MVA Microsoft Virtual Academy

Understanding Active Directory Domain Services

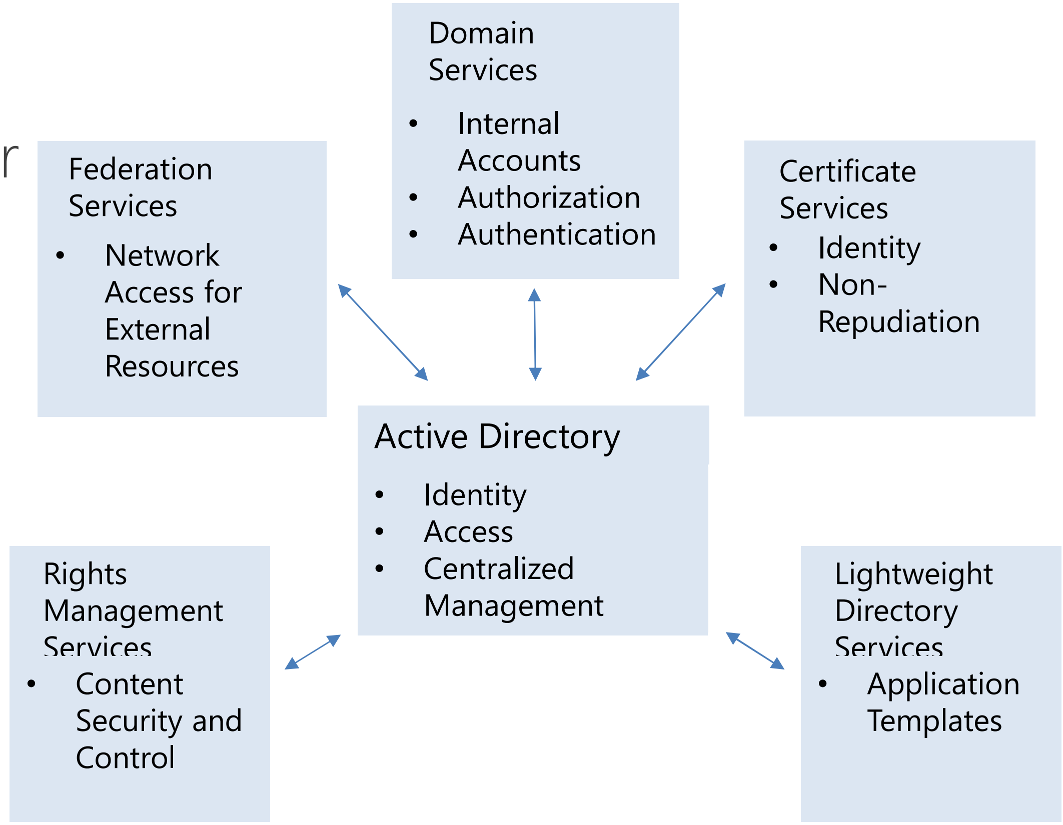
Microsoft

Module Overview

- Overview of AD DS
- AD DS Physical Components
- AD DS Logical Components

What is Active Directory

- What is Active Directory?
  - A collection of services (Server Roles and Features) used to manage identity and access for and to resources on a network



Domain Services

- Internal Accounts
- Authorization
- Authentication

Federation Services

- Network Access for External Resources

Certificate Services

- Identity
- Non-Repudiation

Active Directory

- Identity
- Access
- Centralized Management

Rights Management Services

- Content Security and Control

Lightweight Directory Services

- Application Templates

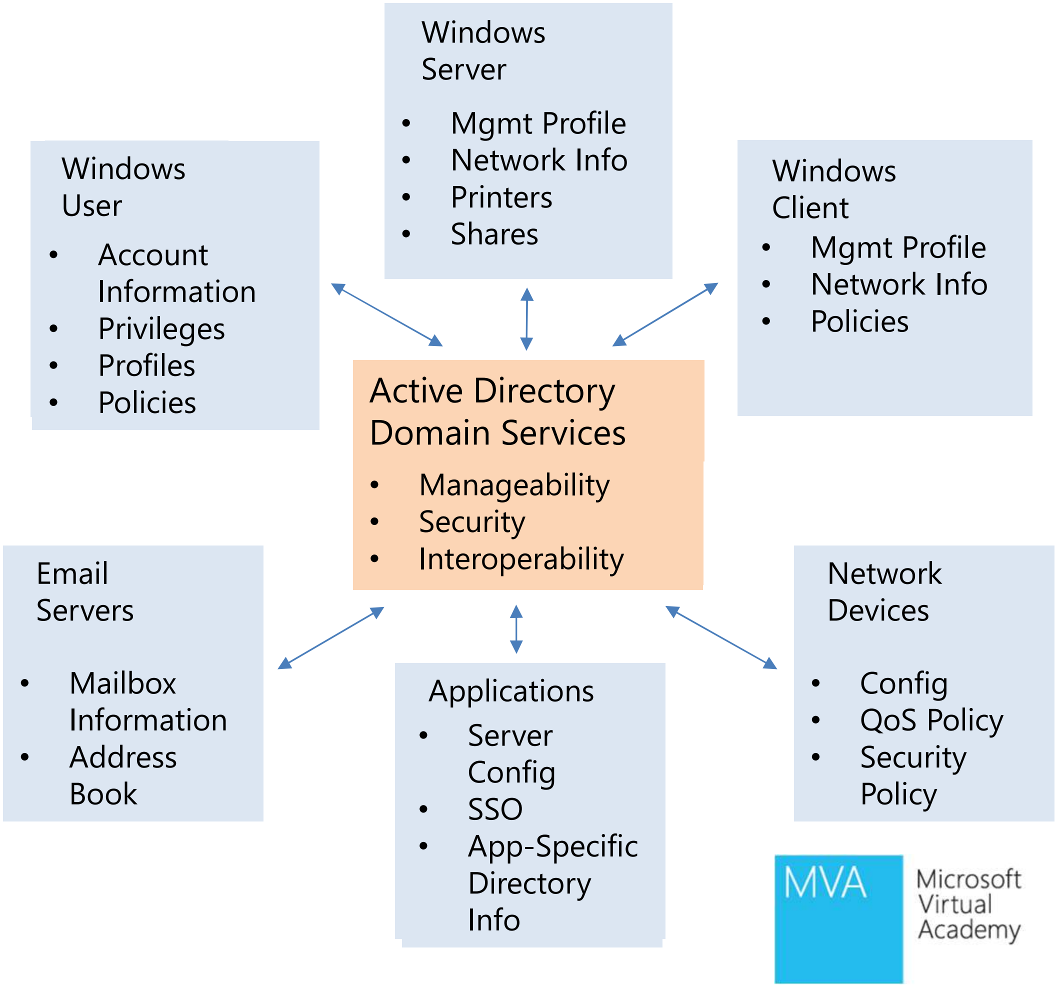
MVA Microsoft Virtual Academy

Active Directory Roles

- AD Domain Services (AD DS)
  - Users, Computers, Policies
- AD Certificate Services (AD CS)
  - Service, Client, Server and User identification
- AD Federation Services (AD FS)
  - Resource access across traditional boundaries
- AD Rights Management Services (AD RMS)
  - Maintain security of data
- AD Lightweight Directory Services (AD LDS)

What is AD DS?

- What is Active Directory Domain Services?
  - A directory service is both the directory information source and the service that makes the information available and usable
  - A phone book…



Windows Server
- Mgmt Profile
- Network Info
- Printers
- Shares

Windows User
- Account Information
- Privileges
- Profiles
- Policies

Windows Client
- Mgmt Profile
- Network Info
- Policies

Active Directory Domain Services
- Manageability
- Security
- Interoperability

Email Servers
- Mailbox Information
- Address Book

Applications
- Server Config
- SSO
- App-Specific Directory Info

Network Devices
- Config
- QoS Policy
- Security Policy

MVA Microsoft Virtual Academy

What does AD DS do?

- Scalable, secure, and manageable infrastructure for user and resource management
  - stores and manages information about network resources
  - provides support for directory-enabled applications such as Microsoft® Exchange Server
  - allows for centralized management
  - AD DS provides built in replication and redundancy: if one Domain Controller (DC) fails, another DC picks up the load
  - All access to network resources goes through AD DS, which keeps network access rights management centralized
  - Easily Integrated with Network Devices (ex: Radius, etc)

Lesson 1: Overview of AD DS

- Protocol
- What is Authentication?
- What is Authorization?
- Why Deploy AD DS?
- Centralized Network Management
- Requirements for Installing AD DS
- Overview of AD DS and DNS
- Overview of AD DS Components

Protocol

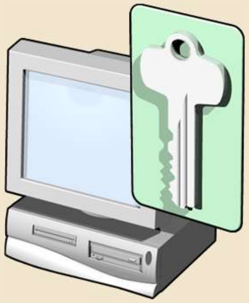
- Lightweight Directory Access Protocol (LDAP)
  - X.500 Standard
  - Based on TCP/IP
  - A method for accessing, searching, and modifying a directory service
  - A client-server model

What is Authentication?

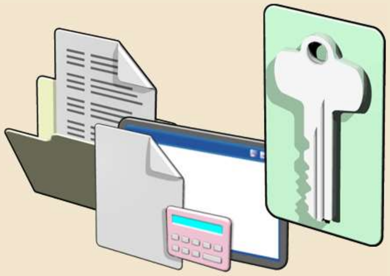
Authentication is the process of verifying a user’s identity on a network

Authentication includes two components:

- Interactive logon: grants access to the local computer



- Network authentication: grants access to network resources



What is Authorization?

Authorization is a process of verifying that an authenticated user has permission to perform an action

- Security principals are issued security identifiers (SIDs) when the account is created

- User accounts are issued security tokens during authentication that include the user's SID and all related group SIDs

- Shared resources on a network include access control lists (ACL) that define who can access the resource

- The security token is compared against the Discretionary Access Control List (DACL) on the resource and access is granted or denied

Why Deploy AD DS?

AD DS provides a centralized system for managing users, computers, and other resources on a network

AD DS features include:

- Centralized directory
- Single sign-on access
- Integrated security
- Scalability
- Common management interface

Centralized Network Management

AD DS centralizes network management by providing:

- Single location and set of tools for managing user and group accounts
- Single location for assigning access to shared network resources
- Directory service for AD DS enabled applications
- Options for configuring security policies that apply to all users and computers
- Group policies to manage user desktops and security settings

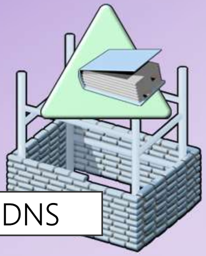
Requirements for Installing AD DS

Object	Description
TCP/IP	• Configure appropriate TCP/IP and DNS server addresses.
Credentials	• To install a new AD DS forest, you need to be local Administrator on the server. To install an additional domain controller in an existing domain, you need to be a member of the Domain Admins group.
Domain Name System)DNS) Infrastructure	• Verify that a DNS infrastructure is in place. When you install AD DS, you can include DNS server installation, if it is needed. • When you create a new domain, a DNS delegation is created automatically during the installation process. Creating a DNS delegation requires credentials that have permissions to update the parent DNS zones.

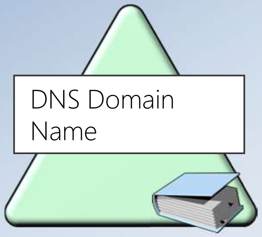
MVA Microsoft Virtual Academy

Overview of AD DS and DNS

- AD DS requires a DNS infrastructure

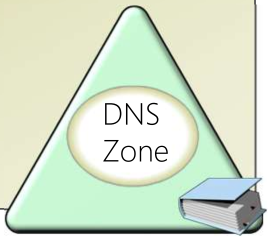


- AD DS domain names must be DNS domain names

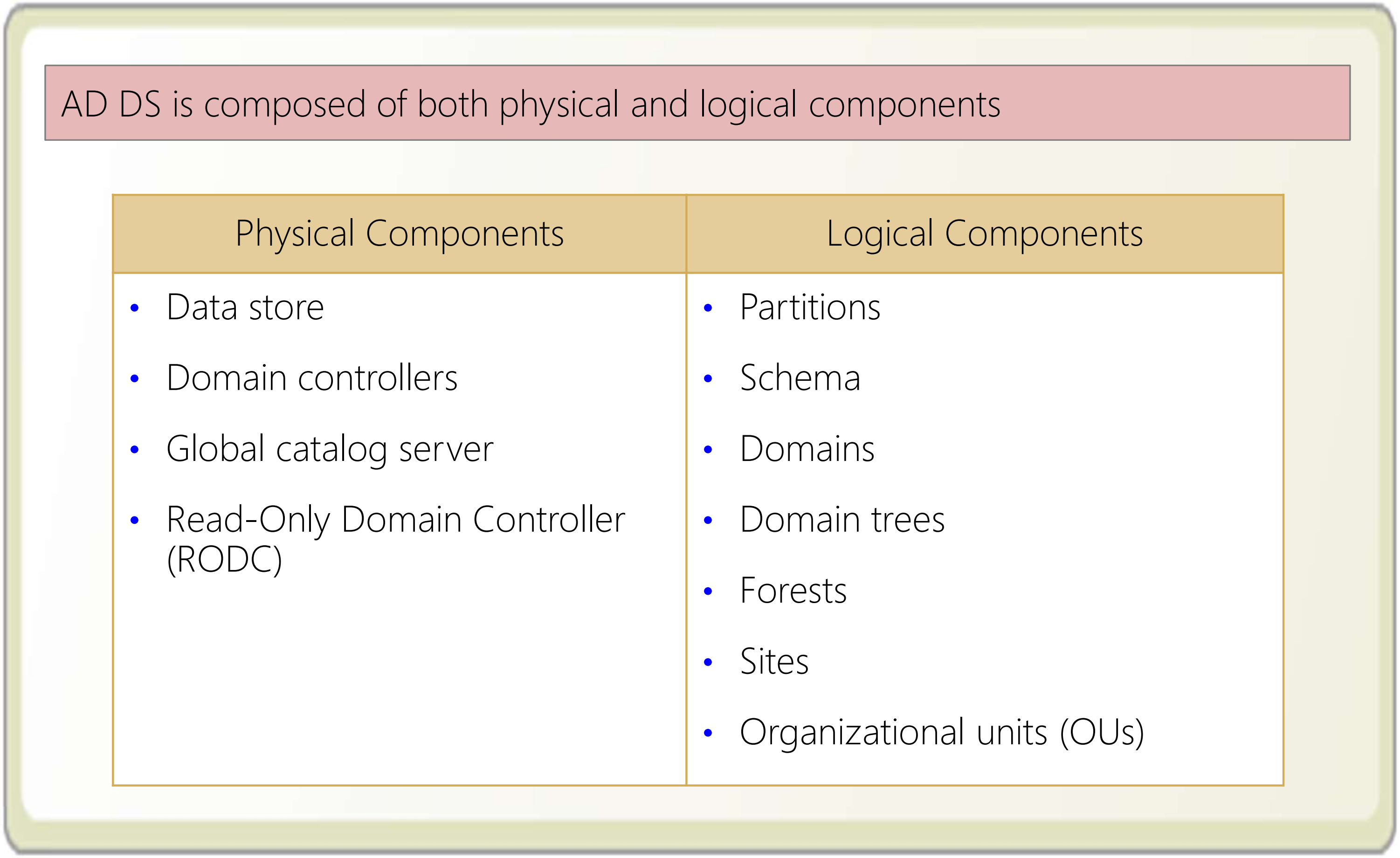


- AD DS domain controller records must be registered in DNS to enable other domain controllers and client computers to locate the domain controllers

- DNS zones can be stored in AD DS as Active Directory integrated zones



Component Overview



AD DS is composed of both physical and logical components

Physical Components	Logical Components
Data store	Partitions
Domain controllers	Schema
Global catalog server	Domains
Read-Only Domain Controller (RODC)	Domain trees
	Forests
	Sites
	Organizational units (OUs)

Lesson 2: Overview of AD DS Physical Components

- Domain Controllers
- Global Catalog Servers
- Data Store
- Replication
- Sites

Domain Controllers

A domain controller is a server with the AD DS server role installed that has specifically been promoted to a domain controller

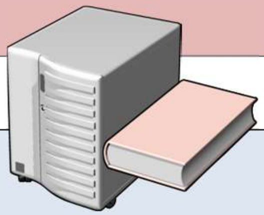
Domain controllers:

- Host a copy of the AD DS directory store
- Provide authentication and authorization services
- Replicate updates to other domain controllers in the domain and forest
- Allow administrative access to manage user accounts and network resources

Windows Server 2008 and later supports RODCs

Global Catalog Servers

Global catalog servers are domain controllers that also store a copy of the global catalog



The global catalog:

- Contains a copy of all AD DS objects in a forest that includes only some of the attributes for each object in the forest

- Improves efficiency of object searches by avoiding unnecessary referrals to domain controllers

- Required for users to log on to a domain

What is the AD DS Data Store?

The AD DS data store contains the database files and processes that store and manage directory information for users, services, and applications

The AD DS data store:

- Consists of the Ntds.dit file
- Is stored by default in the %SystemRoot%\NTDS folder on all domain controllers
- Is accessible only through the domain controller processes and protocols

What is AD DS Replication?

AD DS replication copies all updates of the AD DS database to all other domain controllers in a domain or forest

AD DS replication:

- Ensures that all domain controllers have the same information
- Uses a multimaster replication model
- Can be managed by creating AD DS sites

The AD DS replication topology is created automatically as new domain controllers are added to the domain

What are Sites?

An AD DS site is used to represent a network segment where all domain controllers are connected by a fast and reliable network connection

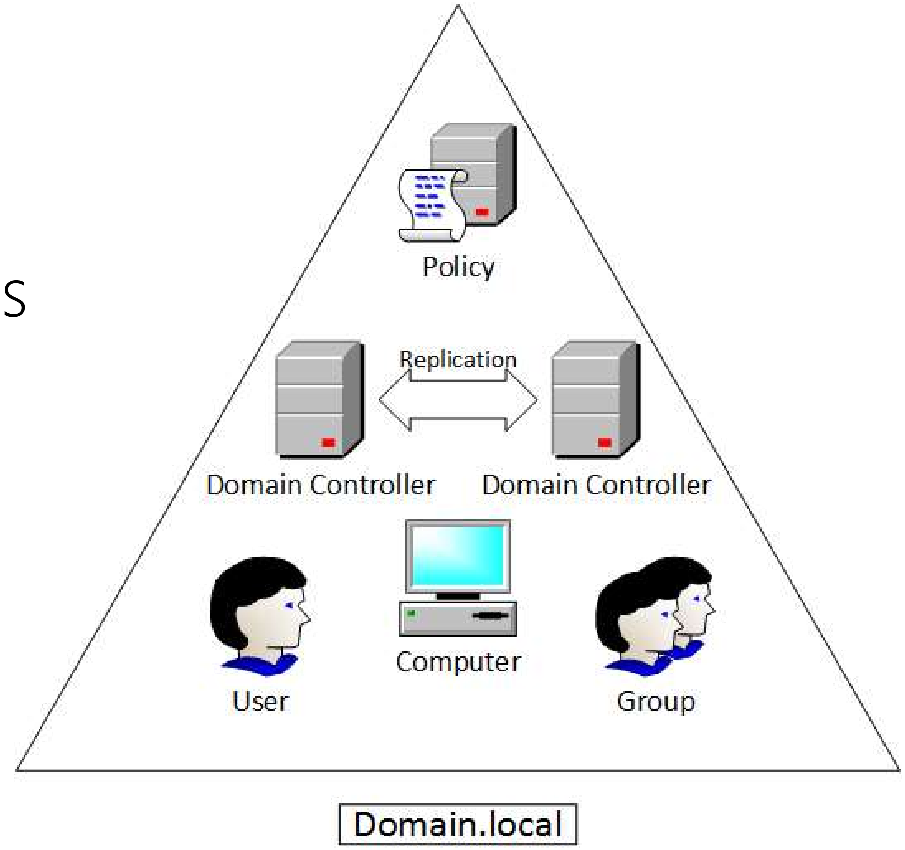
Sites are:

- Associated with IP subnets
- Used to manage replication traffic
- Used to manage client logon traffic
- Used by site aware applications such as Distributed File Systems (DFS) or Exchange Server
- Used to assign group policy objects to all users and computers in a company location

MVA Microsoft Virtual Academy

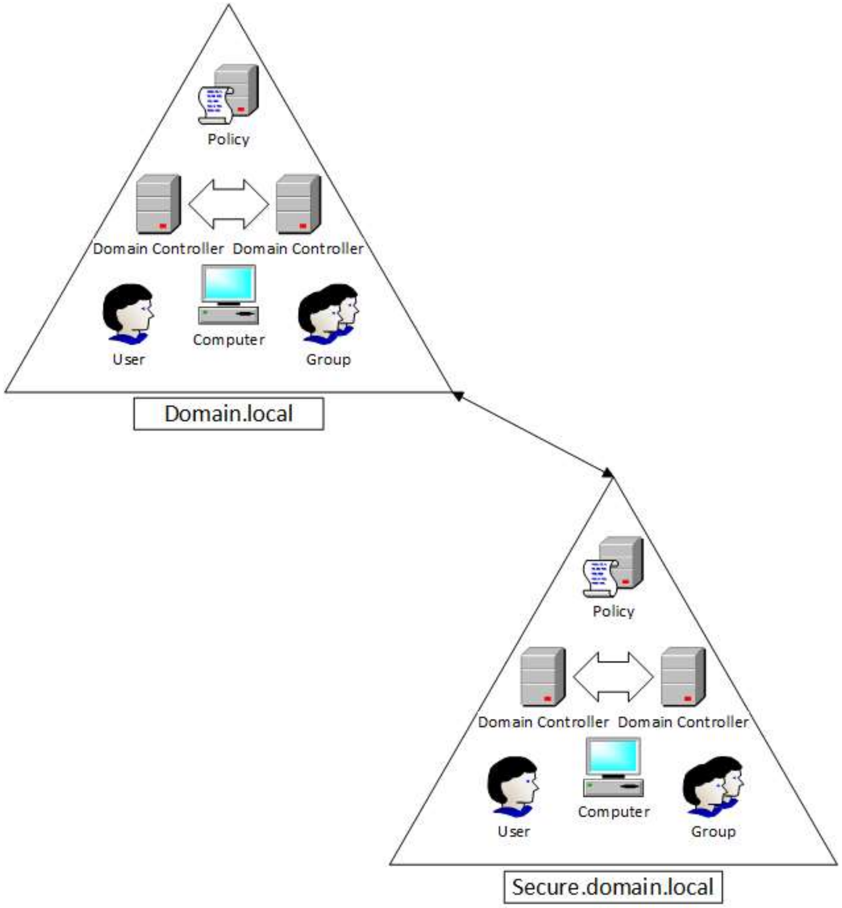
Domains

- Units of Replication
- Maintained by Domain Controllers
- Millions of Objects



MVA Microsoft Virtual Academy

Trees


Policy
Domain Controller
Domain Controller
User
Computer
Group
Domain.local
Policy
Domain Controller
Domain Controller
User
Computer
Group
Secure.domain.local

Lesson 3: Overview of AD DS Logical Components

- AD DS Schema
- The Basics
- Trusts
- AD DS Objects

What is the AD DS Schema?

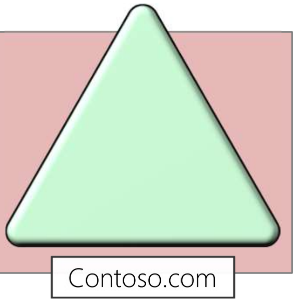
The AD DS Schema:

- Defines every type of object that can be stored in the directory
- Enforces rules regarding object creation and configuration

Object Types	Function	Examples
Class Object	What objects can be created in the directory	• User • Computer
Attribute Object	Information that can be attached to an object	• Display name

The Basics: Domains

Domains are used to group and manage objects in an organization

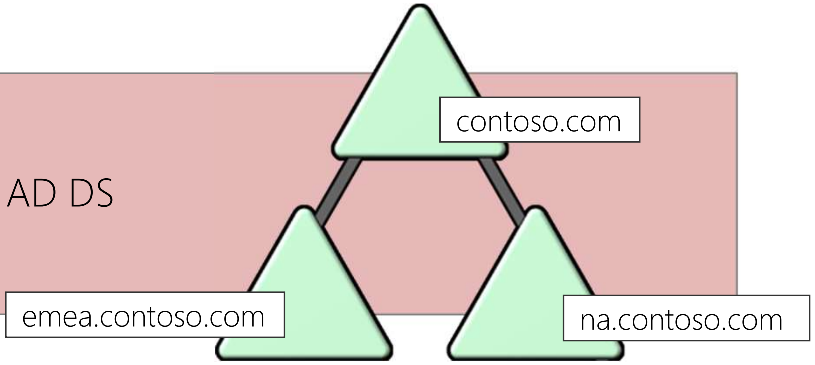


Domains:

- An administrative boundary for applying policies to groups of objects
- A replication boundary for replicating data between domain controllers
- An authentication and authorization boundary that provides a way to limit the scope of access to resources

The Basics: Trees

A domain tree is a hierarchy of domains in AD DS



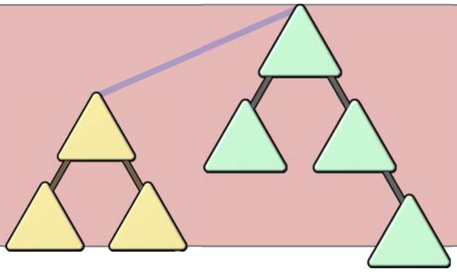
All domains in the tree:

- Share a contiguous namespace with the parent domain
- Can have additional child domains
- By default create a two-way transitive trust with other domains

MVA Microsoft Virtual Academy

The Basics: Forests

A forest is a collection of
one or more domain trees



Forests:

- Share a common schema
- Share a common configuration partition
- Share a common global catalog to enable searching
- Enable trusts between all domains in the forest
- Share the Enterprise Admins and Schema Admins groups

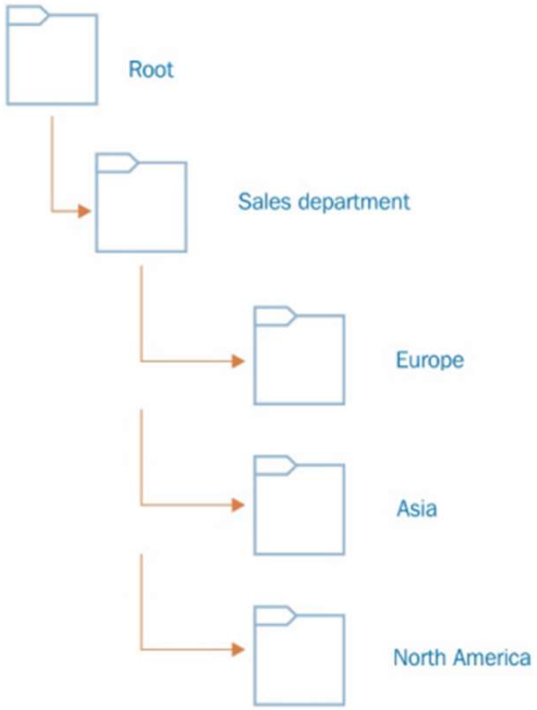
The Basics: Organizational Units (OUs)

OUs are Active Directory containers that can contain users, groups, computers, and other OUs

OUs are used to:

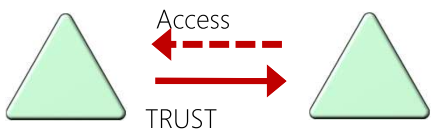
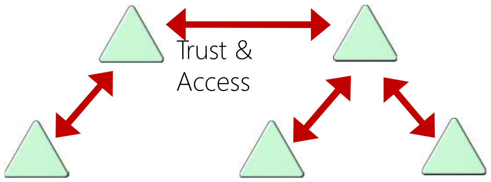
- Represent your organization hierarchically and logically
- Manage a collection of objects in a consistent way
- Delegate permissions to administer groups of objects
- Apply policies

The Basics: Organizational Units (OUs)



Trusts

Trusts provide a mechanism for users to gain access to resources in another domain

Types of Trusts	Description	Diagram
Directional	The trust direction flows from trusting domain to the trusted domain	
Transitive	The trust relationship is extended beyond a two-domain trust to include other trusted domains	

- All domains in a forest trust all other domains in the forest
- Trusts can extend outside the forest

MVA Microsoft Virtual Academy

AD DS Objects

Object	Description
User	- Enables network resource access for a user
InetOrgPerson	- Similar to a user account - Used for compatibility with other directory services
Contacts	- Used primarily to assign e-mail addresses to external users - Does not enable network access
Groups	- Used to simplify the administration of access control
Computers	- Enables authentication and auditing of computer access to resources
Printers	- Used to simplify the process of locating and connecting to printers
Shared folders	- Enables users to search for shared folders based on properties

Microsoft