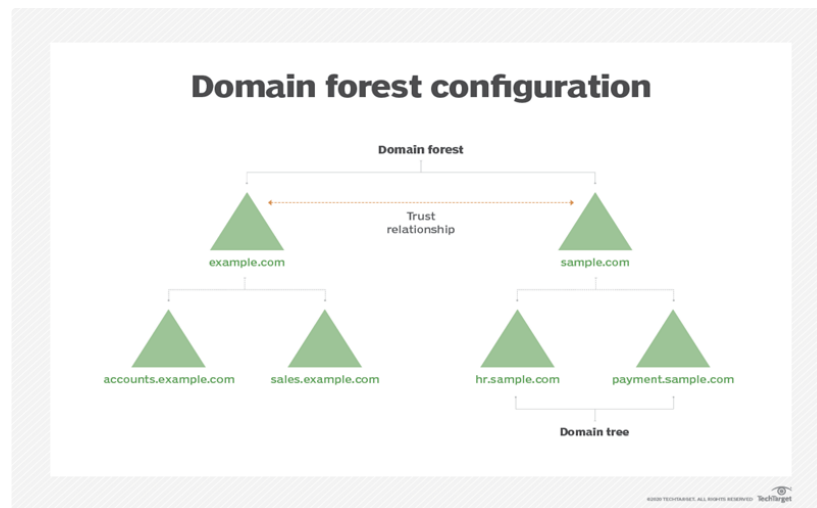
Allows the system administrator to have centralized control of users and computers on the network. Settings can be configured like desktop settings, printers, and login scripts etc.

Working Principle of Group Policy:

Firstly, the administrator and active directory will configure the settings on domain controller, then settings are pushed to server and desktop, further group policy can create separate group for users by which we can restrict the number of users.

Group policy mechanics:

1. Driven by client-side extensions.
2. Depending on the operating systems.
3. Option CSE's for older clients.



Domain Forest Configuration

Domain Creation and System Joining Task:

Steps to create domain and system joining task:

1. Install Windows 12 R2 in virtual machine using virtual box.
2. Go to virtual machine and click on devices and create new disk and drive, click on Guest VSO, and go to devices and click on insert guest option.
3. We get a pop-up of CD- Drive by clicking it we get Install Windows 10 Pro in another virtual machine. A pop-up for installing virtual box extensions.
4. After installing we need to reboot.
5. Next step is to open server manager dashboard and go to add new roles and features.
6. By clicking it we need to make active directory domain services active and install everything we need.
7. To create a new forest, we need to click on promote this server to a domain and here we can create a new forest. Which is defined as the collection of domains.
8. Give a name to the domain, for example KTG.local it can be given as .com, .org, .local, etc.
9. After that we can create a new password, next step is NetBIOS after checking everything we get a line that all checks are passed, then we should click install.
10. By completing the installation process, we get pop-up of signed out we should close it, now we need to restart the VM.
11. After a restart login account which we created as KTG.local/Administrator will appear.
12. Here we created a domain, but it is not created to host the OS. Now we are going to create a network.
13. Part-2 is to create a network, to create this we need to go to the tools and open Active directory domain services users and computers.
14. Now open KTG and go to users, by right clicking on users we get option new, go to users and create username and password, and click finish.
15. Now open another virtual machine installed with windows 10 pro and make a settings of bridge adapter to adapter1 and NAT to adapter2.
16. The bridge adapter helps to connect the machines' local network to the host local network.
17. Basically, we connected through a cable from VM.
18. Now we are going to turn off fire wall from the windows firewall so that connections can be made easily.
19. After the firewall we are going to change the settings of our ethernet network. We should disable IPv6 services in both VM's.
20. Make sure of IP address and check the connection between the two VM's which is the most important part.
21. Change the DNS server of windows 10 VM to IP address of windows 12 VM.
22. Open this pc and go to properties to change the settings in windows 10.
23. Open the advanced settings and allow the remote access settings to this computer and change the name of the system as Windows10 pro, now we get a restart pop-up.

24. After getting restart we are going to join the system to the domain.
25. So, we set it to be able to communicate with the domain in terms of network connections of the domain, so we are going to set the preferred DNS server to be address of domain.
26. By giving the domain name we are able create an account in windows 10 with a new username and password.
27. After this we get a restart, here we can see the new user account in logon windows.
28. The final step is to check the account we created in windows 10 VM in Active directory. Open the dashboard of server manager and go to users we can find a domain account of windows 10.

The key difference between a Bridged Adapter and a NAT Adapter in VirtualBox is the level of network integration and accessibility:

- A Bridged Adapter provides **full integration with the external network, with the VM having its own IP address and being directly accessible from the external network.**
- A NAT (**Network Address Translation**) Adapter allows the VM to access the **external network by sharing the host's IP address, but it keeps the VM isolated from inbound connections on the external network.** It provides a level of security and is suitable for outbound internet access while keeping the VM hidden from external devices.