Lesson 13: Installing Domain Controllers

MOAC 70-410: Installing and Configuring Windows Server 2012
Overview

• Exam Objective 5.1: Install Domain Controllers
• Introducing Active Directory
• Deploying Active Directory Domain Services
Introducing Active Directory

Lesson 13: Installing Domain Controllers
Introducing Active Directory

• A directory service is a repository of information about the resources—hardware, software, and human—that are connected to a network.

• Users, computers, and applications throughout the network can access the repository for a variety of purposes:
  o User authentication
  o Storage of configuration data
  o Accessing files and printers
Active Directory Domain Services (AD DS)

- AD DS is a directory service that enables administrators to create organizational divisions called domains.
- A domain is a logical container of network components, hosted by at least one server designated as a domain controller.
Active Directory Functions

- **Authentication** is the process of verifying a user’s identity by using:
  - Passwords
  - Smart cards
  - Biometrics (fingerprint scan)

- **Authorization** is the process of granting the user access only to the resources he or she is permitted to use by using:
  - ACLs and ACEs
The Active Directory Architecture

• Active Directory is a hierarchical directory service, based on the domain, which is scalable in both directions.
• You can subdivide a domain into organizational units and populate it with objects.
• You can create multiple domains and group them into sites, trees, and forests.
• AD DS provides a highly flexible architecture that can accommodate the smallest and the largest organizations.
Objects and Attributes

- An AD DS domain is a hierarchical structure that takes the form of a tree, much like a file system.
- Consists of **objects**, each of which represents a logical or physical resource.
- Each object consists of **attributes** which store information about the object.
- Different objects have different attributes, depending on their function.
- The **directory schema** defines the attributes for each object and the information that is required and optional.
Classes of Objects

A **container object** can have other objects subordinate to it:
- Domain
- Organizational unit

A **leaf object** cannot have subordinate objects:
- Users
- Computers
- Groups
- Applications
- Network resources
Objects and Attributes

The attributes of a user object, as displayed in its Properties sheet.
Domains

• You can create a hierarchy within a domain.
• You can create a hierarchy out of multiple domains.
• You begin the process of designing an Active Directory infrastructure by deciding what domains to create and you begin deploying AD DS by creating your first domain.
Organizational Units (OUs)

- Are container objects within a domain, used to divide the security and administrative responsibility among several divisions or departments
- Function in a subordinate capacity to a domain, like a subdomain, but without the complete separation of security policies
- Can contain other OUs, as well as leaf objects
- Can have separate Group Policy settings applied to them
Organizational Units

Organizational units subordinate to a domain
Groups

• Group objects contain users (from a single or multiple domains or OUs) who require similar access to resources or rights to perform tasks.

• Members of a group inherit rights and permissions assigned to the group.
Domain Trees (1)

• When you create your first domain on an Active Directory network, you are creating the root of a **domain tree**.

• You can populate the tree with additional domains, as long as they are part of the same contiguous namespace.

• When using registered Internet domain names, subdomains can be used to create other domains within the domain tree.
Domain Trees (2)

• You can add as many domains to the tree as you need.
• Each domain in a tree is a separate security entity with its own separate Group Policy settings, permissions, and user accounts.
• Unlike OUs, subdomains in a tree do not inherit permissions and policies from their parent domains.
• Domains in the same tree have bidirectional trust relationships between them, which means that an administrator of a particular domain can grant any user in the tree access to that domain’s resources.
Domain Trees

An internal Active Directory domain tree
Domain Trees

An Active Directory domain tree using an Internet domain name
Forests

• An Active Directory forest consists of one or more separate domain trees, which have the same two-way trust relationships between them as two domains in the same tree.

• When you create the first domain on an Active Directory network, you are creating a new forest, and that first domain becomes the forest root domain.
Global Catalog

Each forest has a global catalog, which is a list of all of the objects in the forest, along with a subset of each object’s attributes.
Functional Levels

• **Functional levels** are designed to provide backwards compatibility in AD DS installations with domain controllers running various versions of the Windows Server operating system.

• By selecting the functional level representing the oldest Windows version running on your domain controllers, you disable the new features so that the various domain controllers can interoperate properly.
Functional Levels

Raising functional levels
Active Directory Communications

- Active Directory services are implemented in the network’s domain controllers.
- Each domain controller hosts one domain, storing the domain’s objects in a database.
- Users and computers that are members of a domain access the domain controller frequently, as they log on to the domain and access domain resources.
- You should have at least two domain controllers to ensure the Active Directory database is available to clients at all times.
Introducing LDAP

• Lightweight Directory Access Protocol (LDAP) has become the standard communications protocol for directory service products, including Active Directory.
• Defines the format of the queries that Active Directory clients send to domain controllers.
• Provides a compound naming structure for uniquely identifying objects in the directory.
Replication

- Replication is when domain controllers within a domain synchronize their database information.
- It is imperative that each domain controller has a database that is identical to the others.
Types of Replication

- **Single-master replication**: A single primary system replicates the contents of its database to one or more secondary systems on the network.

- **Multiple-master replication**: It is possible to make changes to domain objects on any domain controller, which replicates those changes to all of the other domain controllers.
Replication

Single-master replication
Replication

Multiple-master replication
Read-Only Domain Controllers (RODCs)

• A domain controller that supports only incoming replication traffic.
• It is not possible to create, modify, or delete Active Directory objects.
• Intended for use in locations that require a domain controller, but which have less physical security or where there are no administrators present who need read/write access to the Active Directory database.
Sites (1)

• A **site** is a collection of subnets that have good connectivity between them.
• Generally speaking, this means that a site consists of all the local area networks (LANs) at a specific location.
• A different site would be a network at a remote location, connected to the other site using a T-1 or a slower WAN technology.
Sites (2)

• Site divisions are wholly independent of domain, tree, and forest divisions:
  o You can have multiple sites that are part of a single domain.
  o You can have separate domains, trees, or forests for each site.

• The primary reason for creating different sites on an Active Directory network is to control the amount of traffic passing over the relatively slow and expensive WAN links between locations.
A site topology consists of three AD DS object types:

- **Sites**: A site object represents the group of subnets at a single location, with good connectivity.
- **Subnets**: A subnet object represents an IP network at a particular site.
- **Site links**: A site link object represents a WAN connection between two sites.
AD DS Regulatory Functions

Once the site topology is in place you can make decisions about:

- Domain controller location
- Replication traffic control
Deploying Active Directory
Domain Services

Lesson 13: Installing Domain Controllers
Deploying AD DS

There are many variables that can affect the performance of an Active Directory installation:

- The hardware you select for your domain controllers
- The capabilities of your network
- The types of WAN links connecting your remote sites
Installing the AD DS Role

The Add features that are required dialog box in the Add Roles and Features Wizard
Installing the AD DS Role

The Installation progress page in the Add Roles and Features Wizard
Creating a New Forest

The Deployment Configuration page of the Active Directory Domain Services Configuration Wizard

© 2013 John Wiley & Sons, Inc.
Creating a New Forest

The Domain Controller Options page of the Active Directory Domain Services Configuration Wizard

© 2013 John Wiley & Sons, Inc.
Creating a New Forest

The Additional Options page of the Active Directory Domain Services Configuration Wizard

More about additional options

© 2013 John Wiley & Sons, Inc.
Creating a New Forest

The Paths page of the Active Directory Domain Services Configuration Wizard

© 2013 John Wiley & Sons, Inc.
Creating a New Forest

The Prerequisites Check page of the Active Directory Domain Services Configuration Wizard

- All prerequisite checks passed successfully. Click 'Install' to begin installation.

View results:
- Windows Server 2012 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.
  
  For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?Linkid=104751).

- This computer has at least one physical network adapter that does not have static IP address(es) assigned to its IP Properties. If both IPv4 and IPv6 are enabled for a network adapter, both IPv4 and IPv6 static IP addresses should be assigned to both IPv4 and IPv6 Properties of the physical network adapter. Such static IP address(es) assignment should be done to all the physical network adapters for reliable Domain Name System.

- If you click 'Install', the server automatically reboots at the end of the promotion operation.

More about prerequisites

© 2013 John Wiley & Sons, Inc. 42
Adding a Domain Controller to an Existing Domain

The Select a domain from the forest page of the Active Directory Domain Services Configuration Wizard

© 2013 John Wiley & Sons, Inc.
Adding a Domain Controller to an Existing Domain

The Domain Controller Options page of the Active Directory Domain Services Configuration Wizard
Adding a Domain Controller to an Existing Domain

The Additional Options page of the Active Directory Domain Services Configuration Wizard
Creating a New Child Domain in a Forest

The Deployment Configuration page of the Active Directory Domain Services Configuration Wizard
Creating a New Child Domain in a Forest

The Domain Controller Options page of the Active Directory Domain Services Configuration Wizard
Installing AD DS on Server Core

• In Windows Server 2012, it is now possible to install Active Directory Domain Services on a computer running the Server Core installation option and promote the system to a domain controller, all using Windows PowerShell.

• To Install the AD DS role, use the following command:

  Install-WindowsFeature -name AD-Domain-Services -IncludeManagementTools
Installing AD DS on Server Core

After installing the role, you must promote the server to a domain controller using the ADDSDeployment PowerShell module.

There are three separate cmdlets for the three deployment configurations:

- Install-AddForest
- Install-AddDomainController
- Install-AddDomain
Installing AD DS on Server Core

Syntax for the Install-AddDSForest cmdlet in Windows PowerShell
Installing AD DS on Server Core

Another way to do this is to use a computer running Windows Server 2012 with the full GUI option to generate a script.

Begin by running the Active Directory Domain Services Configuration Wizard, configuring all of the options with your desired settings. When you reach the Review Option page, click the View Script button to display the PowerShell code for the appropriate cmdlet.
Installing AD DS on Server Core

An installation script generated by the Active Directory Domain Services Configuration Wizard

```
# Windows PowerShell script for AD DS Deployment
#

Import-Module ADDSDeployment
Install-ADDSDomainController -NoGlobalCatalog:$true
-Credential (Get-Credential)
-CriticalReplicationOnly:$false
-DatabasePath "C:\Windows\NTDS"
-DomainName "adatum.info"
-InstallDns:$false
-LogPath "C:\Windows\NTDS"
-NoRebootOnCompletion:$false
-SiteName "Default-First-Site-Name"
-SysvolPath "C:\Windows\SYSVOL"
-Force:$true
```
Install from Media (IFM)

- **Install from media** is an option that enables administrators to streamline the process of deploying replica domain controllers to remote sites.

- Using a command line tool called *Ndsutil.exe*, administrators can create domain controller installation media that includes a copy of the AD DS database.

- When using this installation media, the data is installed along with the database structure and no replication is needed.
Install From Media (IFM)

An Ntdsutil.exe command sequence
Upgrading AD DS

Two ways to upgrade an AD DS infrastructure:

• Upgrade the existing down-level domain controllers to Windows Server 2012.
• Add a new Windows Server 2012 domain controller to your existing installation.
Removing a Domain Controller

• To remove a domain controller from an AD DS installation, you must begin by running the Remove Roles and Features Wizard.
• Select *Demote this Domain Controller*.
Remove a Domain Controller

The Validation Results dialog box of the Remove Roles and Features Wizard

© 2013 John Wiley & Sons, Inc.
Remove a Domain Controller

The Credentials page of the Active Directory Domain Services Configuration Wizard

The server will be automatically restarted after the demotion operation. Role removal needs to be performed after the restart.
Remove a Domain Controller

The New Administrator Password page of the Active Directory Domain Services Configuration Wizard
Configuring the Global Catalog

• The importance of the global catalog varies depending on the size of your network and its site configuration.
• You can make a domain controller a global catalog server when you promote a server to a domain controller, or you can do it afterward.
Create a Global Catalog Server

The Active Directory Sites and Services console
Create a Global Catalog Server

The NTDS Settings Properties sheet

Description: 
Query Policy: 
DNS Alias: E172DEA5-A4F1-4596-9EF3-2AE63C524A4_msdcshelf

Global Catalog
The amount of time it will take to publish the Global Catalog varies depending on your replication topology.
Troubleshooting DNS SRV Registration Failure

• The Domain Name System (DNS) is essential to the operating of Active Directory Domain Services.

• A special DNS resource record (SRV) was created that enables clients to locate domain controllers and other vital AD DS services.

• The `dcdiag` command can be used to confirm that a domain controller has been registered in the DNS.
Troubleshooting DNS SRV Registration Failure

A successful dcdiag test

© 2013 John Wiley & Sons, Inc.
Lesson Summary

• A directory service is a repository of information about the resources—hardware, software, and human—which are connected to a network. Microsoft first introduced the Active Directory directory service in Windows 2000 Server, and they have upgraded it in each successive server operating system release, including Windows Server 2012.

• When you create your first domain on an Active Directory network, you are, in essence, creating the root of a domain tree. You can populate the tree with additional domains, as long as they are part of the same contiguous name space.

• When beginning a new AD DS installation, the first step is to create a new forest, which you do by creating the first domain in the forest, the forest root domain.
Lesson Summary

• In Windows Server 2012, it is now possible to install AD DS on a computer running the Server Core installation option and promote the system to a domain controller, all using Windows PowerShell.

• Install from media (IFM) is an option that enables administrators to streamline the process of deploying replica domain controllers to remote sites.

• There are two ways to upgrade an AD DS infrastructure. You can upgrade the existing down-level domain controllers to Windows Server 2012, or add a new Windows Server 2012 domain controller to your existing installation.
Lesson Summary

• The global catalog is an index of all the AD DS objects in a forest that prevents systems from having to perform searches among multiple domain controllers.

• The Domain Name System (DNS) is essential to the operating of Active Directory Domain Services. To accommodate directory services such as AD DS, a special DNS resource record was created that enables clients to locate domain controllers and other vital AD DS services.
Copyright 2013 John Wiley & Sons, Inc.
All rights reserved. Reproduction or translation of this work beyond that named in Section 117 of the 1976 United States Copyright Act without the express written consent of the copyright owner is unlawful. Requests for further information should be addressed to the Permissions Department, John Wiley & Sons, Inc. The purchaser may make back-up copies for his/her own use only and not for distribution or resale. The Publisher assumes no responsibility for errors, omissions, or damages, caused by the use of these programs or from the use of the information contained herein.