Domain Functional Level

1. **What is Domain Functional level?**

Ans: Domain functional levels determine the Active Directory functionality and features that are  
available. A domain functional level defines the minimum version of the Windows Sever operating system that can be used on domain controllers.

The higher the domain functional levelis, the more functionality and features are available.

Note: The domain functional level is dependent on the earliest version of the Windows Sever operating system used on a domain controller in a domain.

1. **Which Domain functional levels Windows Server 2012 domain controllers have?**

Ans: You can use Windows Server 2012 domain controllers with the following domain  
functional levels:

■ Windows Server 2003  
■ Windows Server 2008  
■ Windows Server 2008 R2  
■ Windows Server 2012

1. **Write The Windows Server 2003 domain functional level  
   features?**
2. **Write The Windows Server 2008 domain functional level  
   features?**
3. **Write The Windows Server 2008 R2 domain functional level  
   features?**

The Windows Server 2008R2 domain functional level includes the following  
features:

■ Managed service account support, which enables you to automatically manage service  
account passwords rather than manually managing them  
■ Support for command-line-based Active Directory Recycle Bin if the forest functional  
level is raised to Windows Server 2008 R2

1. **Write The Windows Server 2012 domain functional level  
   features?**
2. **What is Forest Functional Level?**

Ans: A forest can host domains running at different domain functional levels.Forest functional levelis dependent on the minimum domain functional level of any domain in the forest.

Note: Each domain in a forest can have a different functional level. The forest functional level depends on the lowest domain functional level in the forest.

**Q. Define User Principal Name (UPN) suffixes:**

User Principal Name (UPN) suffixes are the part of a user’s UPN that trails the @ symbol. For example, in the UPN [arif@at.com](mailto:arif@at.com), the UPN suffix is the domain name at.com. UPN suffixes enable users to sign on an account name that includes the name of their domains.

MCQ

1. If your organization has Windows Server 2003 domain controllers, you aren’t  
   able to raise the functional level until you replace or upgrade those domain controllers to a more recent version of the Windows Server operating system.
2. The Windows Server 2003 domain functional level is the lowest level
3. The Windows Server 2008 domain functional level requires that all domain controllers be running the Windows Server 2008, Windows Server 2008 R2, or Windows Server 2012 operating systems.
4. The Windows Server 2008 R2 domain functional level requires that all domain controllers are running the Windows Server 2008 R2 or Windows Server 2012 operating systems.
5. The Windows Server 2012 domain functional level requires that all domain controllers be running the Windows Server 2012 operating system.
6. You can raise the forest functional level using the Active Directory Domains and Trusts  
   console
7. You need to use a user account that is a member of the Enterprise Admins group to perform this task.

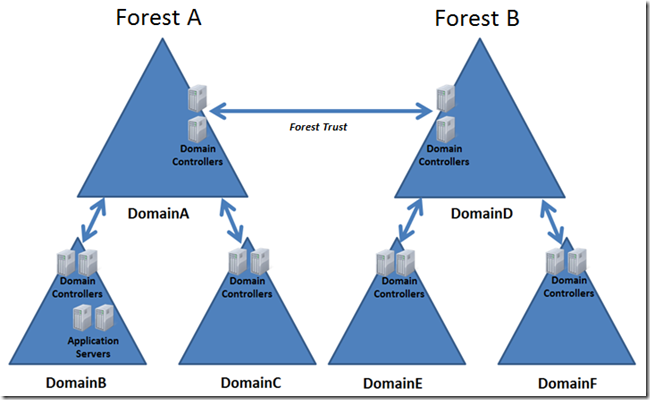
**What is Domain Trust?**

Domain Trusts make it possible for users in one domain to be authenticated by domain controllers in a separate domain. For example, if there is a bidirectional trust relationship between the domains contoso.local and adatum.remote users with accounts in the contoso.local domain are able to authenticate in the adatum.remote domain.

**What is Forest Trust:**

Ans: A forest trust allows one forest to trust another forest. This means that all domains in the first forest have a trust relationship with all domains in the second forest.

Note: Forest trusts require that each forest be configured to run at the windows server 2003 forest functional level or higher. Forest trusts can be bi- or unidirectional. You are most likely to configure forest trusts if your organization has two or more active directory forests.



**Two types of Authentication scope:**

1. **Forest-wide authentication:**

Ans: When you choose forest-wide authentication, users from the trusted forest are automatically authenticated for all resources in the local forest. You should use this option when both the trusted and trusting forest are part of the same organization.

1. **Selective authentication:**

Ans: When you configure selective trust authentication, windows does not automatically authenticate users from the trusted forest. You can then configure specific servers and domains within the forest to allow users from the trusted forest to authenticate. Use this option when the two forests are from different organizations, or you have more stringent security requirements.

**Configuring selective authentication:**

Configuring selective authentication means granting specific security principals in the trusted forest the Allowed to authenticate (allow) permission on the computer that hosts the resource to which you want to grant access.

**Realm trusts:**

**What is Realm truat?**

You use a realm trust to create a relationship between an Active Directory Services domain and a Kerberos V5 realm that uses a third-party directory service. Realm trusts can be transitive or non-transitive. They can also be uni- or bidirectional.

Note: You’re most likely to configure a realm trust when you need to allow users who use a UNIX directory service to access resources in an Active Directory domain or users in an Active Directory domain to access resources in a UNIX Kerberos V5 realm. You can configure a realm trust from the Active Directory Domains and Trust console

Q- 1. Which of the following trust type when you want to configure a trust between an Active Directory domain and a Kerberos V5 realm?

1. Shortcut trust
2. **Realm trust**
3. Forest trust
4. External trust

Q-2. When you use a realm trust to configure?

1. **a trust between an Active Directory domain and a Kerberos V5 realm**

Q-3 . Which trust you will configure when you need to allow users who use a UNIX directory to access resources in an Active Directory domain?

1. Shortcut trust
2. **Realm trust**
3. Forest trust
4. External trust

Q-4. Which trust you will configure when you need to allow users in an Active Directory domain to access resources in a UNIX Kerberos V5 realm?

1. Shortcut trust
2. **Realm trust**
3. Forest trust
4. External trust

Q-5. You can configure a realm trust from

1. **Active Directory Domains and Trust console**

**Netdom.exe**

Q-6. Why you use netdom.exe with the /trust switch

1. **To create and manage trusts from the command line**

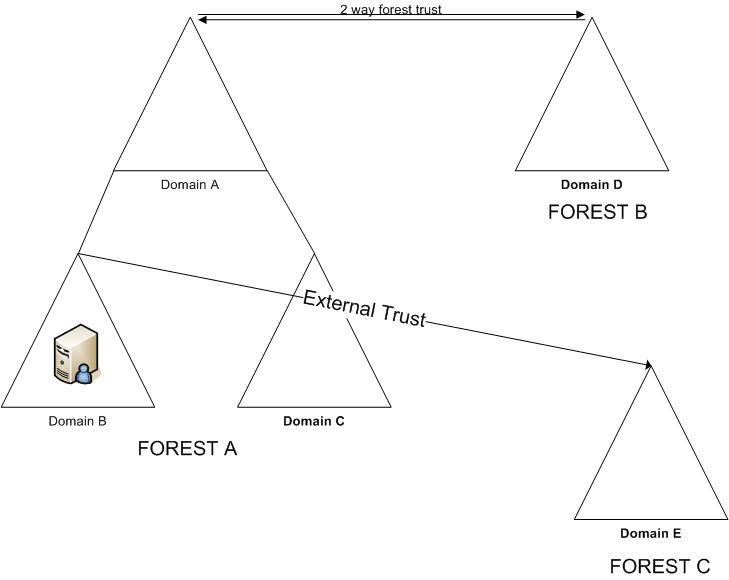
Q-7. You can use netdom.exe with /trust switch to create and manage-

1. **Forest, shortcut, realm, and external trusts.**

Q-8. When using netdom.exe, what should you specify?

1. **The trusting domain and the trusted domain name.**
2. **What is External Trust?**

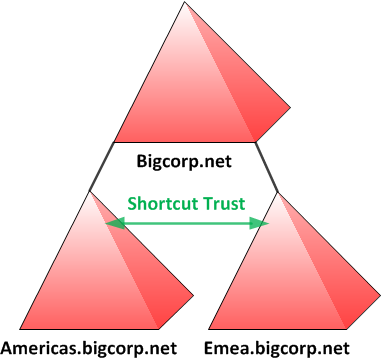
Ans : External trusts enable you to configure one domain in one forest to trust a domain in another forest without enabling a transitive trust.



1. **What is Shortcut trusts?**

Ans : Shortcut trustsenable you to speed up authentication between domains in a forest that  
might be in separate branches or even separate trees.

Or, You can use a shortcut trust between domains in the same forest to speed the authentication process.



**MCQ QUESTION**

1. Whichoperating systems do not support Forest Trusts?

1. Windows 2000 Server
2. Windows NT 4.0

2. You are the administrator of the single domain contoso.local forest. Users in the  
adatum.remote single domain forest need to access resources in the contoso.local domain. Users in contoso.local should not have access to resources in adatum.remote. You are configuring an external trust between these two single domain forests from the contoso.local domain. Which trust direction should you configure to support this configuration?

Ans: One-way outgoing. Remember that the direction of trust is opposite to the direction of authentication. To have incoming users authenticated, you configure an outgoing trust.

**1. What is Multi-domain Active Directory?**  
The majority of current Active Directory deployments in small- and medium-sized enterprises have a single domain. This hasn’t always been the case because earlier versions of the Windows Server operating system, such as Windows NT 4, supported far fewer user accounts. Supporting a smaller number of accounts often necessitated the use of multiple domains, and it wasn’t unusual to see medium-sized organizations that used complicated domain structures

**2. How many objects domain controllers create?**

Each Windows objects approximately 2.15 billion objects during its lifetime, and each domain supports the creation of up to approximately 2.15 billion relative identifiers.

**3. What is Historical domain structure?**

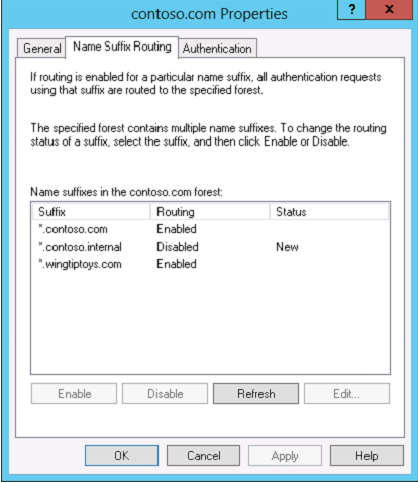
Even though newer versions of the Windows Server operating system handle large numbers of objects more efficiently, some organizations have retained the forest structure that was established when the organization first adopted Active Directory

**4. Organizational or political reasons:** Some organizations are conglomerates, and they might be composed of separate companies that share a common administrative and management core. An example of this is a university faculty in Europe or Australia, such as a Faculty of Science, that is composed of different departments or schools

**5. Security reasons:** Domains enable you to create security boundaries so that you can have one set of administrators who are able to manage computers and users in their own domain, but who are not able to manage computers and users in a separate domain. Although it’s possible to accomplish a similar goal by delegating privileges, many organizations prefer to use separate domains to accomplish this goal.

**Name Suffix Routing**

Name suffix routing enables for a particular name suffix, all authentication requests using that are routed to the specified forest. Actually Name suffix use to when we configure a forest between two active directory forests. Name suffix routing assists when user sign on with a UPN, Such as arif@at.com. You do this by configuring name suffix routing on the Name Suffix Routing tab of the trust’s properties as shown in.



Sid filtering

1. What is SID filtering / Define SID filtering?
2. What is domain quarantine?
3. Which cmdlet use to get verify SID filter setting on a trust?

1.What is Multi-forest Active Directory environments?

Ans: A multi-forest Active Directory deployment allows you to sync users and groups from multiple Active Directory domains or forests to Horizon Workspace in a multi-forest environment. For a multi-forest Active Directory deployment, you must also add one or more identity provider instances with which to associate user stores.

2. Which reasons for having multiple Active Directory forests within a single organization?

Ans: A. **Security requirements**

B.Incompatible schemas

C.Political requirements

3. Add a User Store for a Multi-Forest Active Directory Environment.

Ans: To configure Horizon Workspace in a multi-forest Active Directory environment, you must add a user store for each domain or forest that you plan to integrate with your Horizon Workspace deployment.

The user store is a required construct when you deploy Horizon Workspace in a multi-forest environment. The user store is a collection of users. Associate a user store to an Active Directory forest. This association links one or more identity provider instances, either the Connector or a third-party identity provider, to users and groups in Horizon Workspace.

4. Edit a User Store for a Multi-Forest Active Directory Environment.

Ans: You can edit an existing user store to change the settings. To configure the user login screen to present users with user store names instead of domain names you must edit the existing user stores.

You might want to edit the settings of a user store, such as the sync client or the authenticating identity providers.

**UPN=** User Principal Name.

**Example:** mrs@contoso.com is a UPN.

**Advantages**: To define a user in a specific domain such as Root domain or child domain.

1. **Definition**

UPN suffixes enable users to sign on using an account name that includes the name  
of their domains. UPN suffixes look like email addresses.

1. **Facilities.**

This is useful in complex environments where users might be logging on to computers

that are members of domains that are different from the domains that host their accounts.

1. **Default status**

By default, all users use the UPN suffix that is the name of the root domain, even if their  
accounts are in a child domain

1. **Configuration step**

We configure UPN suffixes using the Active Directory Domains and Trusts console.

1. **Others**

When we are configuring forest trusts, we can block or allow user authentication based on UPN suffix.

***What are Domain trees?***

Ans: A domain tree is a set of names that share a common root domain name. For example contoso.com can have pacifi.contoso.com and atlantic.contoso.com as child domains and these  
Domains can have child domains themselves. A forest can have multiple domain trees. When  
you create a new tree in a forest, the root of the new tree is a child domain of the original root  
domain.

**MCQ:**

**Length for a host of 64 characters**

**When you do need to allow users from partner organizations to have access to resources**

**1. What is Trust?**

**Ans:** Communication between domains occurs through trusts. Trusts are authentication pipelines which make it possible for users to access resources from one domain to another domain.

**2. Trust types?**

**Ans:**

**Default trusts:**

By default, two-way, transitive trusts are automatically created when a new domain is added to a domain tree or forest root domain using the Active Directory Installation Wizard. The two default trust types are defined in the following table.

|  |  |  |  |
| --- | --- | --- | --- |
| **Trust type** | **Transitivity** | **Direction** | **Description** |
| Parent and child | Transitive | Two-way | By default, when a new child domain is added to an existing domain tree, a new parent and child trust is established. Authentication requests made from subordinate domains flow upward through their parent to the trusting domain. |
| Tree-root | Transitive | Two-way | By default, when a new domain tree is created in an existing forest, a new tree-root trust is established |

**Other trusts:**

When creating external, shortcut, realm, or forest trusts, you have the option to create each side of the trust separately or both sides of a trust simultaneously.

**3. What is trust transitivity?**

**Ans:** A transitive trust is one that extends beyond the original trusting domains.

For example, if you have a trust between two domain forests and that trust is transitive; all the domains in each of the forests trust each other.

Forest trusts are transitive by default.

External trusts are not transitive by default.

**4. What is trust direction?**

**Ans:** When we create a new trust, we specify a trust direction.

You can choose a two-way (or bidirectional) trust or a unidirectional trust, which is either one-way incoming or one-way outgoing.

**Upgrading existing domains and forests**

1. You can use one of two strategies when upgrading an existing domain so that you can configure it at the Windows Server 2012 functional level

2. You can’t directly upgrade Windows Server 2003 to Windows Server 2012

3. Windows operating systems never support direct upgrades from x86 versions to x64 versions.