- 2. 2. Domain Management -

- INDEX -

- 2. 2. 1. Windows Domains and Active Directory -

Windows Domain

A Windows domain is a form of a computer network in which all user accounts, computers, printers and other security principals, are registered within a central database located on one or more clusters of central computers known as domain controllers.

Authentication takes place on domain controllers.

Each person who uses computers within a domain receives a unique user account that can then be assigned access to resources within the domain.

Starting with Windows 2000, Active Directory is the Windows component in charge of maintaining that central database.

The concept of Windows domain is in contrast with that of a workgroup in which each computer maintains its own database of security principals.

Windows Workgroup

Windows Workgroups, by contrast, is the other model for grouping computers running Windows in a networking environment which ships with Windows.

Workgroup computers are considered to be 'standalone' – i.e. there is no formal membership or authentication process formed by the workgroup.

A workgroup does not have servers and clients, and hence represents the peer-to-peer (or client-to-client) networking paradigm, rather than the centralized architecture constituted by Server-Client.

Workgroups are considered difficult to manage beyond a dozen clients, and lack single sign on, scalability, resilience/disaster recovery functionality, and many security features.

Windows Workgroups are more suitable for small or home-office networks.

Domain Controller

In a Windows domain, the directory resides on computers that are configured as "domain controllers" (DCs).

A domain controller (DC) is a Windows server that manages all security-related aspects between user and domain interactions, centralizing security and administration.

A domain controller is generally suited for businesses and/or organizations when more than 10 PCs are in use.

A domain does not refer to a single location or specific type of network configuration.

The computers in a domain can share physical proximity on a small LAN or they can be located in different parts of the world.

As long as they can communicate, their physical position is irrelevant.

Directory service

In computing, directory service or name service maps the names of network resources to their respective network addresses.

It is a shared information infrastructure for locating, managing, administering and organizing everyday items and network resources, which can include volumes, folders, files, printers, users, groups, devices, telephone numbers and other objects.

A directory service is a critical component of a network operating system.

A directory server is a server which provides such a service.

Each resource on the network is considered an object by the directory server.

Information about a particular resource is stored as a collection of attributes associated with that resource or object.

A directory service defines a namespace for the network.

The namespace is used to assign a “name” (unique identifier) to each of the objects.

Directories typically have a set of rules determining how network resources are named and identified, which usually includes a requirement that the identifiers be unique and unambiguous.

When using a directory service, a user does not have to remember the physical address of a network resource; providing a name locates the resource.

Some directory services include access control provisions, limiting the availability of directory information to authorized users.

Active Directory

Active Directory (AD) is a directory service that Microsoft developed for Windows domain networks.

It is included in most Windows Server operating systems as a set of processes and services.

Initially, Active Directory was only in charge of centralized domain management.

Starting with Windows Server 2008, however, Active Directory became an umbrella title for a broad range of directory-based identity-related services.

A server running Active Directory Domain Services (AD DS) is called a domain controller.

It authenticates and authorizes all users and computers in a Windows domain type network—assigning and enforcing security policies for all computers and installing or updating software.

For example, when a user logs into a computer that is part of a Windows domain, Active Directory checks the submitted password and determines whether the user is a system administrator or normal user.

Also, it allows management and storage of information at admin level and provides authentication and authorization mechanisms and a framework to deploy other related services (AD Certificate Services, AD Federated Services, etc.).

Active Directory uses Lightweight Directory Access Protocol (LDAP) versions 2 and 3, Microsoft’s version of Kerberos, and DNS.

Active Directory: Logical structure

As a directory service, an Active Directory instance consists of a database and corresponding executable code responsible for servicing requests and maintaining the database.

The executable part, known as Directory System Agent, is a collection of Windows services and processes that run on Windows Server.

Objects in Active Directory databases can be accessed via LDAP, ADSI (a component object model interface), messaging API and Security Accounts Manager services.

Active Directory: Objects

Active Directory structures are arrangements of information about objects.

The objects fall into two broad categories: resources (e.g., printers) and security principals (user or computer accounts and groups).

Security principals are assigned unique security identifiers (SIDs).

Each object represents a single entity—whether a user, a computer, a printer, or a group—and its attributes.

Certain objects can contain other objects.

An object is uniquely identified by its name and has a set of attributes—the characteristics and information that the object represents— defined by a schema, which also determines the kinds of objects that can be stored in Active Directory.

The schema object lets administrators extend or modify the schema when necessary.

However, because each schema object is integral to the definition of Active Directory objects, deactivating or changing these objects can fundamentally change or disrupt a deployment.

Schema changes automatically propagate throughout the system.

Once created, an object can only be deactivated—not deleted.

Changing the schema usually requires planning.

Active Directory: Forests, trees, and domains

The Active Directory framework that holds the objects can be viewed at a number of levels.

The forest, tree, and domain are the logical divisions in an Active Directory network.

Within a deployment, objects are grouped into domains.

The objects for a single domain are stored in a single database (which can be replicated).

Domains are identified by their DNS name structure, the namespace.

A domain is defined as a logical group of network objects (computers, users, devices) that share the same Active Directory database.

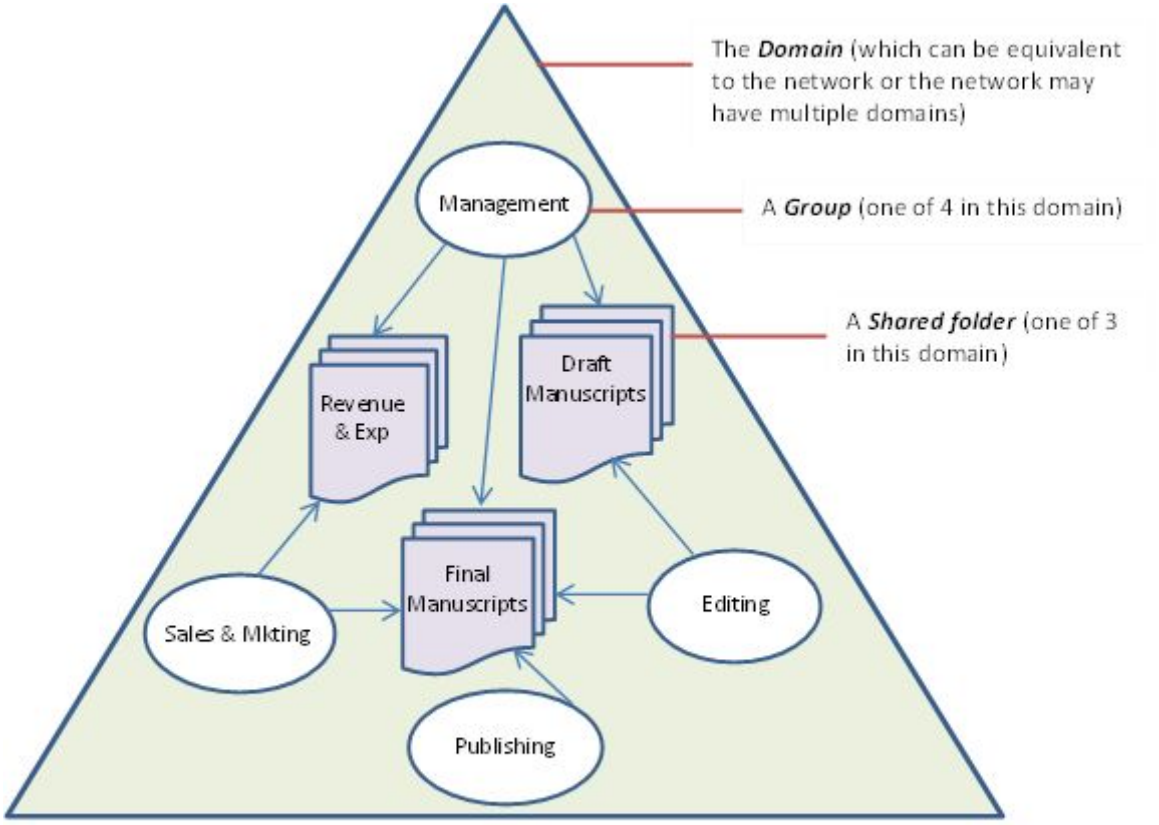
A tree is a collection of one or more domains and domain trees in a contiguous namespace, linked in a transitive trust hierarchy.

At the top of the structure is the forest.

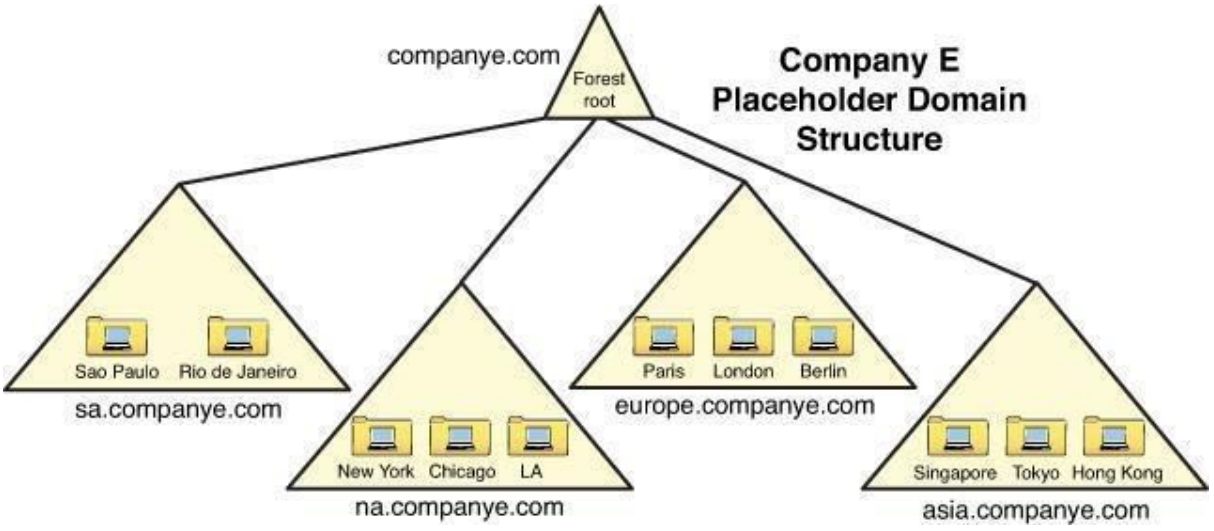
A forest is a collection of trees that share a common global catalog, directory schema, logical structure, and directory configuration.

The forest represents the security boundary within which users, computers, groups, and other objects are accessible.

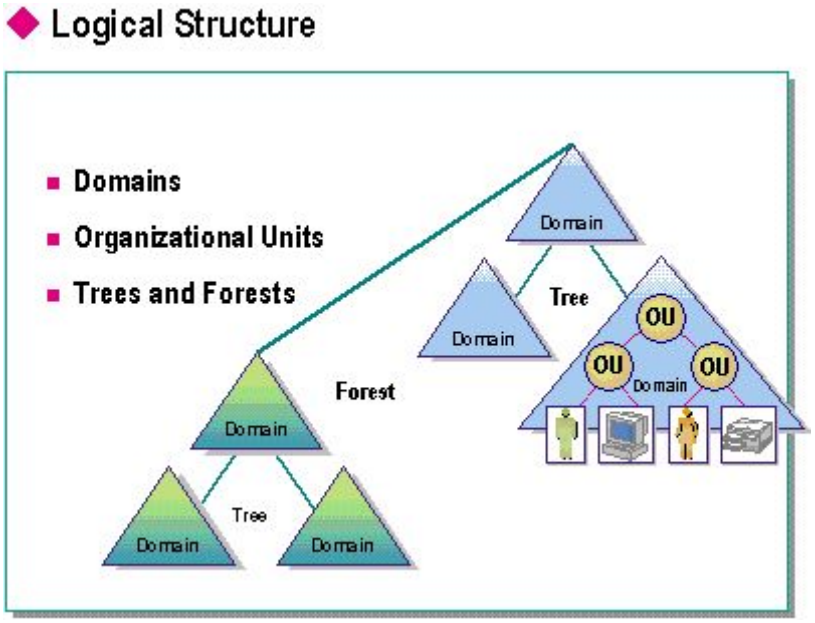
In the following image you can see the logical structure of a domain:



In the following image you can see the logical structure of a tree:



In the following image you can see the logical structure of a forest:



Organizational units

The objects held within a domain can be grouped into Organizational Units (OUs).

OUs can provide hierarchy to a domain, ease its administration, and can resemble the organization's structure in managerial or geographical terms.

OUs can contain other OUs—domains are containers in this sense.

Microsoft recommends using OUs rather than domains for structure and to simplify the implementation of policies and administration.

The OU is the recommended level at which to apply group policies, which are Active Directory objects formally named Group Policy Objects (GPOs), although policies can also be applied to domains or sites.

The OU is the level at which administrative powers are commonly delegated, but delegation can be performed on individual objects or attributes as well.

Organizational units do not each have a separate namespace; e.g. user accounts with an identical username (sAMAccountName) in separate OUs within a domain are not allowed, such as "fred.staff-ou.domain" and "fred.student-ou.domain", where "staff-ou" and "student-ou" are the OUs.

This is because sAMAccountName, a user object attribute, must be unique within the domain.

As the number of users in a domain increases, conventions such as “first initial, middle initial, last name” (Western order) or the reverse (Eastern order) fail for common family names like Li (李), Smith or Garcia.

Workarounds include adding a digit to the end of the username.

Alternatives include creating a separate ID system of unique employee/student id numbers to use as account names in place of actual user’s names, and allowing users to nominate their preferred word sequence within an acceptable use policy.

Because duplicate usernames cannot exist within a domain, account name generation poses a significant challenge for large organizations that cannot be easily subdivided into separate domains, such as students in a public school system or university who must be able to use any computer across the network.

Active Directory: Physical structure

Sites are physical (rather than logical) groupings defined by one or more IP subnets.

Active Directory (AD) also holds the definitions of connections, distinguishing low-speed (e.g., WAN, VPN) from high-speed (e.g., LAN) links.

Site definitions are independent of the domain and Organizational Unit (OU) structure and are common across the forest.

Sites are used to control network traffic generated by replication and also to refer clients to the nearest domain controllers (DCs).

Microsoft Exchange Server (email server) uses the site topology for mail routing.

Policies can also be defined at the site level.

Physically, the Active Directory information is held on one or more peer domain controllers (DCs).

Each Domain Controller (DC) has a copy of the Active Directory.

Servers joined to Active Directory that are not domain controllers are called Member Servers.

A subset of objects in the domain partition replicate to domain controllers that are configured as global catalogs.

Global catalog (GC) servers provide a global listing of all objects in the Forest.

Global Catalog servers replicate to themselves all objects from all domains and hence, provide a global listing of objects in the forest.

However, to minimize replication traffic and keep the GC's database small, only selected attributes of each object are replicated.

This is called the partial attribute set (PAS).

The PAS can be modified by modifying the schema and marking attributes for replication to the GC.

Earlier versions of Windows used NetBIOS to communicate.

Active Directory is fully integrated with DNS and requires TCP/IP—DNS.

To be fully functional, the DNS server must support SRV resource records, also known as service records.

In general, a network utilizing Active Directory has more than one licensed Windows server computer.

Backup and restore of Active Directory is possible for a network with a single domain controller, but Microsoft recommends more than one domain controller to provide automatic failover protection of the directory.

Domain controllers are also ideally single-purpose for directory operations only, and should not run any other software or role.

Certain Microsoft products such as SQL Server (database server) and Exchange (email server) can interfere with the operation of a domain controller, necessitating isolation of these products on additional Windows servers.

Combining them can make configuration or troubleshooting of either the domain controller or the other installed software more difficult.

A business intending to implement Active Directory is therefore recommended to purchase a number of Windows server licenses, to provide for at least two separate domain controllers, and optionally, additional domain controllers for performance or redundancy, a separate file server, a separate Exchange server, a separate SQL Server, and so forth to support the various server roles.

Physical hardware costs for the many separate servers can be reduced through the use of virtualization, although for proper failover protection, Microsoft recommends not running multiple virtualized domain controllers on the same physical hardware.

Active Directory: Management solutions

Microsoft Active Directory management tools include:

- Active Directory Users and Computers.
- Active Directory Domains and Trusts.

- Active Directory Sites and Services.
- ADSI Edit.
- Local Users and Groups.
- Active Directory Schema snap-ins for Microsoft Management Console (MMC).

- Vocabulary -

- i.e.: "id est" (latin), that is, esto es.
- e.g.: "exempli gratia" (latin), for example, por ejemplo.

- 2. 2. 2. Installing Active Directory Domain Services -

You are going to create a new Google Document inside the "2. Windows Server" folder of your Google Drive, named:

"2. 2. Domain Management - Apellidos, Nombre"

being "Apellidos, Nombre" your Last Name and Name.

Inside this Google Document you are going to copy and answer all the "Exercises" of this sub-unit.

- Exercise 1 -

Go to the real computer where you have installed Windows Server 2019. Open "VirtualBox". Start the “Windows Server 2019” virtual machine, if you don't already have started it yet. Login to your “Windows Server 2019” virtual machine.

1. Open “Server Manager” and select “Dashboard” on the left column -> Welcome to server manager -> Quick start -> 1 Configure this local server -> 2 Add roles and features.
   On the “Add Roles and Features Wizard” window -> “Next” -> “Next” -> “Next” -> “Select server roles”: select “Active Directory Domain Services” -> “Add Features”-> “Next” -> “Next” -> “Next” -> “Install”. **Screenshot**. Then: “Close”.
2. After the “Active Directory Domain Services” Role has been installed, restart the server. Open “Server Manager” and click on the “yellow warning” located in the flag icon. Then, click on “Promote this server to a domain controller”.
   On the “Active Directory Domain Services Configuration Wizard”, on “Deployment Configuration”, “Select the deployment operation”: choose “Add a new forest”. On “Root domain name” write: “SI-XY.LOCAL” being XY the last 2 digits of your real computer’s IP (your real computer, not your partner’s real computer). **Screenshot**. Click “Next”.
3. On “Domain Controller Options” -> Forest functional level: “Windows Server 2016” -> Domain functional level: “Windows Server 2016”. On “Specify domain controllers capabilities”: check “Domain Name System (DNS) server”, and check “Global Catalog (GC)”. For the password, type “Balmis1”. **Screenshot**. Click “Next”.
   On “DNS Options”, DO NOT check “Create DNS delegation”. Click “Next”.

On “Additional Options”, DO NOT change “The NetBIOS domain name”. Click “Next”.
On “Paths” -> Click “Next”.
On “Review Options” -> Click “Next”.

4. On “Prerequisites Check”, after the window loads completely, **screenshot** -> Click “Install”.
   Wait until the “Active Directory Domain Services Configuration Wizard” finishes the installation.
   “You’re about to be signed out” blue window -> Click “Close”.
   The server will restart: this can take some minutes.
5. After restarting, login with user “NAME-OF-YOUR-DOMAIN\Administrator” and password “Balmis1”, taking a **screenshot**.
6. Open “Server Manager” and select “Dashboard” on the left column. Scroll down to “ROLE AND SERVER GROUPS” and check the Roles that you have installed and running (green color) on your server. Now you should have 2 new Roles: “AD DS” (Active Directory Domain Services) and “DNS”.
   Go the Start button -> Windows Administrative Tools. You should have like 6 new programs named “Active Directory …”, take a **screenshot**.
7. Click on “Active Directory Users and Computers” to open this program and check it out. Now you have installed “Active Directory Domain Services”: you have a Windows Domain fully functional and your Windows Server is a Domain Controller. **Screenshot**.

- 2. 2. 3. Adding a computer (Windows 10 client) to the Domain -

- Exercise 2 -

With a partner, one first does these exercises and then the other one. Close Windows Server virtual machine and start your **Windows 10 (client) virtual machine**.

1. Go to the TCP/IP settings, and on “Preferred DNS server”, write the IP of your Windows Server machine. **Screenshot**.
2. Go to “File Explorer” -> “This PC” -> Right click “Properties” -> “Change settings” -> “Computer name” tab -> “Change” button -> Check “Domain” -> Write: “NAME-OF-YOUR-DOMAIN”. **Screenshot**.
3. It will prompt a window asking for a user with administrative permissions: write user “Administrator” and password “Balmis1”.
   After being welcomed to your domain, restart your Windows 10 (client) virtual machine.
   On the login window, write user “Administrator” and password “Balmis1” and login to your Windows 10 (client) virtual machine. **Screenshot**.