

Operating system

1. Server OS <ul style="list-style-type: none">- which SERVES- ex:<ul style="list-style-type: none">○ windows server NT○ windows server 2003○ windows server 2008/2008R2○ windows server 2012/2012R2○ windows server 2016○ windows server 2019○ windows server 2022○ windows server 2025	2. Client OS <ul style="list-style-type: none">- sends requests- ex:<ul style="list-style-type: none">○ Windows XP○ Windows Vista○ Windows 7○ Windows 8○ Windows 8.1○ Windows 10○ Windows 11
---	--

Active Directory

- It's a directory service that stores user's information.
- AD performs 2 "A"
 - Authentication
 - Authorization

DHCP

- Dynamic Host Configuration Protocol
- The job is to provide IP address to client dynamically.

DNS

- Domain Name System
- The job of DNS is to resolve names to IP.

Group Policy

- Allow you to manage the users and computers within an organization.
-

Domain → for companies

- It is a logical administrative boundary of an organization.
- You (admin) can control anything and everything within this boundary.
- If any server/client/computer is domain-joined, then this system is totally controlled by the domain admin.
 - Changing the wallpapers.
 - Disabling the USB ports.
 - Disabling the control panel
 - Enabling/forcing the firewall.

Workgroup → individual users

- It is a standalone machine (its not part of any domain)
- It can be managed by the local admins

After the installation of a new windows server OS: - “Post Installation Configuration”

- ✓ Set the IP address.
 - Dynamically using “DHCP server”. OR
 - Manually → “ncpa.cpl”
- ✓ Change the date and time zone
- ✓ Disable the firewall (req. in testing environment). Never do this in production.
 - Public Firewall
 - Private firewall
 - Domain firewall (only after the domain joining of the computer).
- ✓ Change the computer/system name → Reboot your computer.

Note – *These settings must be updated on DC, Node01 and Node02 machines.*

For DC machine:

- IP address: 192.168.10.10
- Subnet Mask: 255.255.255.0
- Default gateway: 192.168.10.10
- DNS: 192.168.10.10
- Hostname: DC
- Firewall: OFF

For Node01 machine:

- IP address: 192.168.10.11
- Subnet Mask: 255.255.255.0
- Default gateway: 192.168.10.10
- DNS: 192.168.10.10
- Hostname: Node01
- Firewall: OFF

For Node02 machine:

- IP address: 192.168.10.12
- Subnet Mask: 255.255.255.0
- Default gateway: 192.168.10.10
- DNS: 192.168.10.10
- Hostname: Node02
- Firewall: OFF

Ping using IP/Name

- DC ↔ Node01
- Node01 ↔ Node02
- Node02 ↔ DC

Adding disk(s) on → DC machine

- Add a new disk using VMWare workstation
- Go to disk management console
 - o Right-click on Windows icon and select Disk management.
 - o Run → “diskmgmt.msc”
- Right-click on the new added disk, select “Online” option.
- Again right-click on this disk and select “Initialize Disk”.
- Right-click on the disk and create a new simple volume.
- Go to this PC and verify.

MBR	GPT
<ul style="list-style-type: none">• Master Boot Record• Old way to create partitions on an HDD.• Primary partitions: 4• Supports HDD capacity up to: 2TB	<ul style="list-style-type: none">• GUID (Globally Unique Identifier) Partition Table• New way to create partitions on an HDD.• Primary partitions: 128• Supports HDD capacity up to: 18Exabytes

Tasks

- Create a total of 3 VMs
 - o Domain controller (DC)
 - o Nodes (Node01 and Node02)
- Perform the post installation on all the 3 VMs.
- Ping all the 3 VMs using IP address.
- Add 2 disks, each of 10GB and ensure that the disks are in GPT format on domain controller (DC) machine.

Installation methods of Windows Server:

- DVD / ISO file
- WDS (Windows Deployment Service) – Network-based installation
 - o WDS is a role and thus it will be installed only on a server OS.
- Pen drives

Server Manager Dashboard Page:

- Dashboard page is a graphical tool (GUI).
- You can manage your local system and remote systems as well.
- We can manage:
 - o Local computer (post-installation configuration)
 - o Install, uninstall a role or a feature in your local machine.
 - o Install, uninstall a role or a feature in your remote machine.
 - o Manage disks
 - o Look and manage the logs, events.
- Alternative is PowerShell (commands, scripts).

Administrative tools:

- Active directory Administrative Center
 - o Manages the users, computers, groups, group policies.
- Active directory users and computers
 - o Manages the users (create, modify, delete) and computers.
- DNS Console
 - o Manages the DNS records
- Performance Monitor (Perfmon)
 - o This looks into the performance of your computers.
- Task Scheduler
 - o Schedules the task.
- IIS Manager
 - o Creating and updating the web pages.
 - o Helps in creating the SSL certificates.

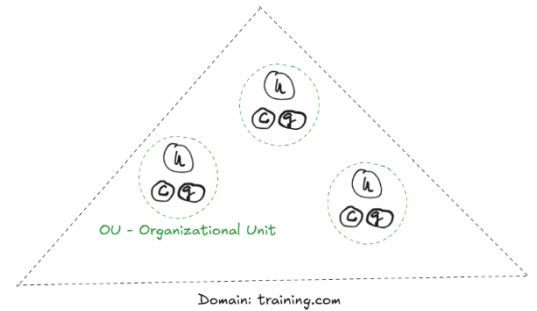
Windows Active Directory (WAD):

- Aka Active Directory (AD)
- It's a directory service developed by Microsoft.
- To store the users, computers information
- It stores the objects:
 - o Users
 - o Groups
 - o Computers
- AD performs:
 - o Authorization
 - o Authentication
 - o Accounting
- You can manage:
 - o Network resources
 - o Policies
 - o User accounts
 - o What users can "access".
- To achieve all this, we need to install a role "**Active Directory Domain Services (AD DS)**".

Terms used in AD / AD Concepts:

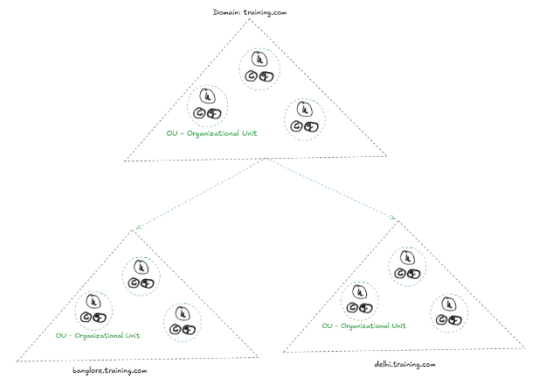
Domain

- It is the logical administrative boundary of an organization.
- In a diagram, it is represented by a 'triangle'.
- A domain is a collection of domain objects:
 - o Users
 - o Computers
 - o Groups
- These objects are stored in a database 'NTDS.DIT'.
 - o NTDS.DIT = New Technology Directory Service.Directory
- Questions
 - o List the domain objects
 - o What is the database name of Active Directory.



Tree

- It's the hierarchy of domains and sub-domains
- It's the collection of various sub-domains.



Forest

- Forest is the collection of trees.
- It shares the same schema (blueprint)

Schema

- It's the blueprint
- This defines the type of objects (user, computer and groups) created in the AD.

Organizational Unit (OU)

- It's like a department
- These OU contains
 - o Users
 - o Computers
 - o Groups
- There are some pre-defined OUs created, after creating a domain.

Global Catalog (GC) Server

- GC is a searchable index for quick search of any object within domain.
- This GC gets installed during the promotion of a domain controller.

Site

- It refers to the physical, geo-graphical location within a domain.
- Ex:
 - o BLR.training.com, Delhi.training.com, India.training.com

Group Policy

- It's a policy which is applied on the domain objects.
- This policy can centrally manage:
 - o Users, Computers, Groups
 - o Login time
 - o Files and folder access permissions
 - o Security, Wallpapers, Drive access.

AD Components:

1. Physical component

- a. *Domain Controller (DC)*
 - i. It controls the domain.
 - ii. It's a server machine that manages the complete domain.
 - iii. It contains the AD database file (NTDS.DIT)
- b. *Data store*
 - i. Data store is a file on domain controller that stores the AD information.
- c. *Global Catalog server*
 - i. It's a server that host "read-only copy" of all objects for quick search.
- d. *Read-Only Domain Controller (RODC)*
 - i. RODC is a special type of DC.
 - ii. We cannot write anything to this RODC, but we can only READ from it.
 - iii. RODC is useful in the branch offices.

2. Logical component

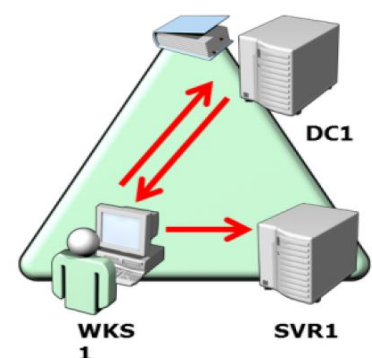
- a. Partition
 - i. Logical sub-division of the NTDS.DIT database.
- b. Domain
 - i. Logical admin boundary
- c. Trees
 - i. Collection of domains
- d. Forest
 - i. Collection of trees
- e. Site
 - i. Physical location
- f. OU
 - i. Like a department.

Types of domain controllers (DCs)

- Domain controller (DC)
- Additional Domain Controller (ADC)
- Backup Domain Controller (BDC)
- Read-Only Domain Controller (RODC)
- Primary Domain Controller (PDC)

AD Logon process:

- User provides username and password and then it gets authenticated by DC.
- DC returns the TGT (Ticket Granting Token).
- Using this TGT, client/user applies to login to the WKS.
- Client is then allowed to login to SVR1



Operation Masters

- Aka FSMO (Flexible Single Master Operation) roles
- This is a special type of domain controller role, that allows only one DC to perform any job without any conflict.
- There are 5 FSMO roles
- These FSMO roles are applied on
 - Forest-level
 - Domain Naming Master
 - Schema Master
 - Domain-level
 - RID Master
 - PDC Emulator/Master
 - Infrastructure Master

Domain Naming Master

- ✓ Adding a new domain to the forest.
- ✓ Removing an existing domain from the forest.
- ✓ Present One-Per Forest.

Schema Master

- ✓ Present One-Per Forest.
- ✓ Control all the updates and modifications to the AD schema.
- ✓ One-blue print through-out forest.

RID Master

- ✓ Relative Identity (ID) Master
- ✓ One-per domain
- ✓ It provides a set of (500 RID) and allocate these individuals RIDs to every domain object.
- ✓ Without RID, you cannot create new users, computers or groups within a domain.

PDC Emulator

- ✓ Makes your machine back compatible.
- ✓ It handles the password change.
- ✓ It also manages the account lockout.
- ✓ It maintains the time across the domain.
- ✓ Useful during the authentication of the user, GPO updates, time sync.
- ✓ One-per domain

Infrastructure Master

- ✓ Related to the updates of objects in another domain.
- ✓ Cross-domain object reference.
- ✓ One-per domain

How to create a Domain Controller (DC):

- ✓ You need to install a Windows Server OS.
- ✓ Then perform the post-installation configuration:
 - Change computer name → DC
 - Change the IP to static IP → 192.168.10.10
 - Change the firewall → OFF
 - Change the time zone → +05:30 ...
- ✓ You need to install the AD DS role on DC machine.
 - GUI → Server Manager Dashboard page
 - CLI → PowerShell command
- ✓ Promote this server to “Domain Controller”
- ✓ Fill the details of domain:
 - Domain name: Training.com
 - GC, RODC ...
- ✓ Restart the DC machine, and after restart login with domain admin.
 - Local administrator → administrator
 - Domain administrator → domain_name\administrator
 - Ex: training\administrator OR
 - administrator@training.com

Storage Spaces:

- Storage spaces allow you to virtualize the storage on your server.
- In this, we pool (club/combine) multiple disks together to form one single-unit.
- Storage pool – is a collection of various physical disks.
- Thin provisioning – allocate the disk size as per requirement.
- Minimum requirement:
 - 2 identical disks are needed for simple/mirror volume.
 - 3 identical disks are needed for parity disks.
- To manage storage spaces:
 - Server manager dashboard page
 - PowerShell cmdlets
 - Windows Admin Center
- Steps to create a storage space → “DC machine”
 - Add 2 physical disks to you DC machine → “Unallocated disks”
 - Create a “storage pool” from these 2 disks.
 - Create a “virtual disk” (storage space) from this pool.
 - Select resiliency, size, provisioning type.
 - Format this new disk into required file system
 - FAT32 (File Allocation Table)
 - NTFS (New Technology File System)
 - ReFS (Resilient File System)
 - Assign a drive letter to it.
 - Then start using it.