# Active Directory - Forest, Tree, Domain

## Knowledge Base Questions & Answers

### What is Forest?

- The Forest is a collection of one or multiple trees, which shares a typical configuration, GC (Global Catalog), logical structure, directory configuration, and directory schema.
- There is always as a minimum one Forest on a domain network, and it is created when the first AD (Active Directory) DC (Domain Controller) is installed.
- If there are no forest root domains, then a single tree can also be called a Forest.
- Domain trees, which are in the Forest, do not form a contiguous namespace.
- Domains function in a Forest independently.
- In a Forest, all trees are connected by transitive two-way trust relationships, thus allowing users in any tree access to resources in another domain.

### What is Tree?

- The tree is a collection of one or more domains, which are connected by a transitive two-way trust.
- Domains in a Tree share common schema and a contiguous namespace.
- The first domain, which is created in a Tree, is called the root domain.
- All domain in Tree can be viewed in two ways:
  - Trust relationships between domains.
  - The namespace of the domain tree.
- Example of Tree contiguous namespace:
  ***abc.com > it.abc.com > usa.it.abc.com***

### What is Domain?

The domain is a collection of users, group, computers, and printers and so on in a network. These objects share a common AD database, security policies, and security relationships with other domains.

### What is the Forest Root Domain?

- The first DC, which installed on the network, and which are not in any existing forests, is called the Forest Root Domain.
- Forest Root Domain cannot be removed from the forest without removing the entire forest itself.
- No other domains can ever be created above the Forest Root Domain in the forest domain hierarchy.

### What is Empty Root Domain?

- Empty Root Domain is an AD design element that is useful for organizations with decentralized IT authority such as universities.
- It acts as a placeholder for the root of AD and does not typically contain any users or resources, which are not required.

### What is the Child Domain?

- When a new domain is installed and added to the existing tree, it will be called a Child Domain.
- Child Domain name space appends to the parent domain name.

### What is Functional Level?

- Functional Level helps the coexistence of AD versions for Windows Servers 2008 and earlier.
- Although low functional levels help to coexist with legacy AD, it will disable some of the new features of AD.
- Functional Level's conversion can be reversed.

### What types of authentication exist between forests?

Four types of authentication exist across forests:

- Kerberos and NTLM (NT LAN Manager) network logon for remote access to a server in another forest.
- Kerberos and NTLM interactive logon for physical logon in case if a user outside of the user's home forest.
- Kerberos delegation to N-tier application in another forest.
- UPN (User Principal Name) credentials.

## Experience-Based Questions & Answers

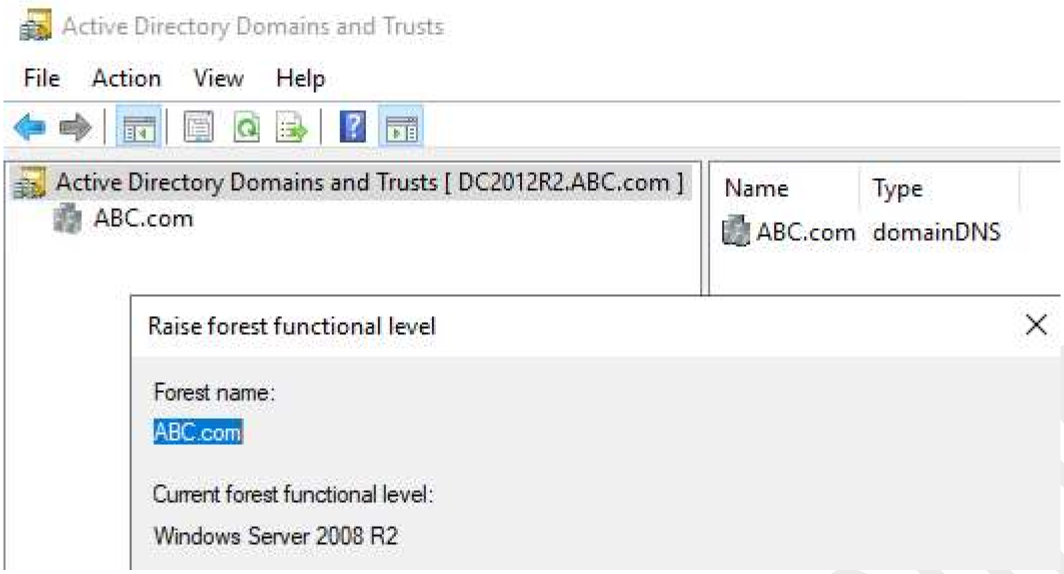
### For which purposes of multiple domains are using?

There are the following purposes of implementing multiple domains:

- Decentralize administration.
- Management and controlling of replication in AD.
- Through the utilization of multiple domains, different security policies for each domain can be implemented.
- Multiple domains are also implemented when the number of objects in the directory is quite substantial.

### How do you check the forest functional level?

- Use "Active Directory Domain and Trusts" MMC (Microsoft Management Console) snap-in.



Active Directory Domains and Trusts [ DC2012R2.ABC.com ]

ABC.com

| Name | Type |
|---|---|
| ABC.com | domainDNS |

Raise forest functional level

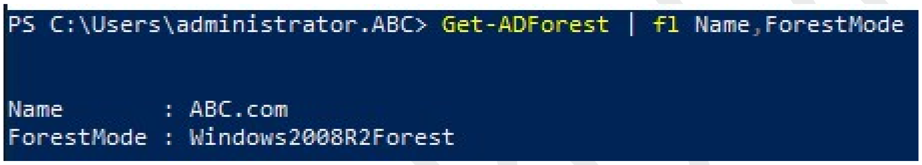
Forest name:

ABC.com

Current forest functional level:

Windows Server 2008 R2

- Run command:
  **get-adforest | fl Name,Forestmode**

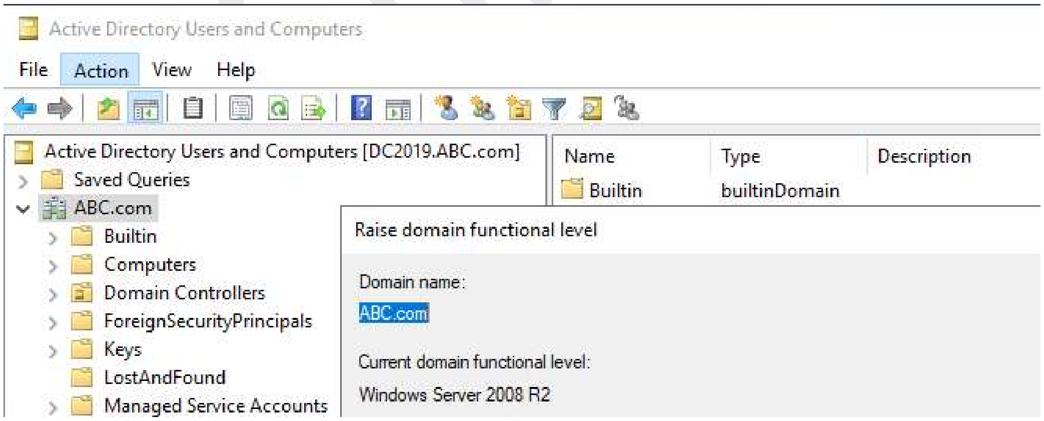


```
PS C:\Users\administrator.ABC> Get-ADForest | fl Name,ForestMode


Name       : ABC.com
ForestMode : Windows2008R2Forest
```

## How do you check domain functional levels?

To check the domain functional level, use “Active Directory Users and Computers” MMC snap-in.


Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Computers [DC2019.ABC.com]
Saved Queries
ABC.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Keys
LostAndFound
Managed Service Accounts

| Name | Type | Description |
|---|---|---|
| Builtin | builtinDomain | |

Raise domain functional level

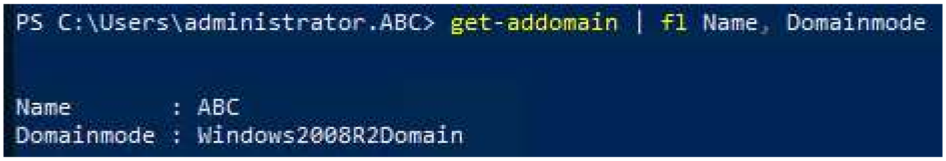
Domain name:

ABC.com

Current domain functional level:

Windows Server 2008 R2

- Run command:
  **get-addomain | fl Name, DomainMode**

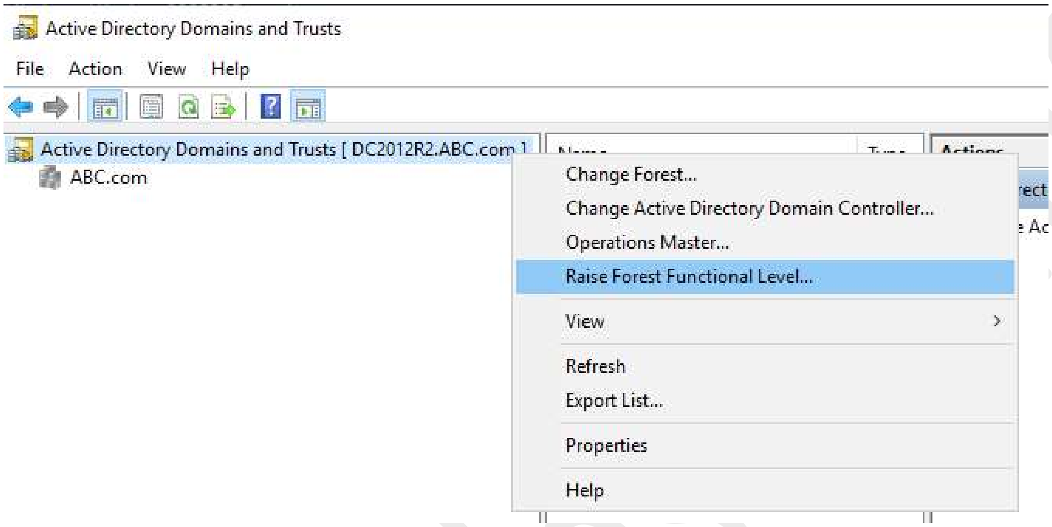


```
PS C:\Users\administrator.ABC> get-addomain | fl Name, Domainmode

Name       : ABC
Domainmode : Windows2008R2Domain
```

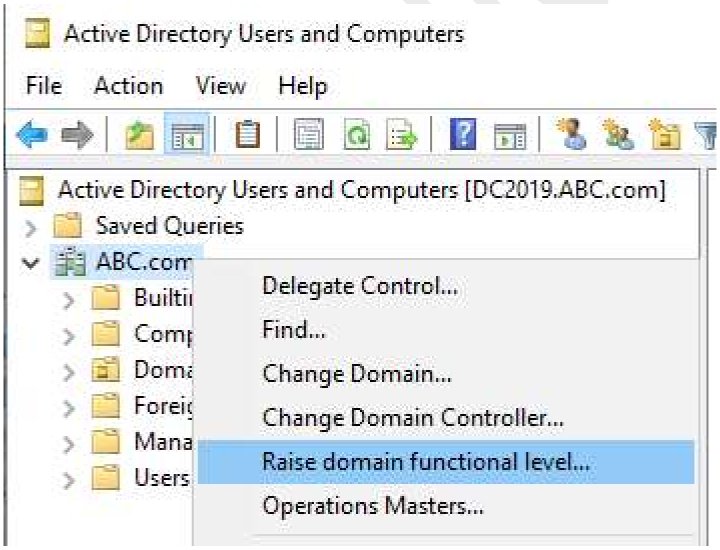
## How to raise forest functional level in the GUI?

You can raise forest functional level on “Active Directory Domains and Trusts” MMC snap-in.


Active Directory Domains and Trusts
File
Action
View
Help
Active Directory Domains and Trusts [ DC2012R2.ABC.com ]
ABC.com
Change Forest...
Change Active Directory Domain Controller...
Operations Master...
Raise Forest Functional Level...
View
Refresh
Export List...
Properties
Help

## How to raise domain functional level in the GUI?

You can raise the domain functional level on “Active Directory Users and Computers” MMC snap-in.


Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Computers [DC2019.ABC.com]
Saved Queries
ABC.com
Builti
Comp
Doma
Foreig
Mana
Users
Delegate Control...
Find...
Change Domain...
Change Domain Controller...
Raise domain functional level...
Operations Masters...

## Can be domain name renamed?

Yes. You can rename the domain even without making it down.

### In which case a domain name can be renamed?

- All DCs must run Windows Server 2003 or later.
- AD functional level must at least be Windows Server 2003.

### What are the benefits of multiple Forests?

- Total control of departmental security.
- Control of the Schema.
- Enterprise and Schema Administrators now report directly to the department.
- Full control of information published in the GC.
- Does not automatically have a trust relationship with all organizations.

### What are the drawbacks of multiple Forests?

- The cost of administration has increased.
- It has increased the complexity of DNS (Domain Name System).
- Difficulties in collaboration.
- Explicit NTLM trust is not as secure as Kerberos Trust and can be difficult for managing and troubleshooting.
- If institutional applications are rolled out that requires a schema change, each forest must perform the modifications.

### What are the drawbacks of using multiple domains?

- Administrative inconsistency.
- Increased management of challenges.
- Decreased flexibility.

### What is the difference between Workgroup and Domain?

- The workgroup is an interconnection of some systems that share resources such as files and printers between each other. Each workgroup maintains a local database for user accounts, security, etc..
- The domain is an interconnection of systems that share resources with one or more dedicated server, which can be used to control security and permissions for all users in the domain.
- Domain maintains a centralized database and hence, centralized management of user accounts, policies, etc. are established. If you have a user account on a domain, then you can log on to any system without a user account on that particular system.