Lesson 14: Configuring a Domain and Forest

MOAC 70-412: Configuring Advanced Windows Server 2012 Services

Microsoft Official Academic Course

WILEY

Overview

- Objective 5.1 – Configure a domain and forest.
  - Implement multi-domain and multi-forest Active Directory environments including interoperability with previous versions of Active Directory
  - Upgrade existing domains and forests including environment preparation and functional levels
  - Configure multiple user principal name (UPN) suffixes

Implementing Complex Active Directory Environments

Lesson 14: Configuring a Domain and Forest

Directory Service

- A ***directory service***
  - Stores, organizes, and provides access to information in a directory.
  - Is used for locating, managing, administering, and organizing common items and network resources (e.g., volumes, folders, files, printers, users, groups, devices, telephone numbers, and other objects).
- One popular directory service used by many organizations is Microsoft's Active Directory.

Active Directory

- ***Active Directory*** is a technology created by Microsoft that provides a variety of network services, including:
  - Lightweight Directory Access Protocol (LDAP)
  - Domain Name System (DNS) based naming and other network information
  - Security mechanism for authentication that includes Kerberos-based and single sign-on authentication
  - Security mechanism for authorization and auditing
  - Central location for network administration and delegation of authority
  - Policy-based management for user and computer accounts

Logical Components of Active Directory

- ***Organizational units***
  - Containers in a domain that allow you to organize and group resources for easier administration, including delegating administrative rights.
- ***Domains***
  - An administrative boundary for users and computers, which are stored in a common directory database.
  - A single domain can span multiple physical locations or sites and contain millions of objects.
- ***Domain trees***
  - Collections of domains that are grouped together in hierarchical structures and that share a common root domain.
  - Can have a single domain or many domains. The domains within a tree have a contiguous namespace.

Logical Components of Active Directory

- ***Forests***
  - Collections of domain trees that share a common AD DS directory schema.
  - Can contain one or more domain trees or domains, all of which share a common logical structure, global catalog, directory schema, and directory configuration, as well as automatic two-way transitive trust relationships.
  - The first domain in the forest is called the *forest root domain*.
  - For multiple domain trees, each domain tree consists of a unique namespace.
- ***Trust relationships***
  - Allow users in one domain to access resources in another domain.
  - Domains within a tree and forest are automatically created as two-way transitive trusts.
    - A transitive trust is based on the following concept: If domain A trusts domain B, and domain B trusts domain C, then domain A trusts domain C.

Physical Components of Active Directory

- ***Domain controllers***
  - The servers that contain the Active Directory databases.
  - A domain partition stores only the information about objects located in that domain.
  - All domain controllers are peers in the domain and manage replication as a unit.
- ***Global catalog servers***
  - A domain controller that stores a full copy of all Active Directory objects in the directory for its host domain and a partial copy of all objects for all other domains in the forest.
  - A global catalog is created automatically on the first domain controller in the forest.
  - Optionally, other domain controllers can be configured to serve as global catalogs.

Active Directory Database

- Active Directory data is stored in an Active Directory database.
- By default, the Active Directory database is stored in an Active Directory database file (C:\Windows\NTDS\Ntds.dit) along with its associated log and temporary files. The Active Directory database uses the Extensible Storage Engine (ESE), which is an indexed and sequential access method (ISAM) database.
- The ESE (Esent.dll) indexes the data in the database file and provides the mechanism to store and retrieve data.
- It supports up to a little over 2 billion objects and up to 16 TB in size. The maximum size of a database record is 8110 bytes, based on an 8-kilobyte (KB) page size.
- The ntds.dit file is approximately 400 MB in size per 1000 users.

Active Directory Database

- An Active Directory database is logically separated into the following directory partitions:
  - **Schema partition (one per forest)**
  - **Configuration partition (one per forest)**
  - **Domain partition (one per domain)**
  - **Application partition**

Single Domain versus Multiple Domains

- A single domain offers centralized management, where a set of administrators manage everything within the domain.
- Although multiple domains can be centrally managed, multiple domains also offer decentralized management, where different administrators manage each domain.
- If an organization establishes a presence in a foreign country and there are political or legal reasons to have separate security domains, you might consider implementing separate domains.

User and Resource Domains

- Some companies define user domains and resource domains:
  - **User domains**: Used to manage users. Administrators of the user domain have full administrative control over the user accounts, and can create, manage, and remove user accounts.
  - **Resource domains**: Sometimes managed by different management teams that help secure resources.

Multi-Forest Active Directory Environments

- Separate Active Directory forests also offer isolated security.
- By having separate forests, each forest root domain has the Schema Admins and Enterprise Admins AD DS forest.
- Separate forests are often deployed by government defense contractors and other organizations that require security isolation.

Active Directory Schema

- The ***Active Directory schema*** defines the objects and attributes of those objects.
- Because the schema is shared between domains, the domain admins of the various domains must agree on the schema changes.
- Therefore, if you require different schemas, you can use multiple forests.

Upgrading Existing Domains and Forests

Lesson 14: Configuring a Domain and Forest

Upgrading Existing Domains and Forests

- As each version of Windows is introduced, the new version generally includes new features and functionality that was not available previously.
- To get the most out of Windows Server 2012, you should consider upgrading the domain controllers, domains, and forests to Windows Server 2012.

Upgrading Existing Domains and Forests

- Because Active Directory is a key component for many organizations, you must maintain Active Directory and be careful when upgrading to a newer version.
- Depending on your needs, the current state of Active Directory, and the hardware that Active Directory is running on, there are several options you can use to upgrade the Active Directory environment. These options include:
  - *In-place upgrade*
  - Add servers running Windows Server 2012 and promote to domain controllers
  - Create a new AD DS Windows Server 2012 domain and migrate the objects to the new domain or merge the domains together

Understanding Domain and Forest Functional Levels

- ***Domain functional levels*** and ***forest functional levels*** allow administrators to enable domain- or forest-wide Active Directory features within a network environment, while maintaining compatibility for older operating systems.
- The functional level of the domain or forest depends on the version of the domain controllers in the domain or forest.
- After all domain controllers are upgraded within a domain or forest, the domain or forest functional level can be upgraded so that newer features can be made available.

Domain Functional Levels

- As of Windows Server 2012, there are four available domain functional levels: Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012.
- If you have multiple domains within a tree, you can upgrade the functional level of a domain, without affecting the other domains.
- Windows Server 2012 domain controllers do not support the Windows 2000 native mode functional level that was available with Windows Server 2008 R2 and earlier.
- The Windows Server 2003 domain functional level supports domain controllers running Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012. It does not allow the presence of Windows 2000 domain controllers.

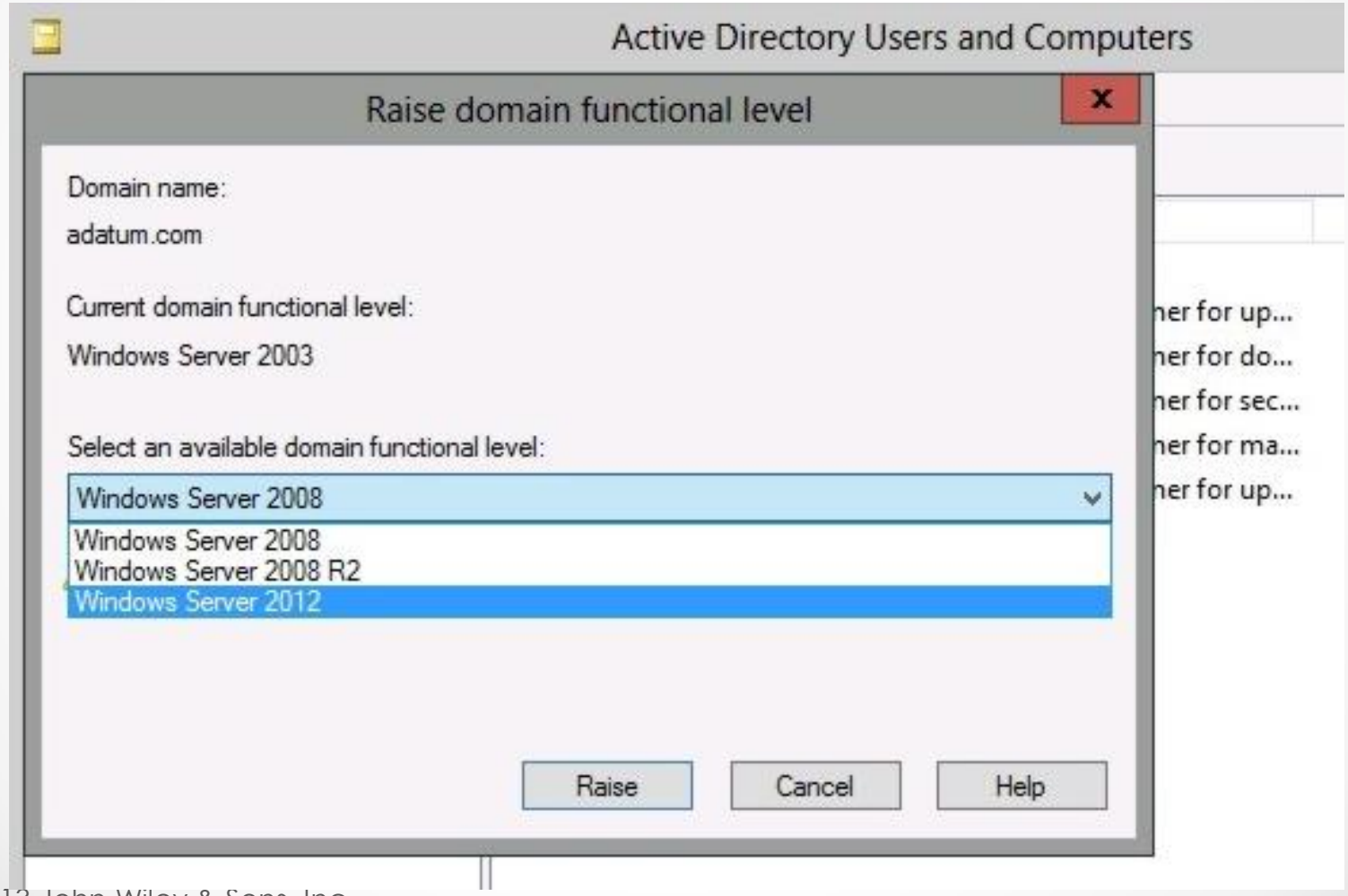
Domain Functional Levels

- The Windows Server 2012 domain functional levels support only domain controllers running Windows Server 2012. It includes all the features of Windows Server 2008 R2 domain functional mode and includes Key Distribution Center (KDC) support for claims, compound authentication, and Kerberos armoring.
- By using a KDC administrative template policy setting, you can configure domain controllers to support claims and compound authentication for Dynamic Access Control and Kerberos armoring by using Kerberos authentication.

Raising Domain Functional Level

- To raise the domain functional level, you must be a member of the Domain Admins group.
- In addition, the PDC Emulator must be available.
- Before you can raise the domain functional level, ensure that all domain controllers within that domain are running the required version of the Windows operating system.
- Raising the domain functional level is generally a one-way process that cannot be reversed, short of performing an authoritative restore of Active Directory.

Raising Domain Functional Level



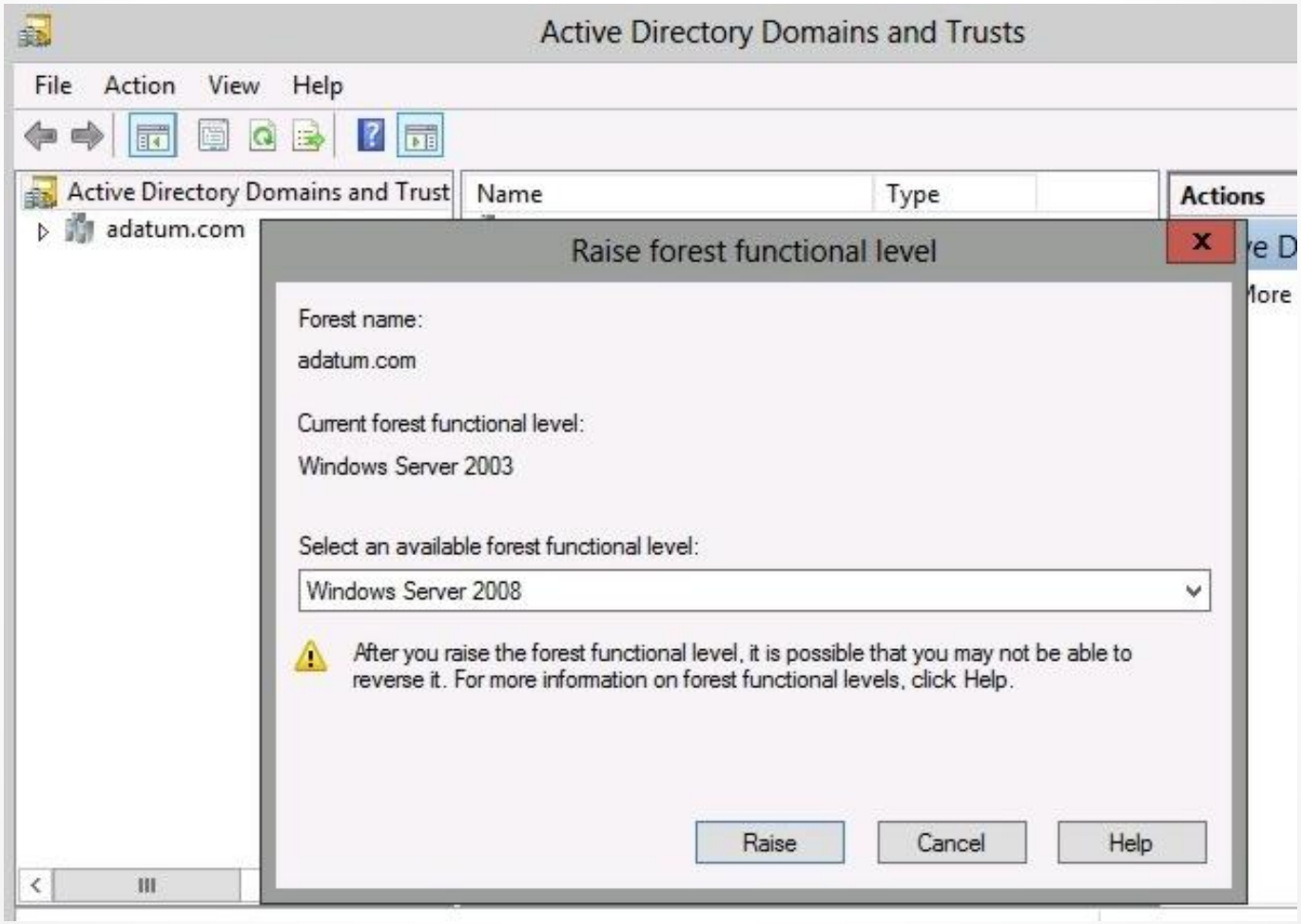
Forest Functional Level

- A forest functional level is similar to a domain functional level, except that it affects all domains within the forest.
- Windows Server 2012 domain controllers support the following forest functional levels: Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012.
- When a forest is raised to a functional level, older domain controllers cannot be introduced into the domain.

Forest Functional Level

- To raise the forest functional level, you must be a member of the Enterprise Admins group.
- In addition, the Schema Master role must be available.
- Before you can raise the forest functional level, ensure that all domains are running the required version of the Windows operating system.
- Raising the forest functional level is generally a one-way process that cannot be reversed, short of performing an authoritative restore of Active Directory.

Forest Functional Level



Upgrading Domain Controllers

- To upgrade from Windows Server 2008 or Windows Server 2008 R2 Active Directory Domain Services (AD DS), you can:
  - Upgrade the operating system of the existing domain controllers to Windows Server 2012 (assuming the hardware can support it)
  - Introduce Windows Server 2012 servers as domain controllers, and then decommission the older domain controllers

Clean Installation

- If you have a server running an old operating system, and you want to move to the new operating system, you can choose to perform an upgrade or perform a clean install.
- An upgrade usually consists of starting the install program and letting the new files overwrite the old files.
- Although the upgrade tends to be simple, and quicker, the clean install allows you to start fresh with no old files or configuration on the machine.
- When you want the most reliable system, it is always best to perform a clean install.

Upgrading the Schema

- For a domain running in Windows Server 2003, Windows Server 2008, or Windows Server 2008 R2 functional level, you can install Windows Server 2012 and add the computer to the domain.
- However, before you promote a server running Windows Server 2012 to a domain controller, you must upgrade the schema.
- In previous versions of Windows, you would use the adprep.exe tool to upgrade the schema.
- While the Windows Server 2012 includes adprep32.exe, it has been deprecated.
- Instead, the Active Directory Domain Services Installation Wizard included in Server Manager incorporates the commands necessary to upgrade the AD DS forest schema.

Configuring Multiple UPN Suffixes

Lesson 14: Configuring a Domain and Forest

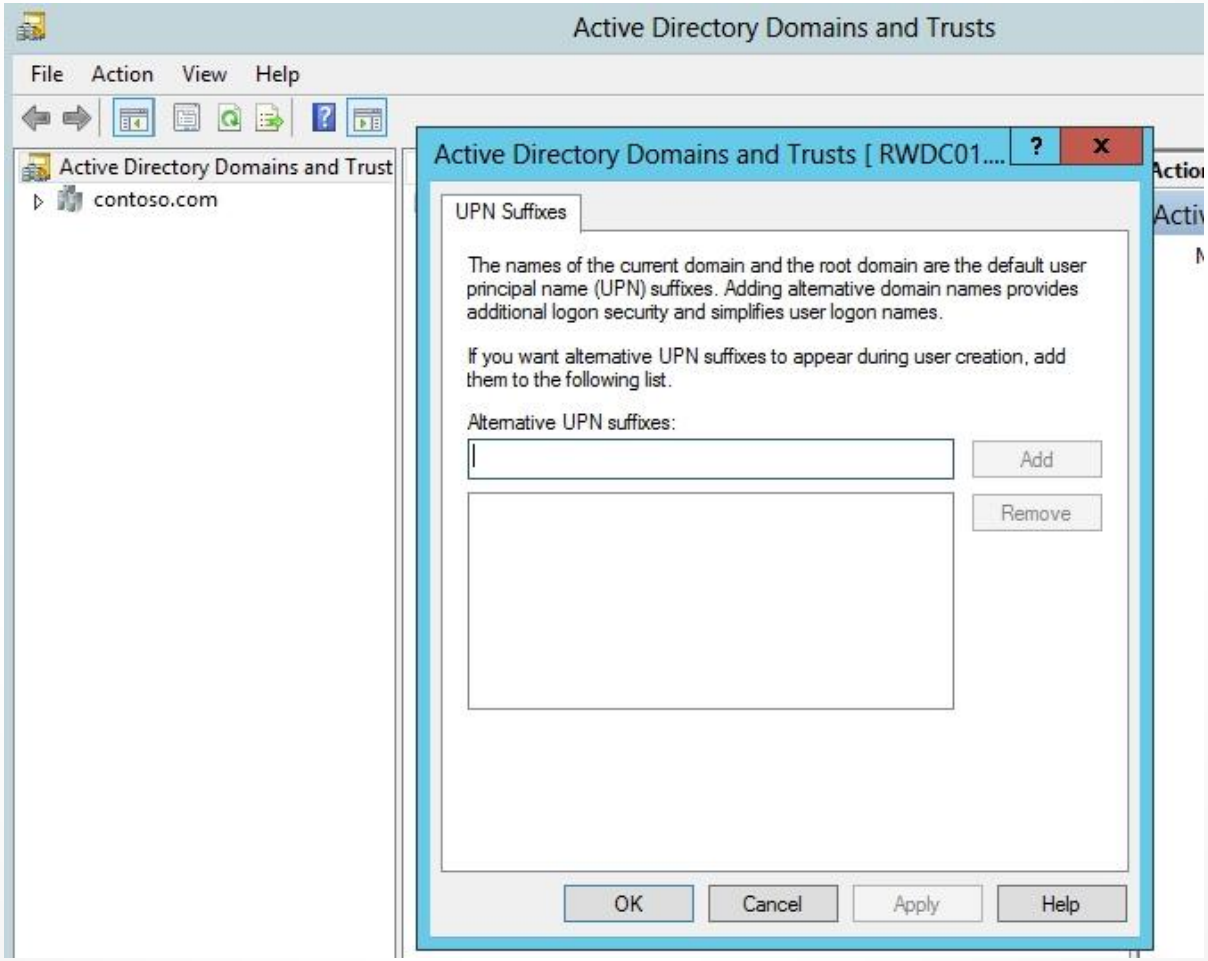
Multiple UPN Suffixes

- Users can log on using one of two ways:
  - Domain username (domain_name\username)
  - ***User Principal Names (UPNs)*** that use an e-mail address format (username@domainname.ext).
- The global catalog resolves the UPN name to a username.
- Using multiple UPN suffixes allows users to log on using an e-mail account name with different DNS namespace names.

Multiple UPN Suffixes

- To add multiple UPN suffixes, use the Active Directory Domains and Trusts management console to manage the domain properties.
- After adding the additional UPN suffixes, users can log on with the alternative UPN suffixes.
- Because two users cannot use the same login name with a multi-domain environment, you must make sure the UPNs are unique.

Multiple UPN Suffixes



Lesson Summary

- A domain is an administrative boundary for users and computers, which is stored in a common directory database. A single domain can span multiple physical locations or sites and can contain millions of objects.
- A domain tree is a collection of domains that are grouped together in hierarchical structures and that share a common root domain. A domain tree can have a single domain or many domains.
- A forest is a collection of domain trees that share a common Active Directory Domain Services (AD DS) database.

Lesson Summary

- Creating a child domain is similar to installing a stand-alone domain controller. The primary difference is that you must link the child domain to the parent domain.
- Some organizations need more complex environments that require multiple forests. By having a multi-forest organization, each forest has its own configuration, schema, and global catalogs.
- The Active Directory schema defines the objects and attributes of those objects. Because the schema is shared between domains, all domains administrators must agree on the schema changes.
- If the domain controller is running Windows Server 2008 or Windows Server 2008 R2, you can upgrade each domain controller one by one to Windows Server 2012.

Lesson Summary

- To provide backward compatibility with older systems, Windows domains and forests can run at various levels of functionality. However, to get the most out of the domain controllers and utilize all of the available features, you need to upgrade the domain controllers to Windows Server 2012 and raise the domain and forest functional levels to Windows Server 2012.
- Before you can raise the domain functional level, ensure that all domain controllers within that domain are running the required version of the Windows operating system.
- Raising the domain or forest functional level is generally a one-way process that cannot be reversed, short of performing an authoritative restore of Active Directory.

Lesson Summary

- A forest functional level is similar to a domain forest functional level, except that it affects all domains within the forest.
- Although the upgrade tends to be simple, and quicker, the clean install allows you to start fresh with no old files or configuration on the machine.
- Using multiple UPN suffixes allows users to log on using an e-mail account name with different DNS namespace names.