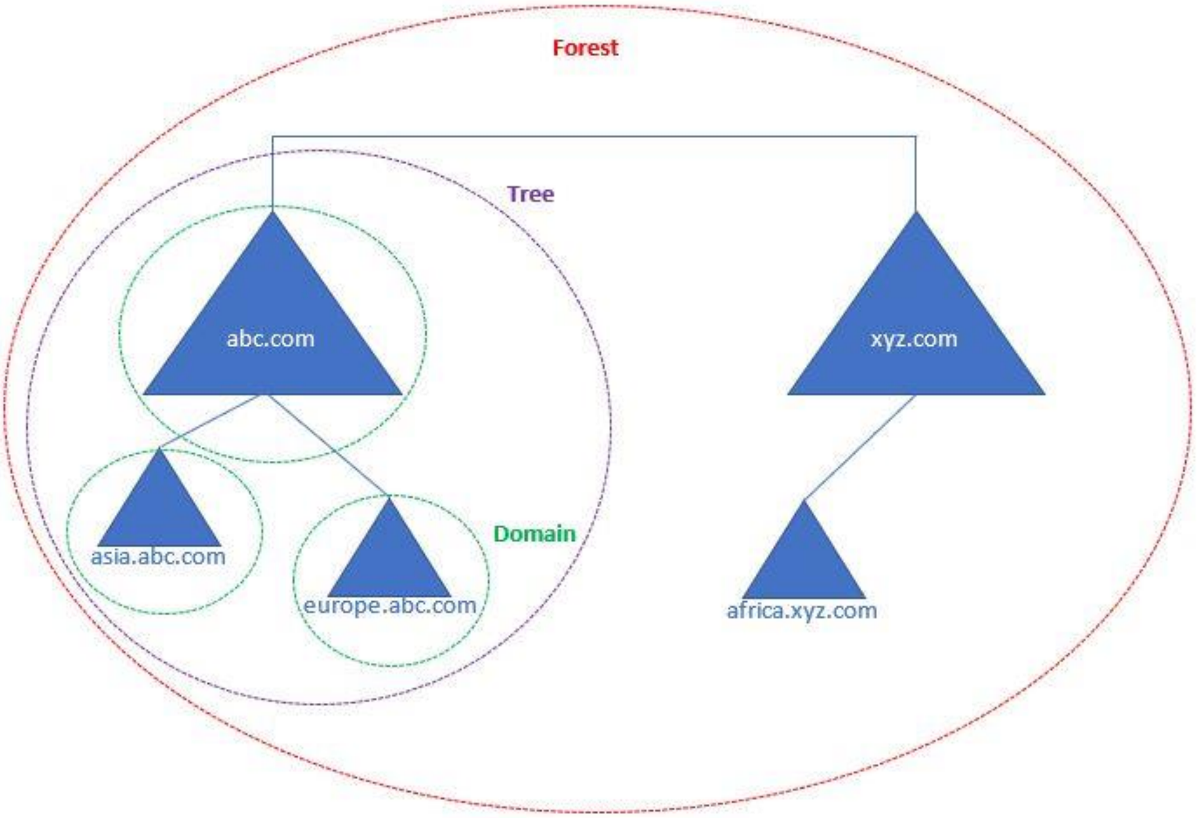
Domain Controller (DC)

- A domain controller is a server that responds to authentication requests and verifies users on computer networks.
- The domain controller keeps all of that data organized and secured.
- The domain controller (DC) is the box that holds the keys to the Active Directory (AD).
- The primary responsibility of the DC is to authenticate and validate user access on the network.
- When users log into their domain, the DC checks their username, password, and other credentials to either allow or deny access for that user.

ACTIVE DIRECTORY : DOMAIN CONTROLLER :: car : engine

- Active Directory is a type of domain, and a domain controller is an important server on that domain.
- Kind of like how there are many types of cars, and every car needs an engine to operate. Every domain has a domain controller, but not every domain is Active Directory.

Domains, Trees and Forests



- The best way to think of a forest is to imagine it in its traditional sense.
- A forest is a group of one or more trees.
- In the figure provided above, the outermost boundary is the forest or a group of one or more trees.
- The next layer is the tree.
- Unlike a forest, a tree must have a unique name.
- In the figure, there are two trees: 1) abc.com and 2) xyz.com.
- Trees are a group of one or more domains.
- A domain is a group of shared resources such as computers or users.
- The domains within a tree share the same namespace as the tree.
- For example, asia.abc.com and europe.abc.com share the same namespace as abc.com.

Functional Levels

- Functional levels determine the available Active Directory Domain Services (AD DS) domain or forest capabilities.
- They also determine which Windows Server operating systems you can run on domain controllers in the domain or forest.
- Functional levels do not affect which operating systems you can run on workstations and member servers that are joined to the domain or forest.

Organizational Unit (OU)

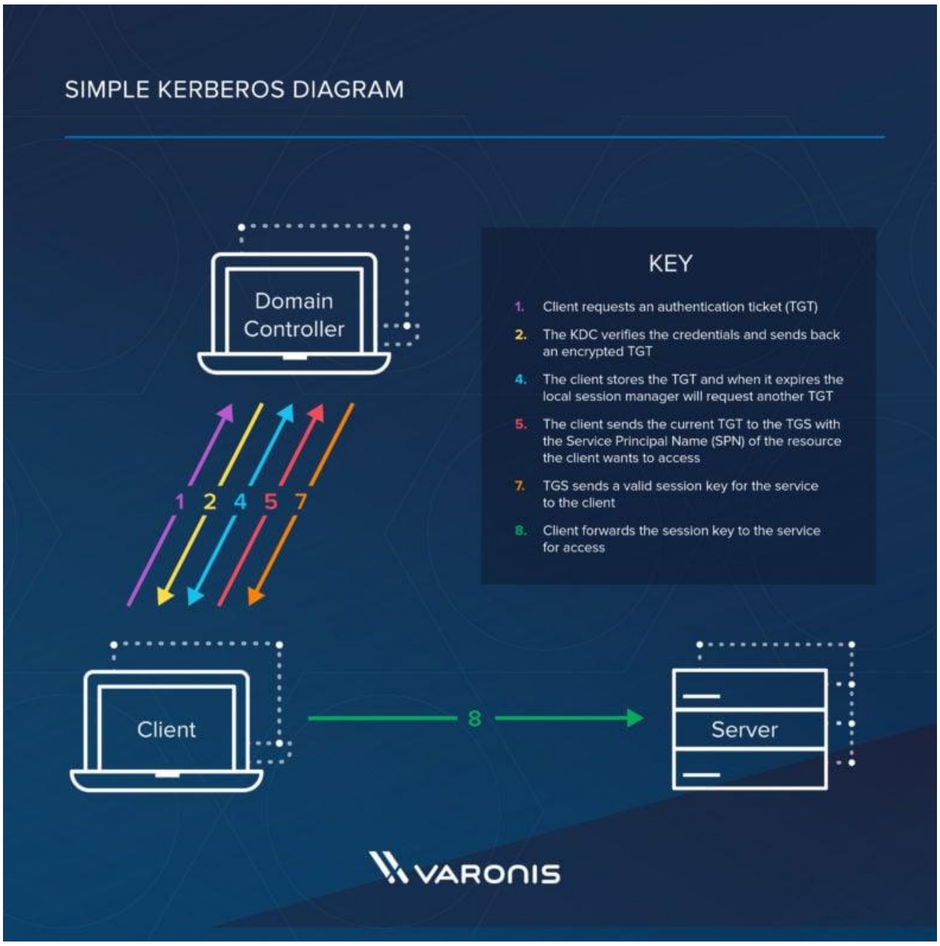
- An organizational unit (OU) is a subdivision within an Active Directory into which you can place users, groups, computers, and other organizational units.
- You can create organizational units to mirror your organization's functional or business structure.
- Each domain can implement its own organizational unit hierarchy.
- If your organization contains several domains, you can create organizational unit structures in each domain that are independent of the structures in the other domains.

Sites

- Sites are highly connected networks of IP subnets that define the physical structure of Active Directory (AD).
- These networks are highly reliable and fast, which is why it’s important to ensure that traffic for Active Directory change replication does not slow down the entire network and does not put load on domain controllers.
- Every AD site is mapped to an AD domain, and an AD domain can have multiple sites mapped to it.

Kerberos Authentication

- MIT Computer Scientists used the name and visual of Kerberos (3 headed dog that guards the hell) for their computer network authentication protocol.
- Kerberos uses symmetric key cryptography and requires trusted third-party authorization to verify user identities.
- Kerberos authentication is currently the default authorization technology used by Microsoft Windows, and implementations of Kerberos exist in Apple OS, FreeBSD, UNIX, and Linux.



KEY

1. Client requests an authentication ticket (TGT)
2. The KDC verifies the credentials and sends back an encrypted TGT
4. The client stores the TGT and when it expires the local session manager will request another TGT
5. The client sends the current TGT to the TGS with the Service Principal Name (SPN) of the resource the client wants to access
7. TGS sends a valid session key for the service to the client
8. Client forwards the session key to the service for access

Here are the most basic steps taken to authenticate in a Kerberos environment.

- Client requests an authentication ticket (TGT) from the Key Distribution Center (KDC)
- The KDC verifies the credentials and sends back an encrypted TGT and session key
- The TGT is encrypted using the Ticket Granting Service (TGS) secret key
- The client stores the TGT and when it expires the local session manager will request another TGT (this process is transparent to the user)

If the Client is requesting access to a service or other resource on the network, this is the process:

- The client sends the current TGT to the TGS with the Service Principal Name (SPN) of the resource the client wants to access
- The KDC verifies the TGT of the user and that the user has access to the service
- TGS sends a valid session key for the service to the client
- Client forwards the session key to the service to prove the user has access, and the service grants access.