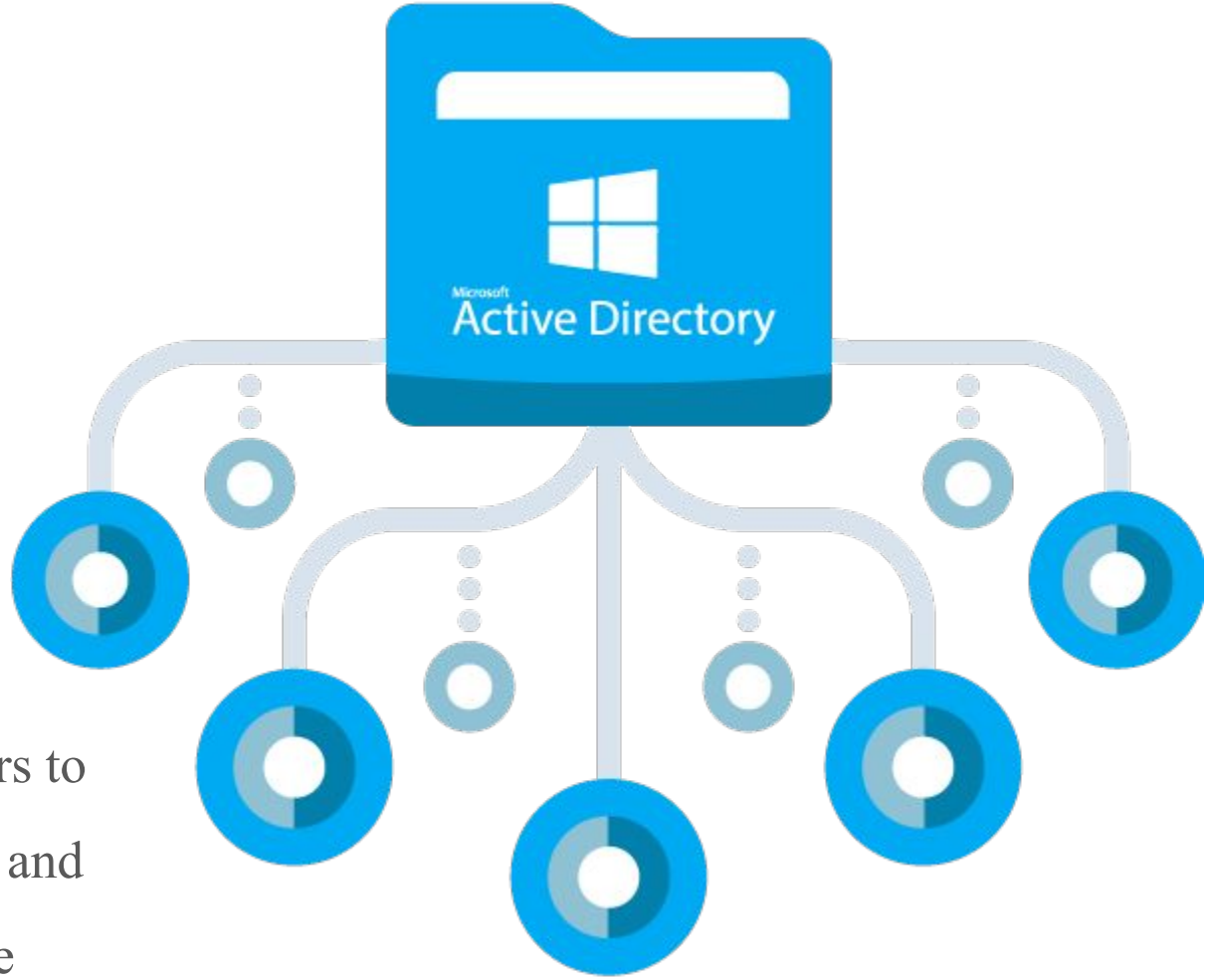
Introduction to Active Directory

Course Incharge: **Yahya Batla**

Course Instructor: **Umar Bilal**

What is Active Directory

Active Directory is a centralized directory service provided by Microsoft, used to manage and organize resources such as users, computers, and other network objects in a Windows domain environment.



AD enables administrators to authenticate and authorize users to access resources, enforce security policies, deploy software, and manage group policies across the network. It serves as a core component for managing and securing network infrastructure in Windows environments.

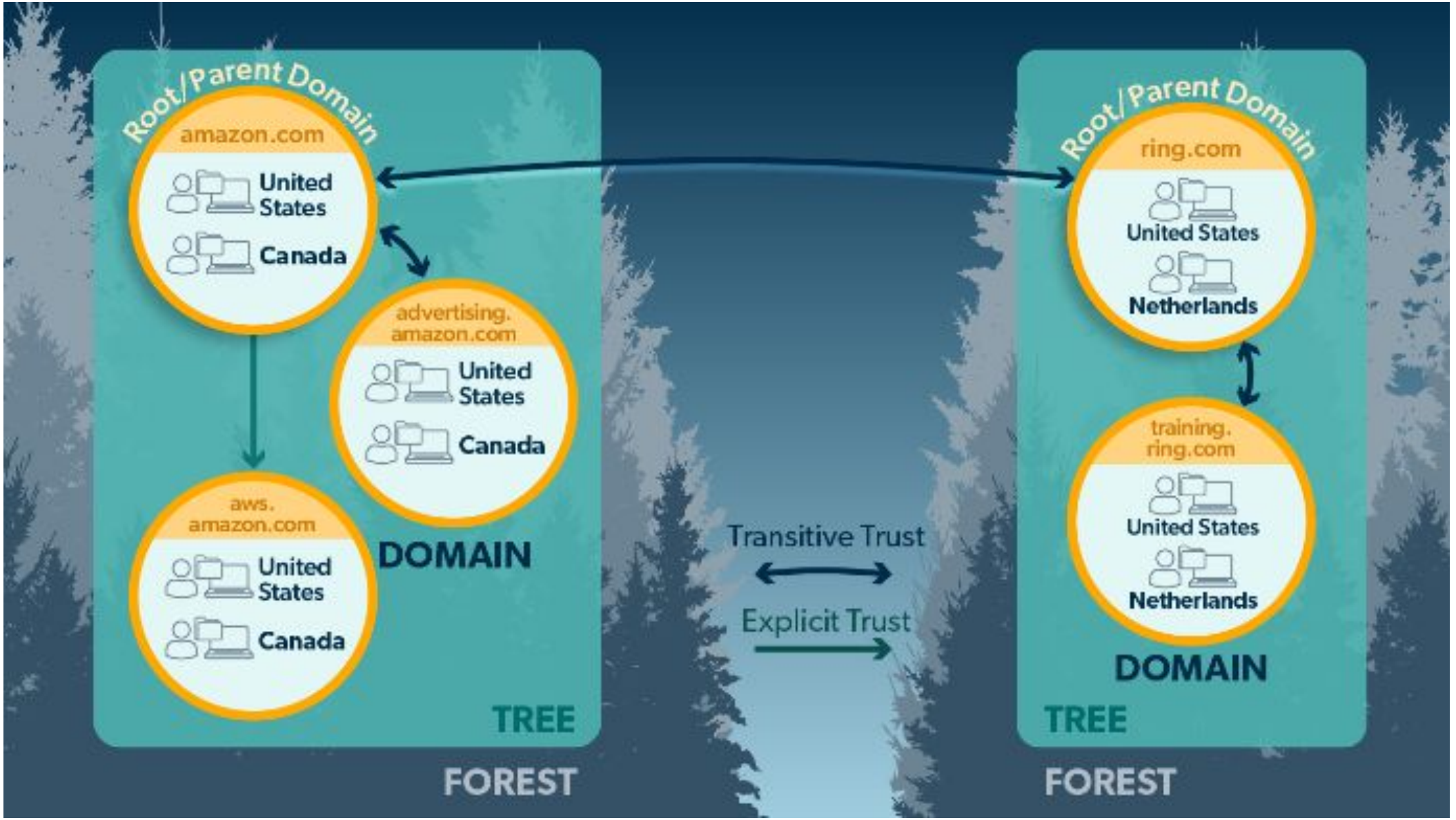
Purpose of Active Directory

Active Directory stores information as “objects”, which are any resources within the network, such as computers, user accounts, contacts, groups, organisational units and shared folders. Objects are categorised by name and attributes. The information is kept in a structured data store optimised to enhance query performance and scalability, which makes it easy for network users and applications to locate and use any needed bits of information. So, the purpose of Active Directory is to enable organisations to keep their network secure and organised efficiently.

Components of Active Directory

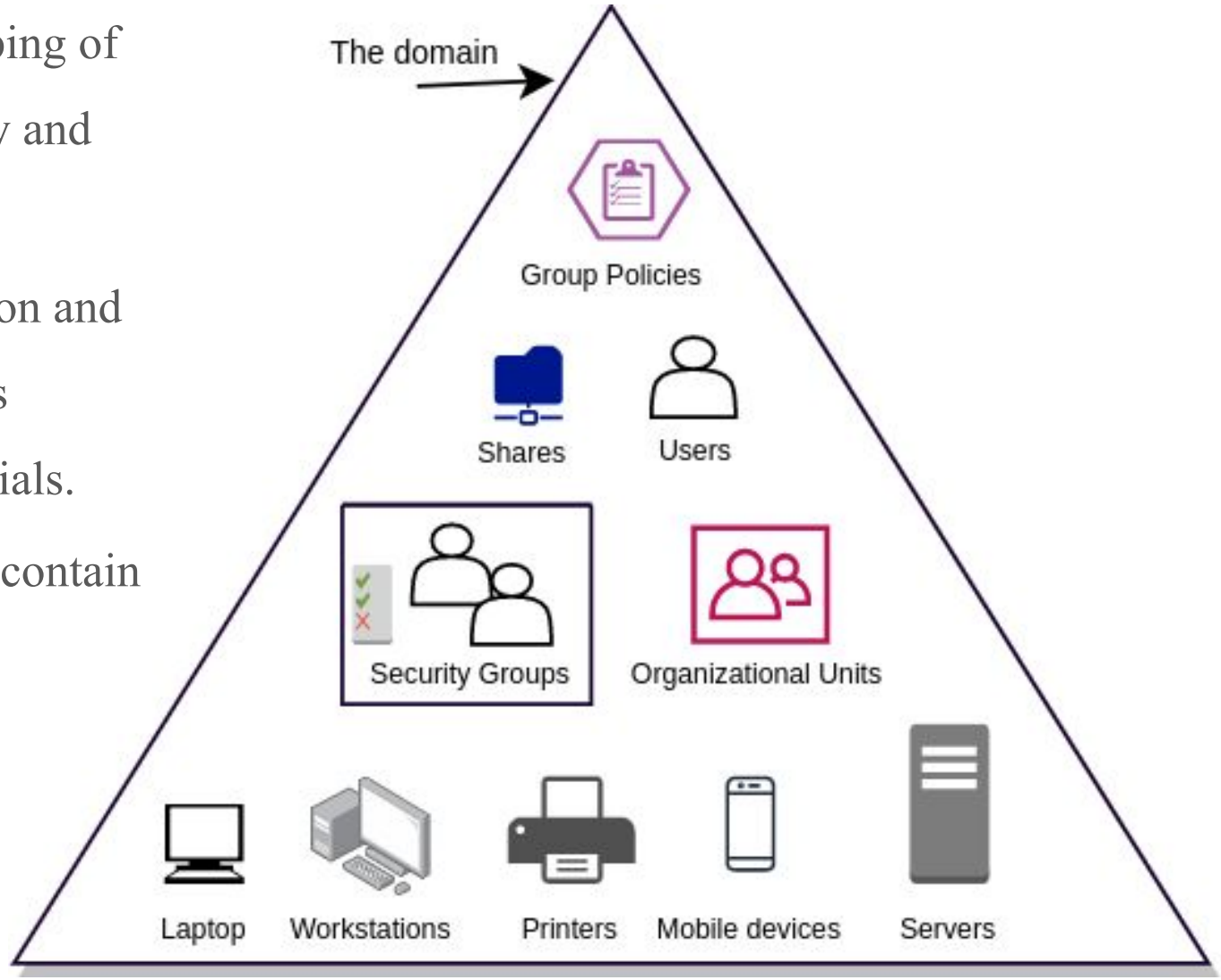
Active Directory stores information about network users (names, phone numbers, passwords, etc.) and resources (servers, storage volumes, printers, etc.) in a hierarchical structure consisting of domains, trees, and forests.

1. A **domain** is a collection of objects (e.g. users, devices) that share the same Active Directory database. A domain is identified by a DNS name like company.com.
2. A **tree** is a collection of one or more domains with a contiguous namespace (they have a common DNS root name like marketing.company.com, engineering.company.com, and sales.company.com).
3. A **forest** is a collection of one or more trees that share a common schema, global catalog, and directory configuration—but aren't part of a contiguous namespace. The forest typically serves as the security boundary for an enterprise network.


Root/Parent Domain
amazon.com
United States
Canada
advertising.amazon.com
United States
Canada
aws.amazon.com
United States
Canada
DOMAIN
TREE
FOREST
Transitive Trust
Explicit Trust
Root/Parent Domain
ring.com
United States
Netherlands
training.ring.com
United States
Netherlands
DOMAIN
TREE
FOREST

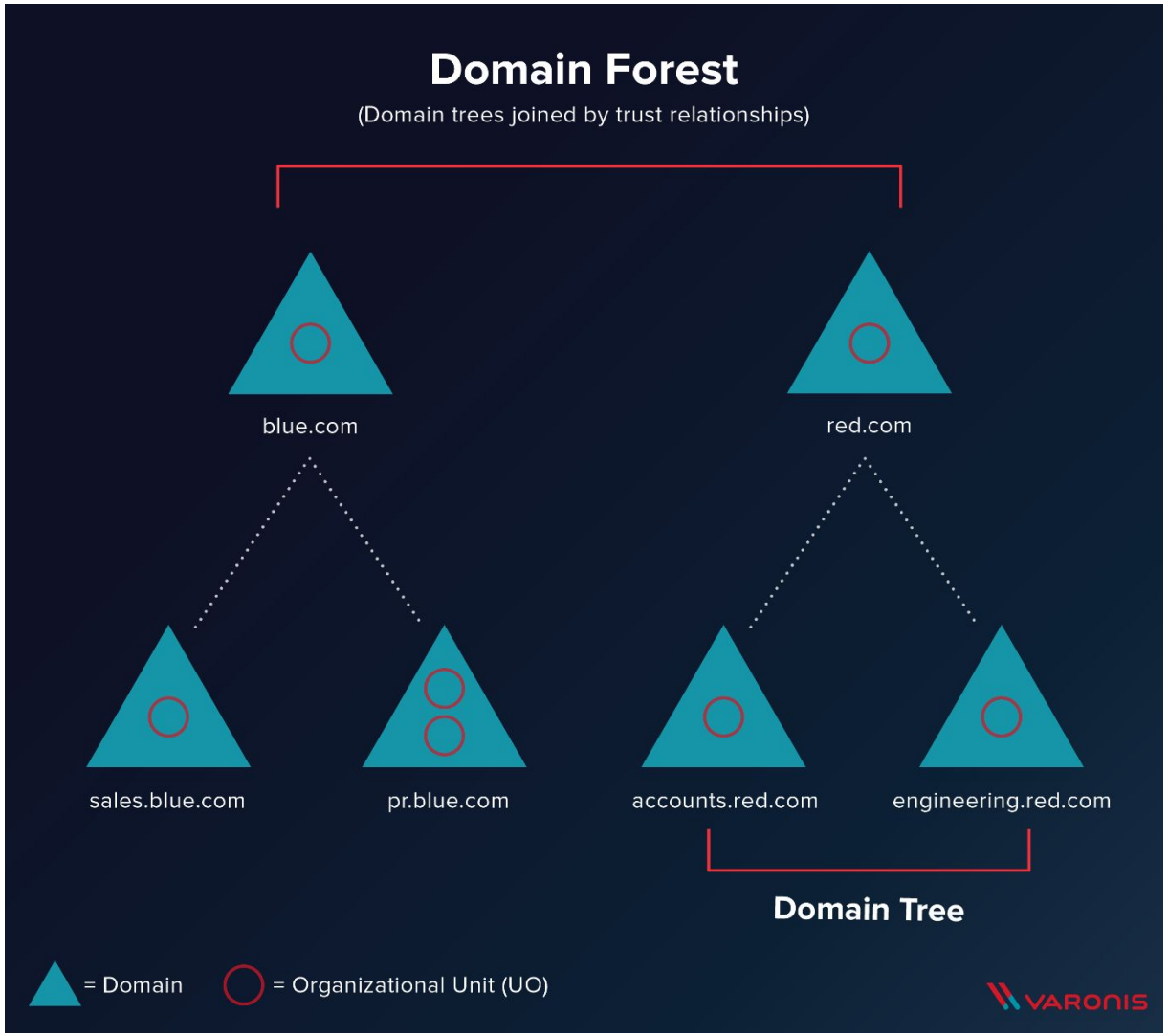
Active Directory Domain

1. A domain in Active Directory is a logical grouping of network resources that share a common security and administrative boundary.
2. It serves as a security boundary for authentication and authorization purposes, allowing users to access resources within the domain using their credentials.
3. Domains are identified by DNS names and can contain users, groups, computers, and other objects.



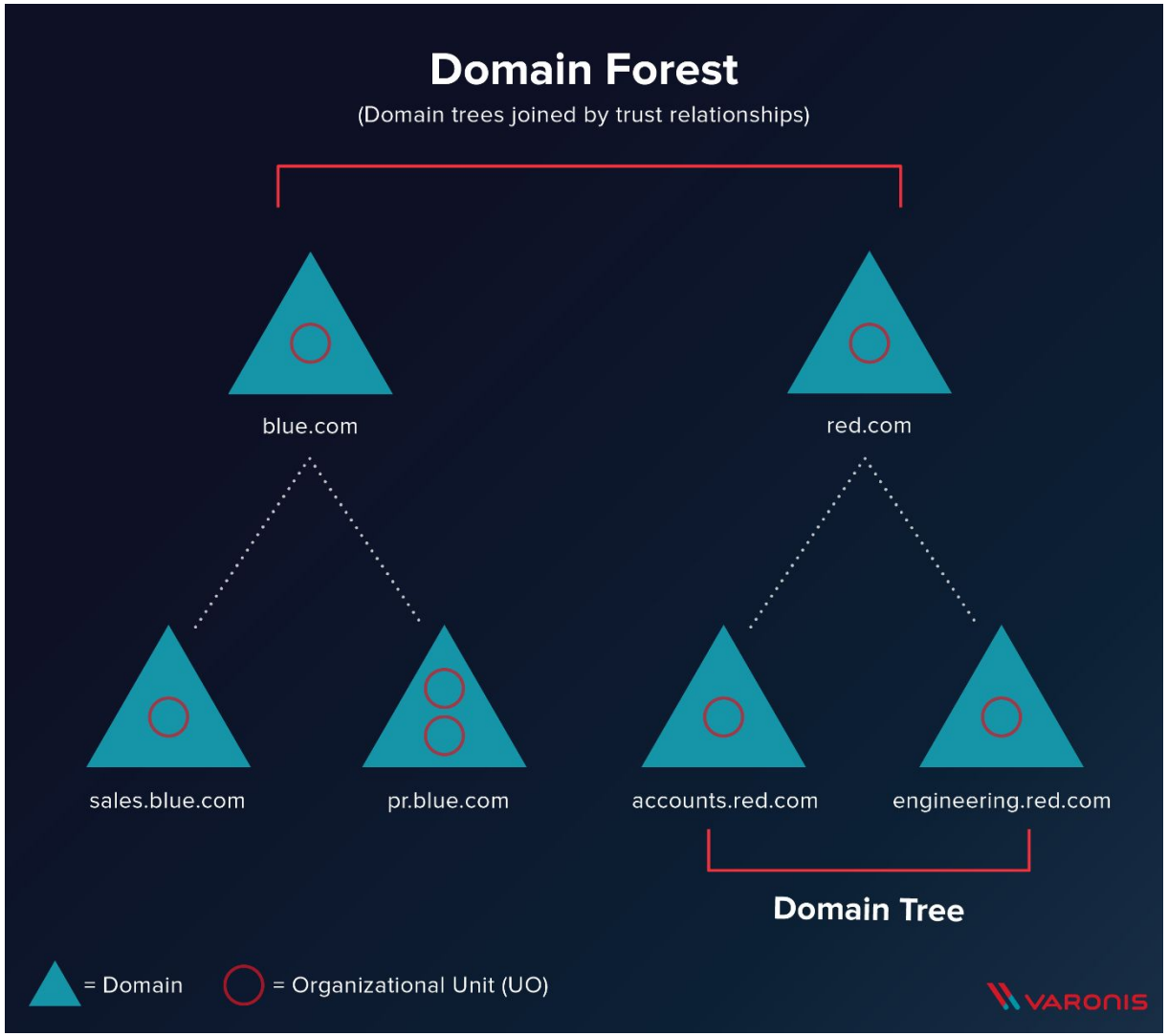
Active Directory Tree

1. A tree in Active Directory is a hierarchical structure of one or more domains that share a contiguous namespace.
2. Domains within a tree are connected by trust relationships, which enable users from one domain to access resources in another domain.
3. The first domain created in a tree is called the root domain, and subsequent domains added to the tree become child domains of the root domain.



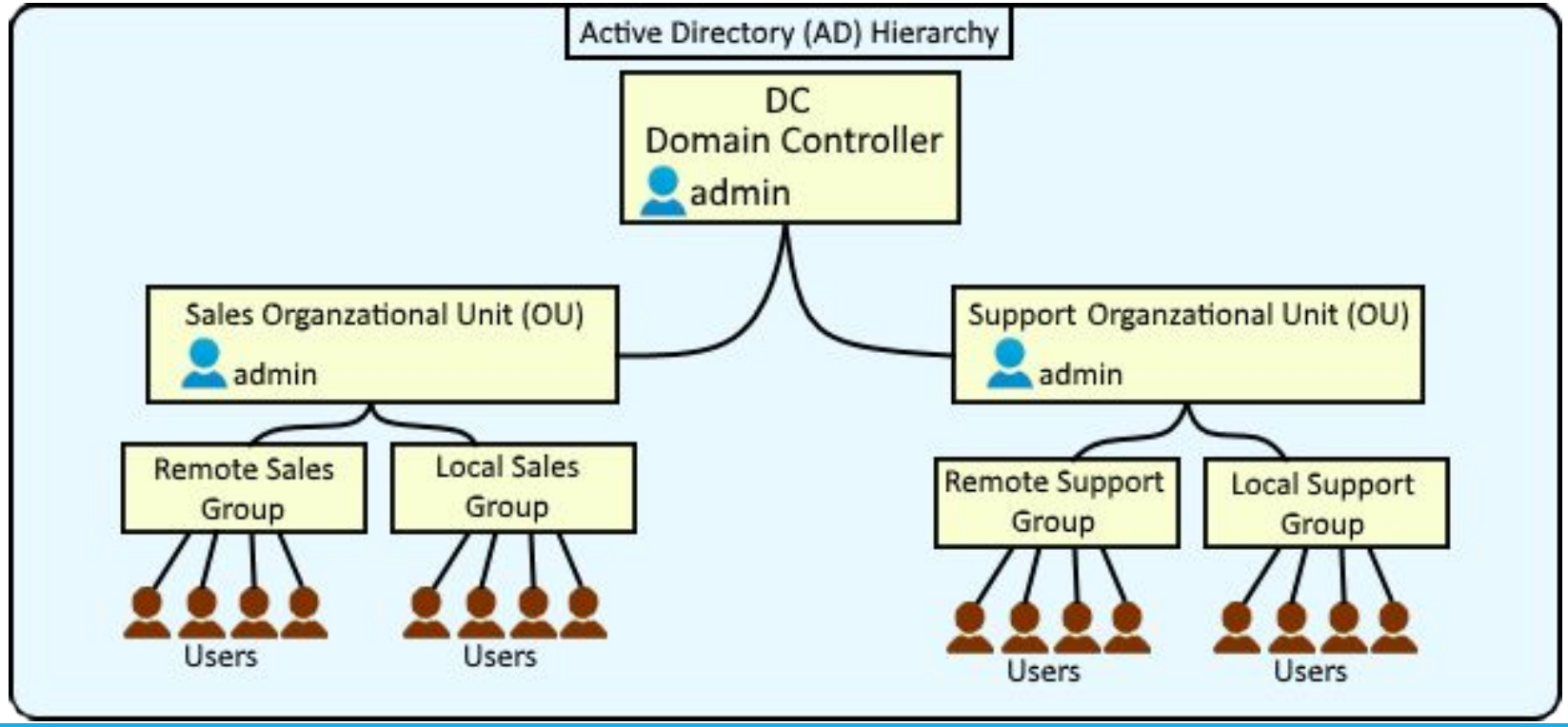
Active Directory Forest

1. An Active Directory forest is a collection of one or more domain trees that share a common schema, configuration, and global catalog.
2. It represents the highest level of organization within Active Directory and establishes security and administrative boundaries for objects within the network.
3. Forests enable organizations to manage multiple domains and establish trust relationships between them, allowing for seamless authentication and access to resources across the entire forest.



Active Directory Organizational Unit

1. An Organizational Unit (OU) is a container within a domain that helps organize and manage objects such as users, groups, computers, and other OUs.
2. OUs provide a way to delegate administrative authority, allowing administrators to assign permissions and policies to specific sets of objects.
3. Group Policy settings can be applied at the OU level, enabling administrators to enforce configurations and restrictions on objects within the OU.



Benefits of Using Active Directory

Streamlined User Management

AD simplifies user account management by providing a centralised platform to create, modify or delete users across the entire network. This means that manual administration of users on individual machines within your network is a thing of the past.

Enhanced Network Security

AD's robust security features safeguard sensitive data against cyber threats. Group policies and access controls enforce strict password requirements and limit users' access to specific files or applications based on their specific roles within the company.

Simplified Resource Sharing

Sharing resources like printers or files across a network is much simpler with AD. Administrators can manage these resources centrally, making them available to all users without additional software installation

Benefits of Using Active Directory

Better Group Policy Implementation

The Group Policy feature in AD enables admins to control how systems operate and what users can do on those systems. From setting up firewall rules to disabling USB ports on endpoints for enhanced security--everything becomes easier with group policies in place.

Faster Troubleshooting

When issues arise, having a centralised system like AD helps diagnose problems faster by providing detailed logs about user activities and system events.

Practice:

https://tryhackme.com/room/winadbasics

Students are advised to complete this THM room.

THANK YOU

Recommended Video

Introduction to Cybersecurity