Department of Information Technology

Lesson 3: Installing Domain Controllers

Server Management

Zina Yaaqub

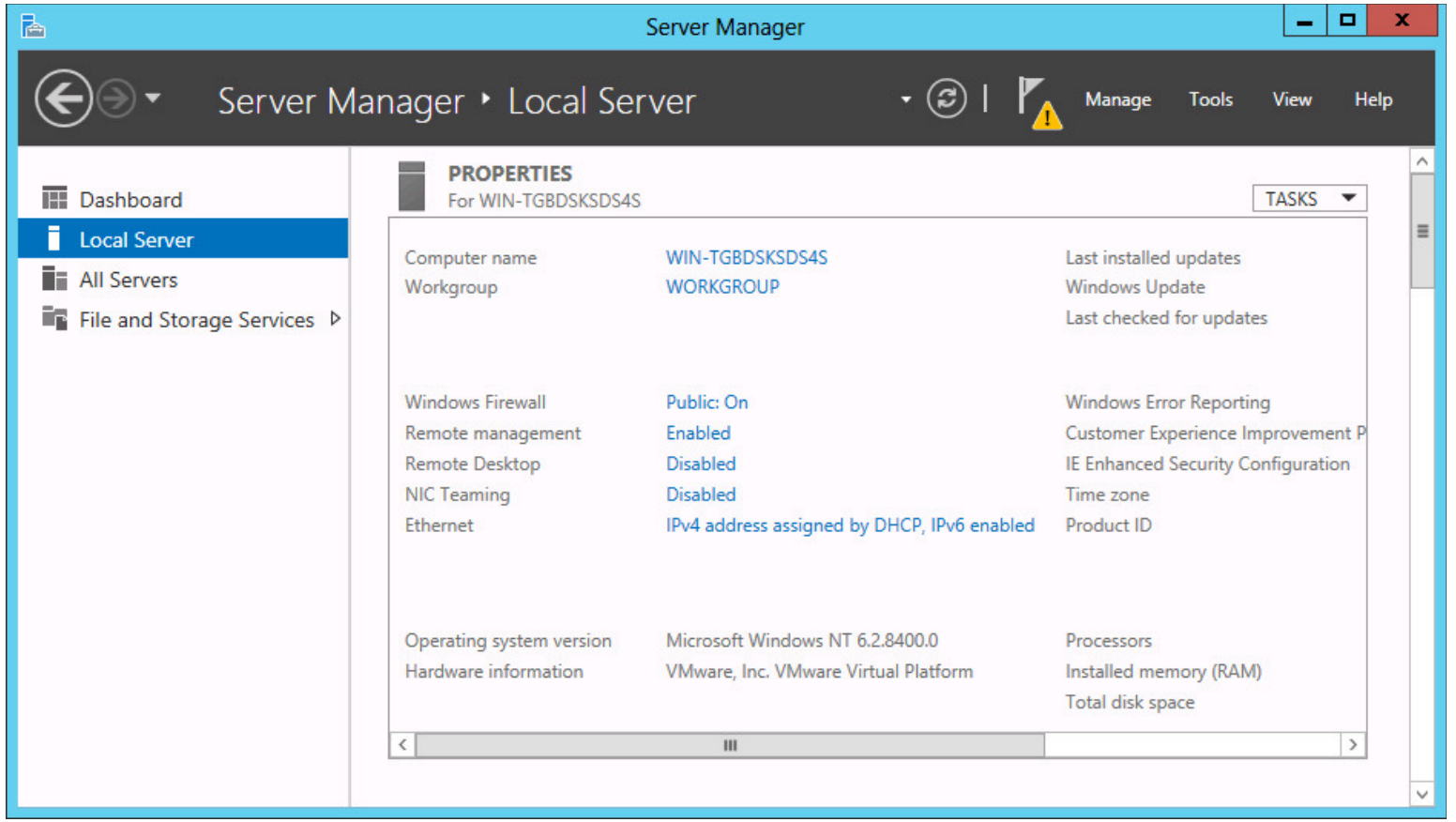
Overview

- Exam Objective : Introducing Active Directory
- Using Roles, Features, and Services
- Using Server Manager
- Replication
- Installing AD DS Role
- Adding a Domain Controller to an Existing Domain

Configuring Services

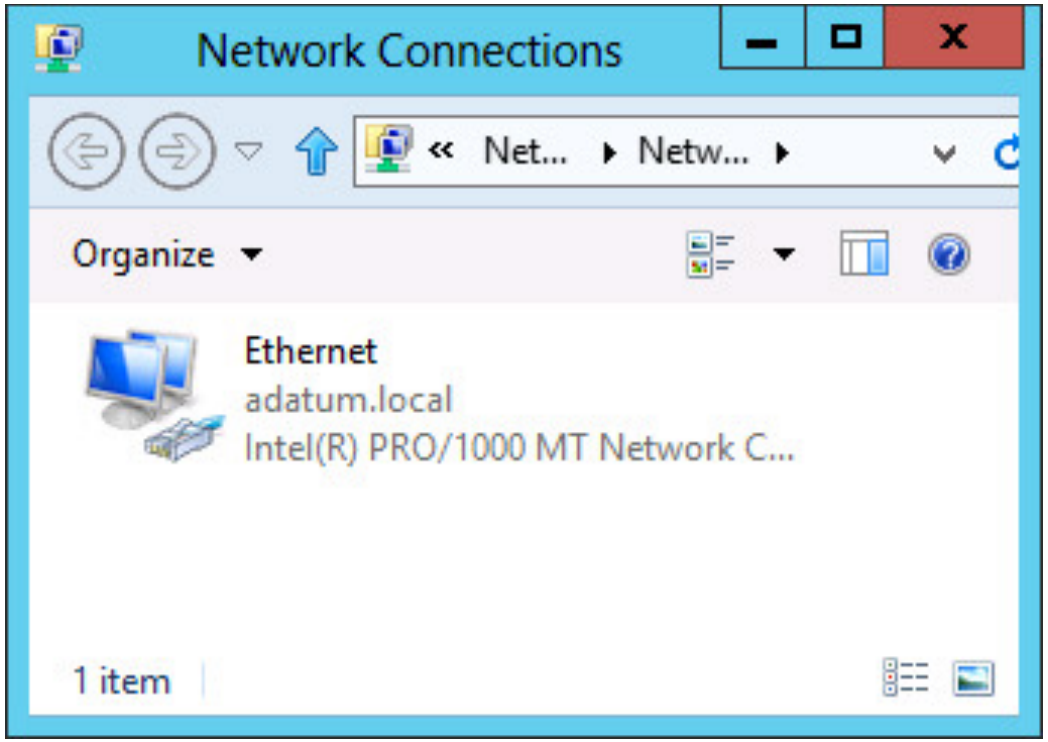
- Server Manager will allow you to view all of the services installed on a server and stop, start, restart, pause, and resume a service.

Using GUI Tools



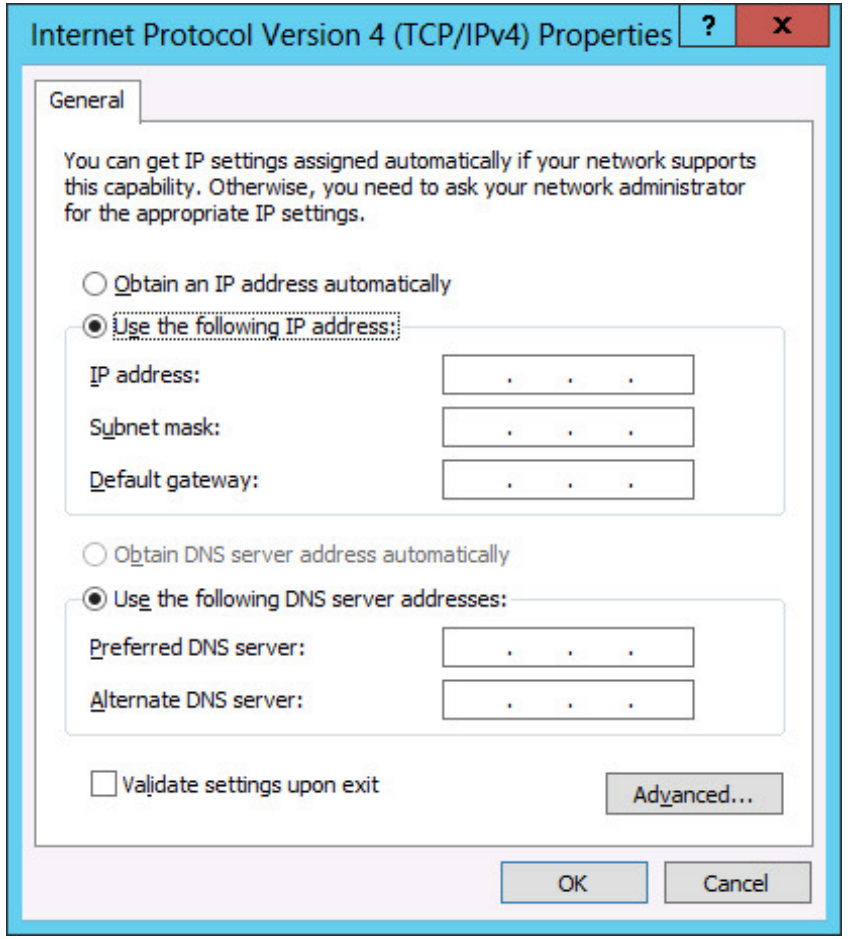
Use the Server Manager for the Local Server to Complete Post-Installation Tasks

Using GUI Tools



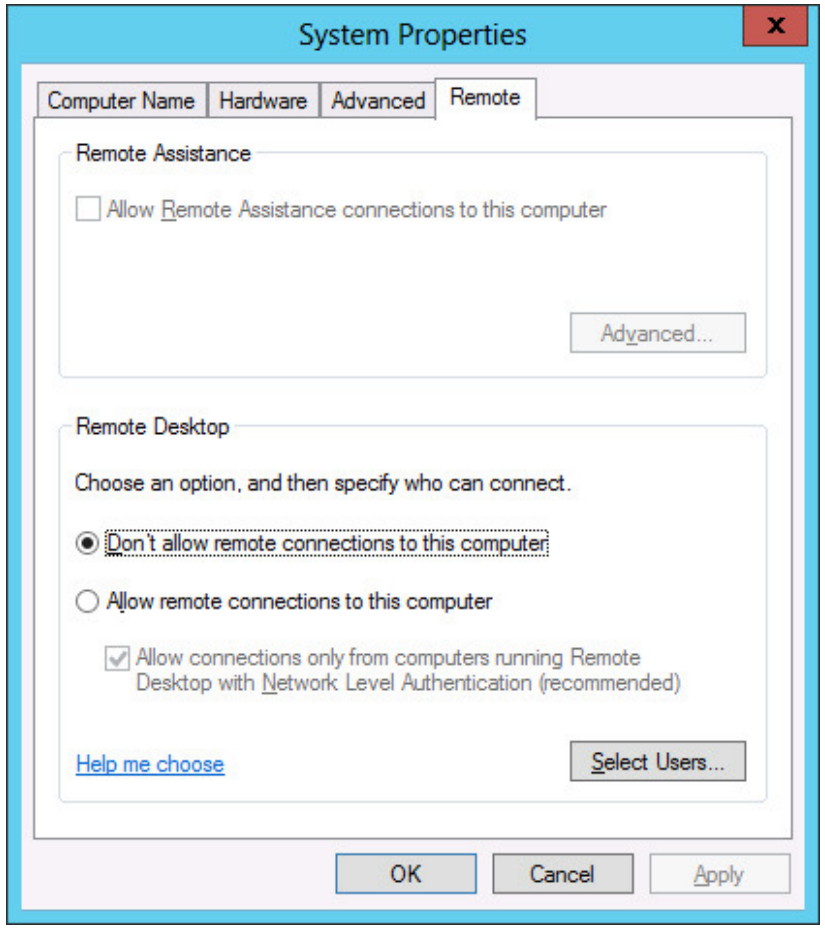
The Network Connections window

Using GUI Tools



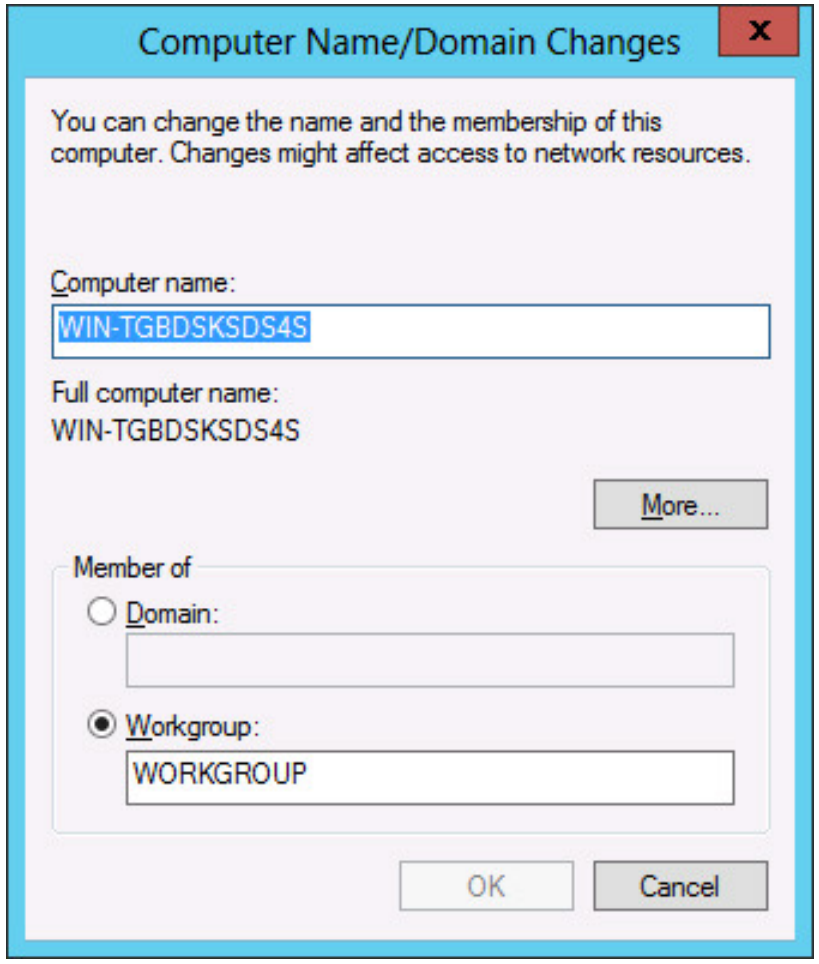
The Internet Protocol Version 4 (TCP/IPv4) Properties sheet

Using GUI Tools



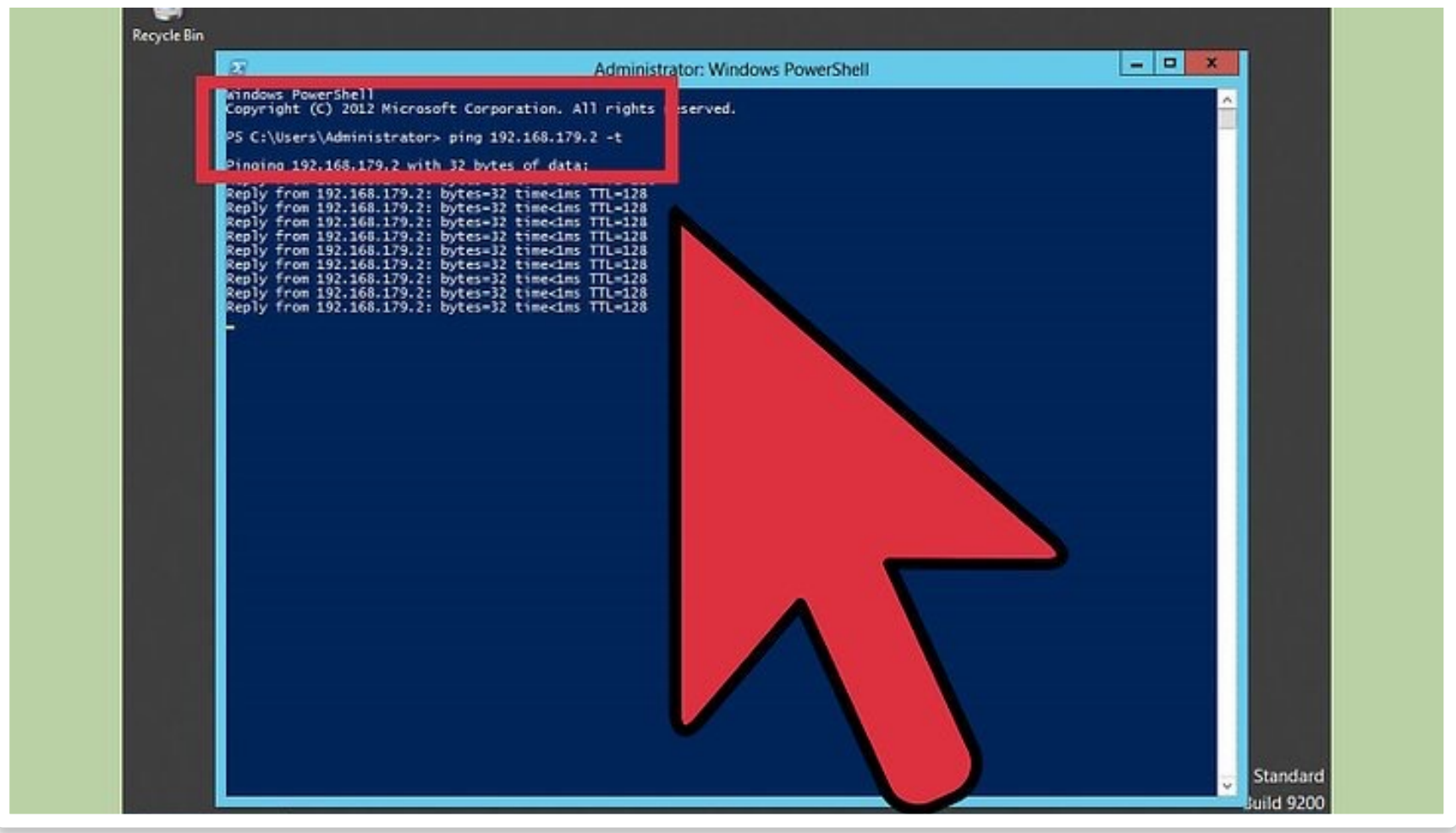
The Remote tab of the System Properties sheet

Using GUI Tools



The Computer Name/Domain Changes dialog box

Using the Ping Command



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:
  - User authentication
  - Storage of configuration data
  - 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**.

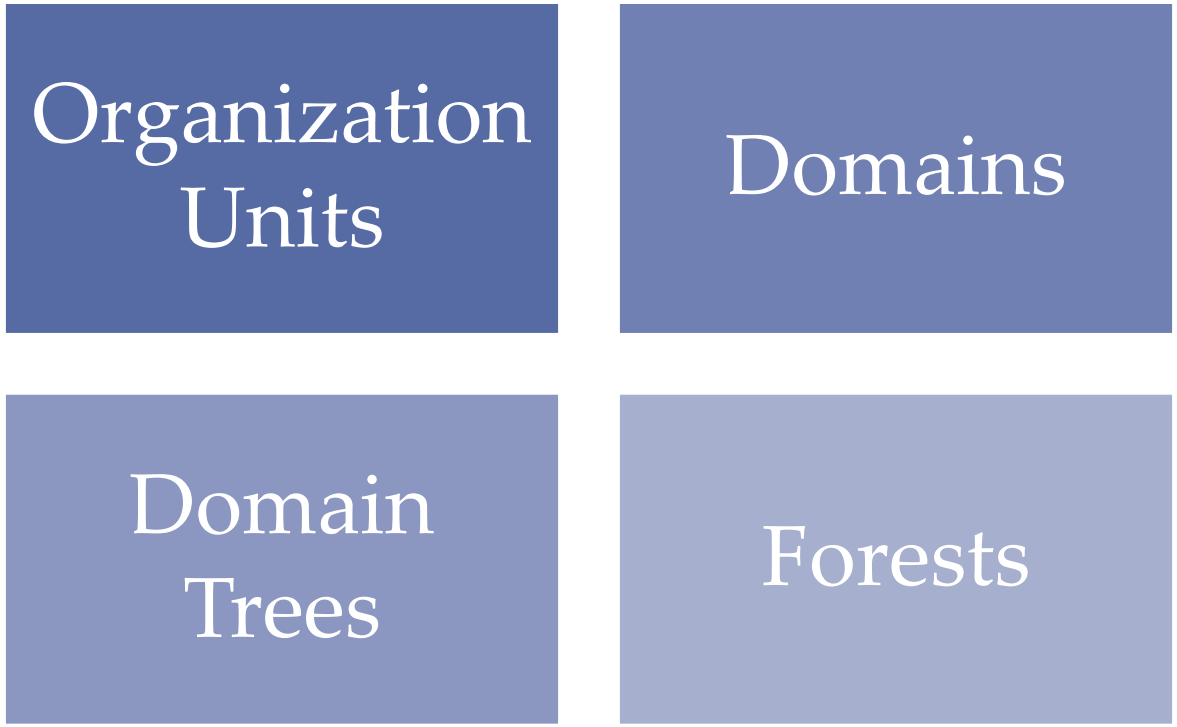
Active Directory Functions

- **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.

Active Directory Logical Components



Active Directory Physical Components

- Domain Controllers
- Global Catalog Servers
- Operations Masters
- Read-Only Domain Controllers

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.

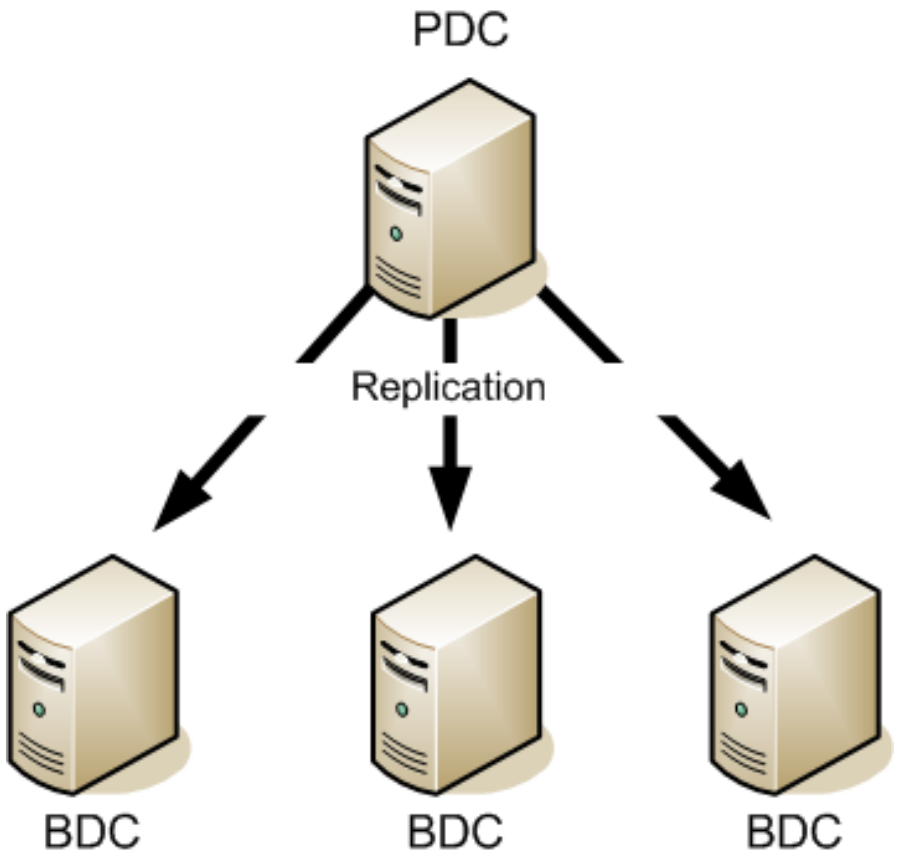
Replication

- **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

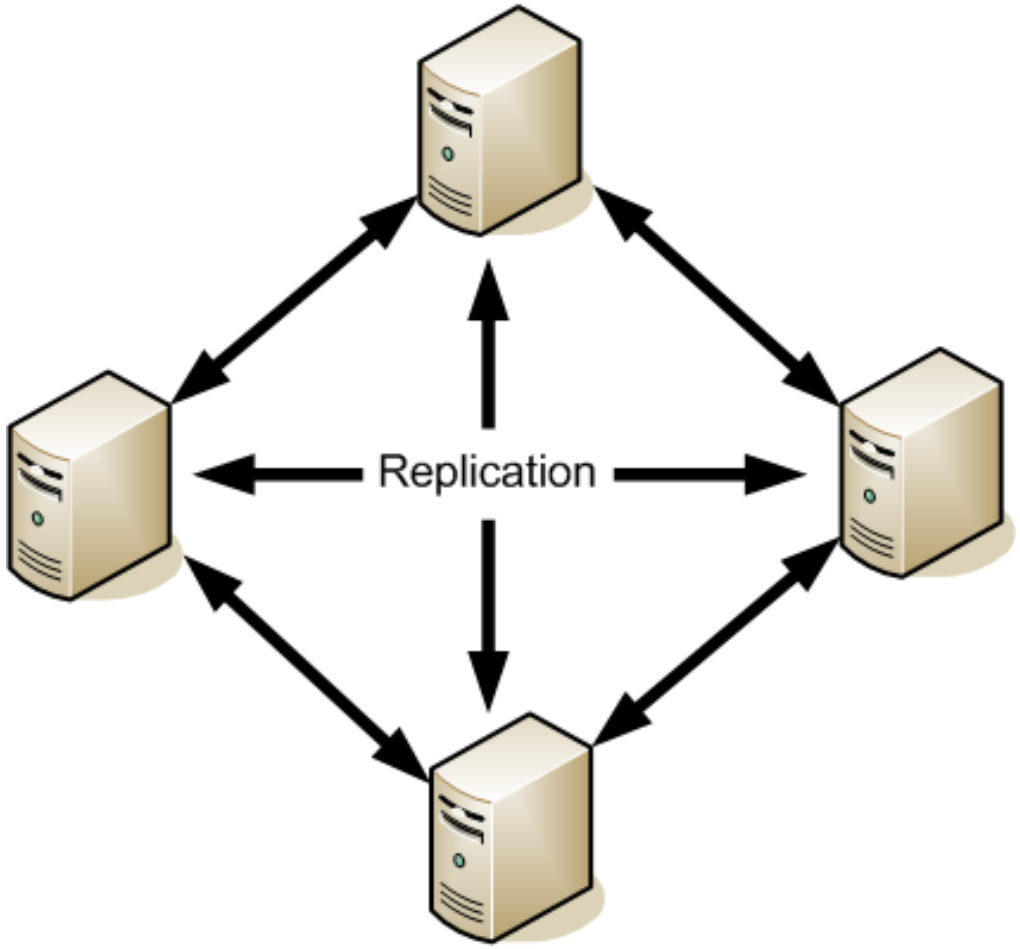
- **Single-master replication**: A single primary system replicates the contents of its database to one or more secondary systems on the network.
- **Multiple-master replication:** It is possible to make changes to domain objects on any domain controller, which replicates those changes to all of the other domain controllers.

Replication



Single-master replication

Replication



Multiple-master replication

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

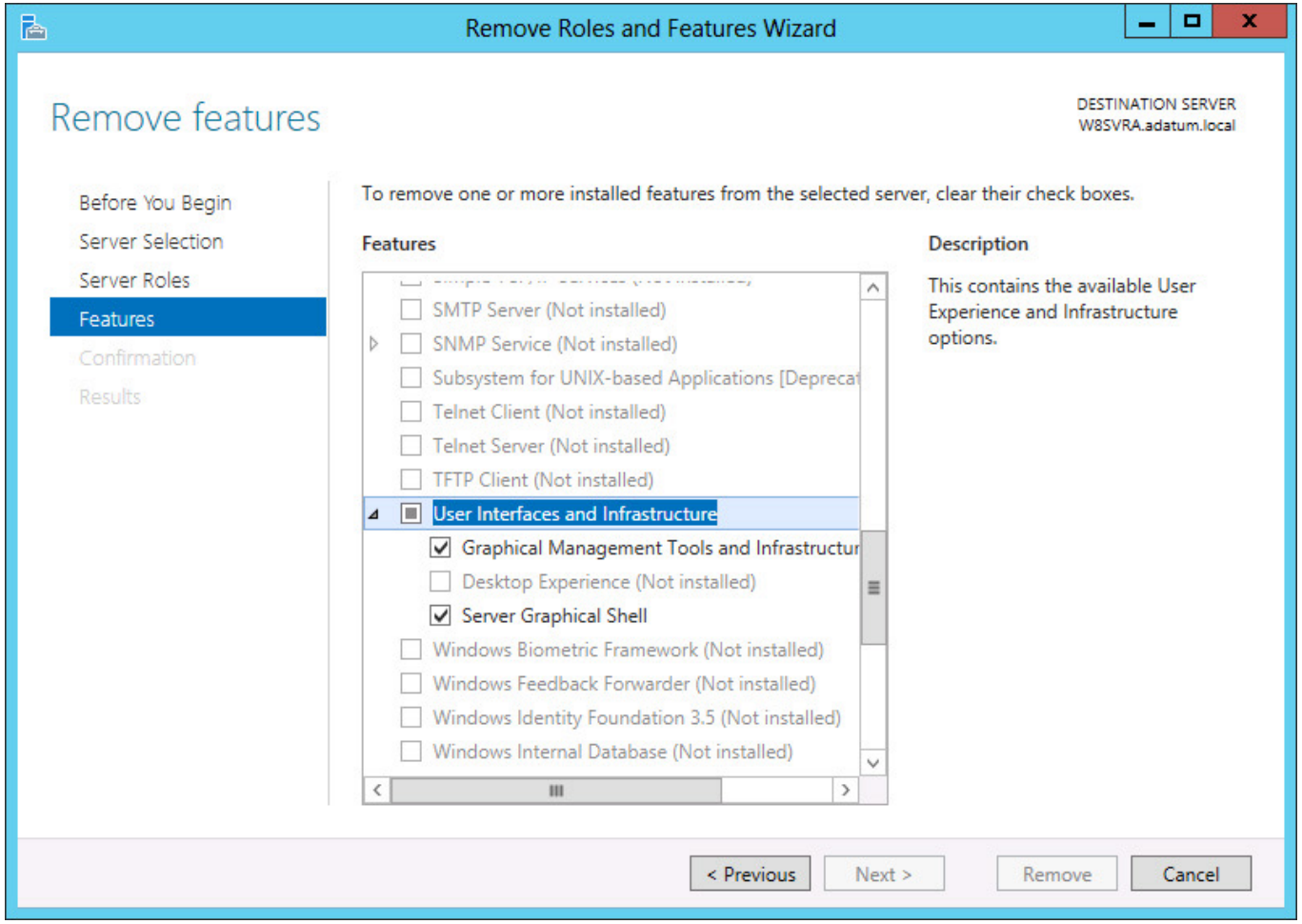
Using Roles, Features, and Services

- **Role**: Define the primary function of a server
  - Example: Web Server (IIS)
- **Feature**: A smaller module, typically with a single purpose
  - Example: a management tool, extension, or optional component
- **Service**: Programs that run continuously in the background, waiting for a client to send a request

Adding Roles and Features

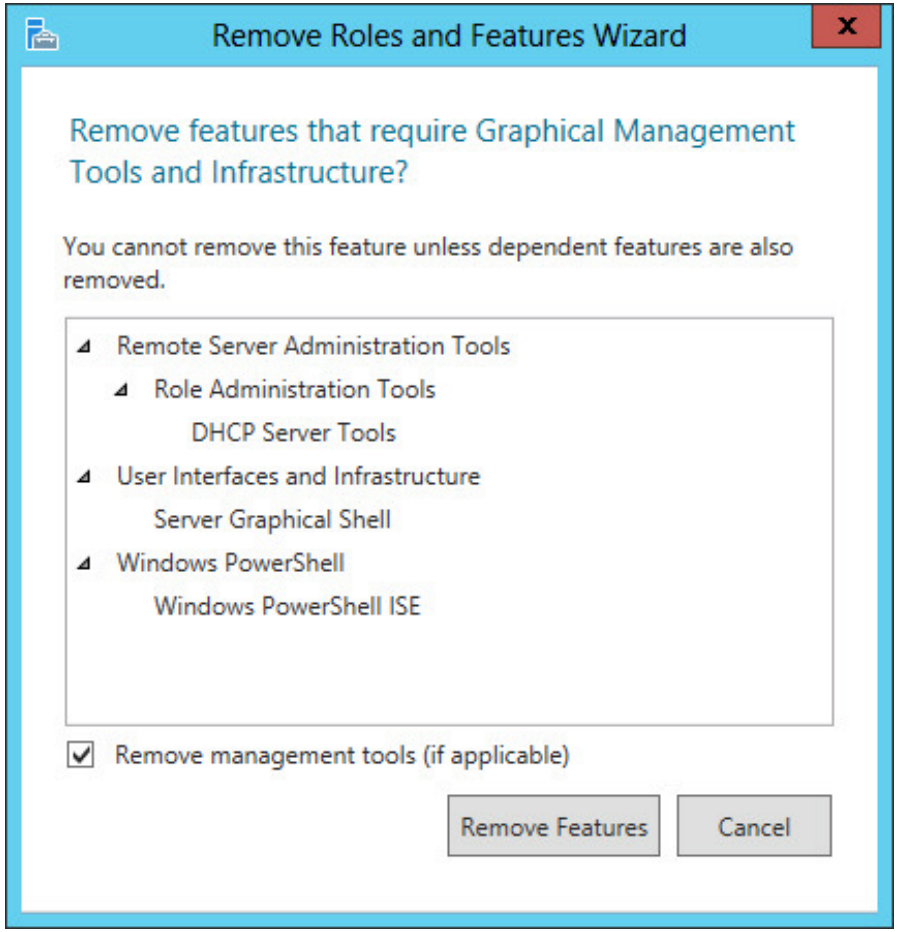
- Use the Add Roles and Features Wizard in the Server Manager.
- Add multiple servers to the Server Manager interface to deploy roles and features to any of your servers.

Converting a GUI Server to Server Core



The Remove features page in Server Manager

Converting a GUI Server to Server Core

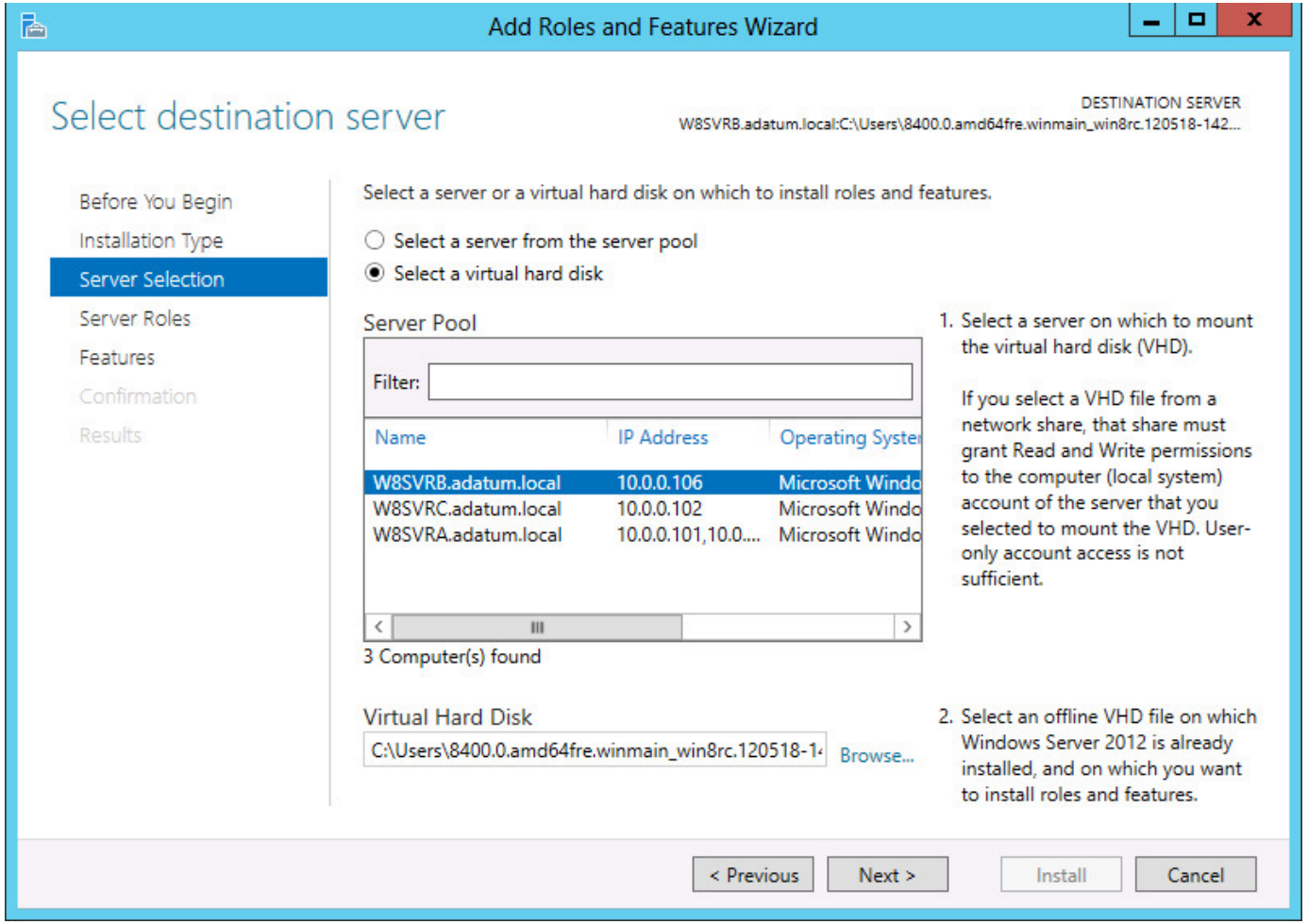


The Remove features that require Graphical Management Tools and Infrastructure dialog box

Deploying Roles to VHDs

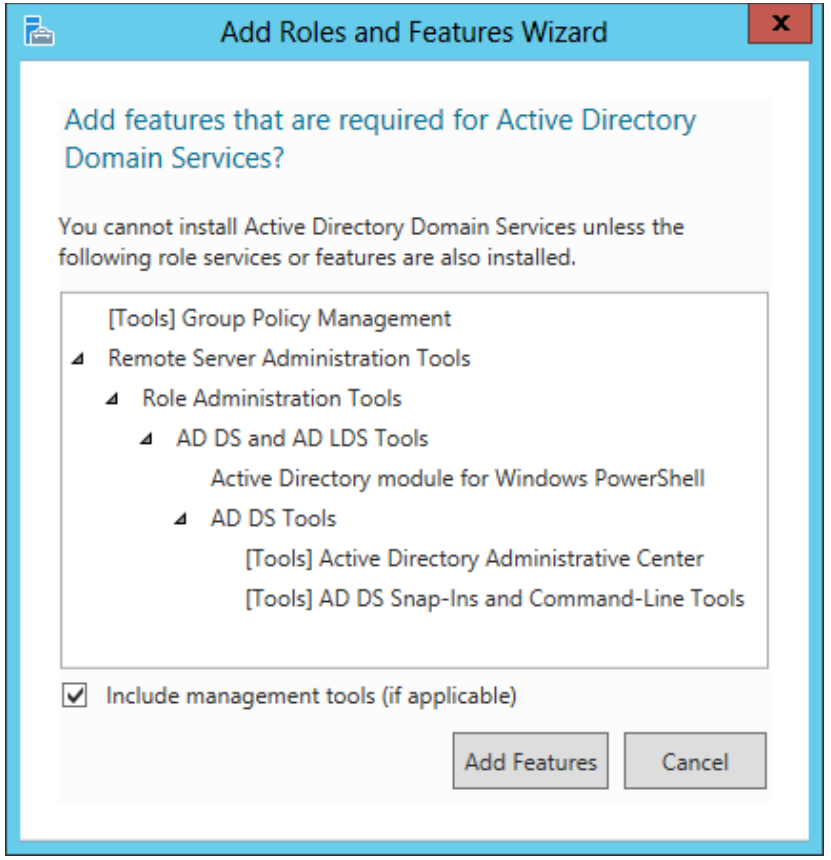
- In addition to installing roles and features to servers on the network, Server Manager enables administrators to install them to virtual machines that are in an offline state.

Installing Roles and Features— Offline VHD



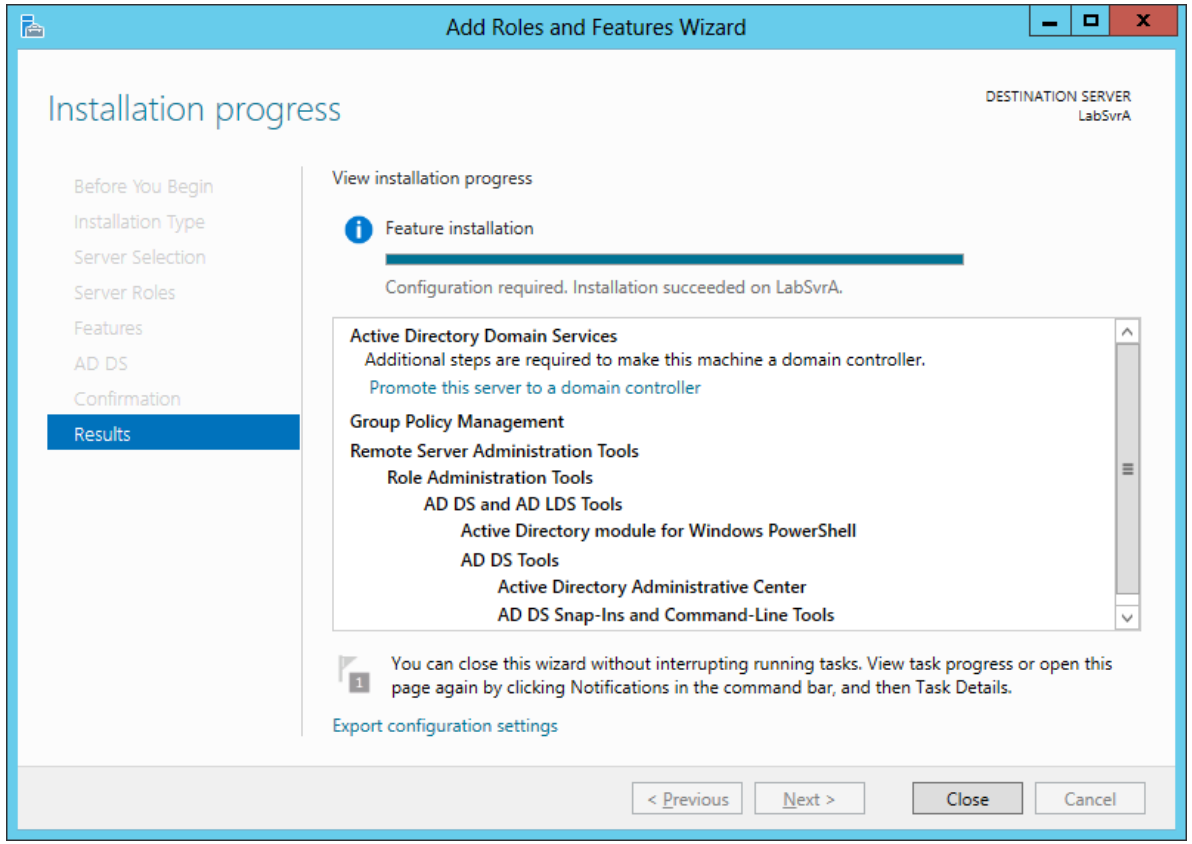
The Select destination server page in the Add Roles and Features Wizard

Installing the AD DS Role



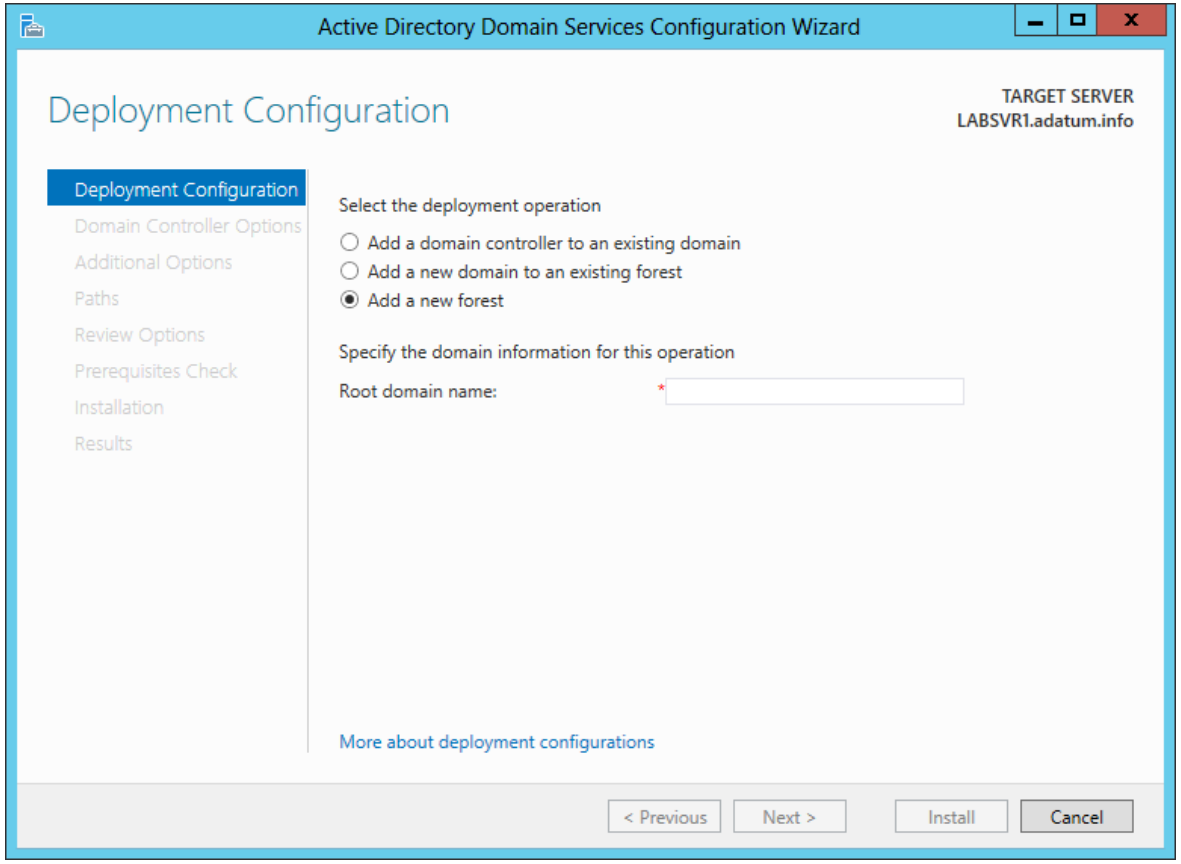
The Add features that are required dialog box in the Add Roles and Features Wizard

Installing the AD DS Role



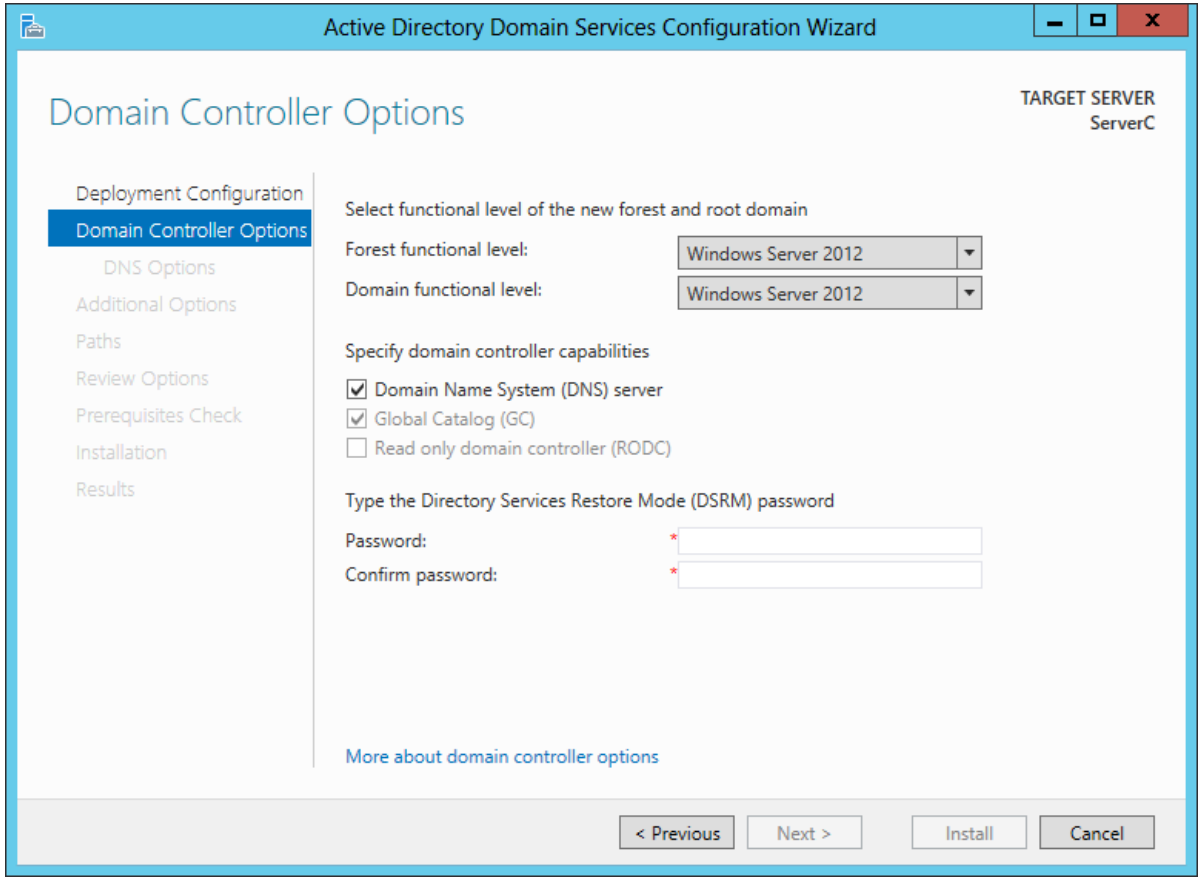
The Installation progress page in the Add Roles and Features Wizard

Creating a New Forest



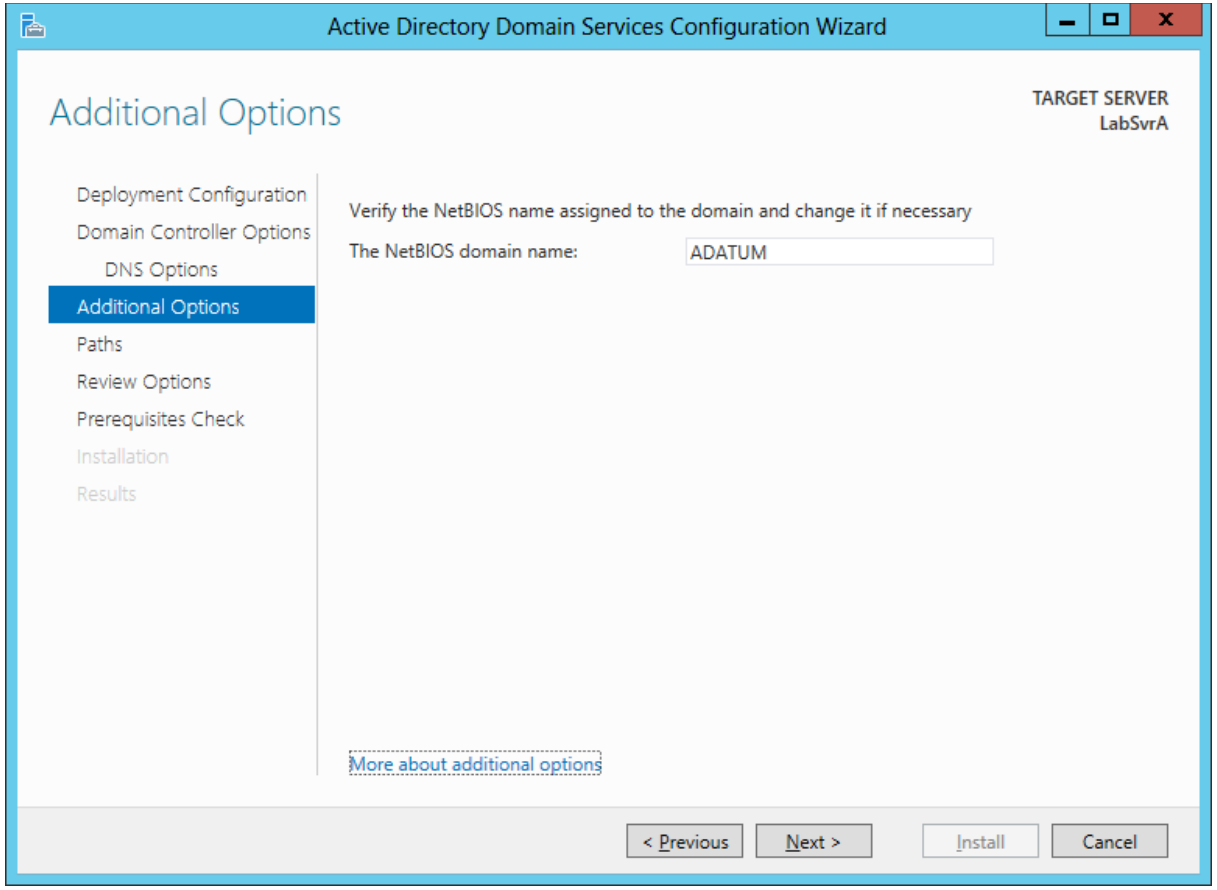
The Deployment Configuration page of the Active Directory Domain Services Configuration Wizard

Creating a New Forest



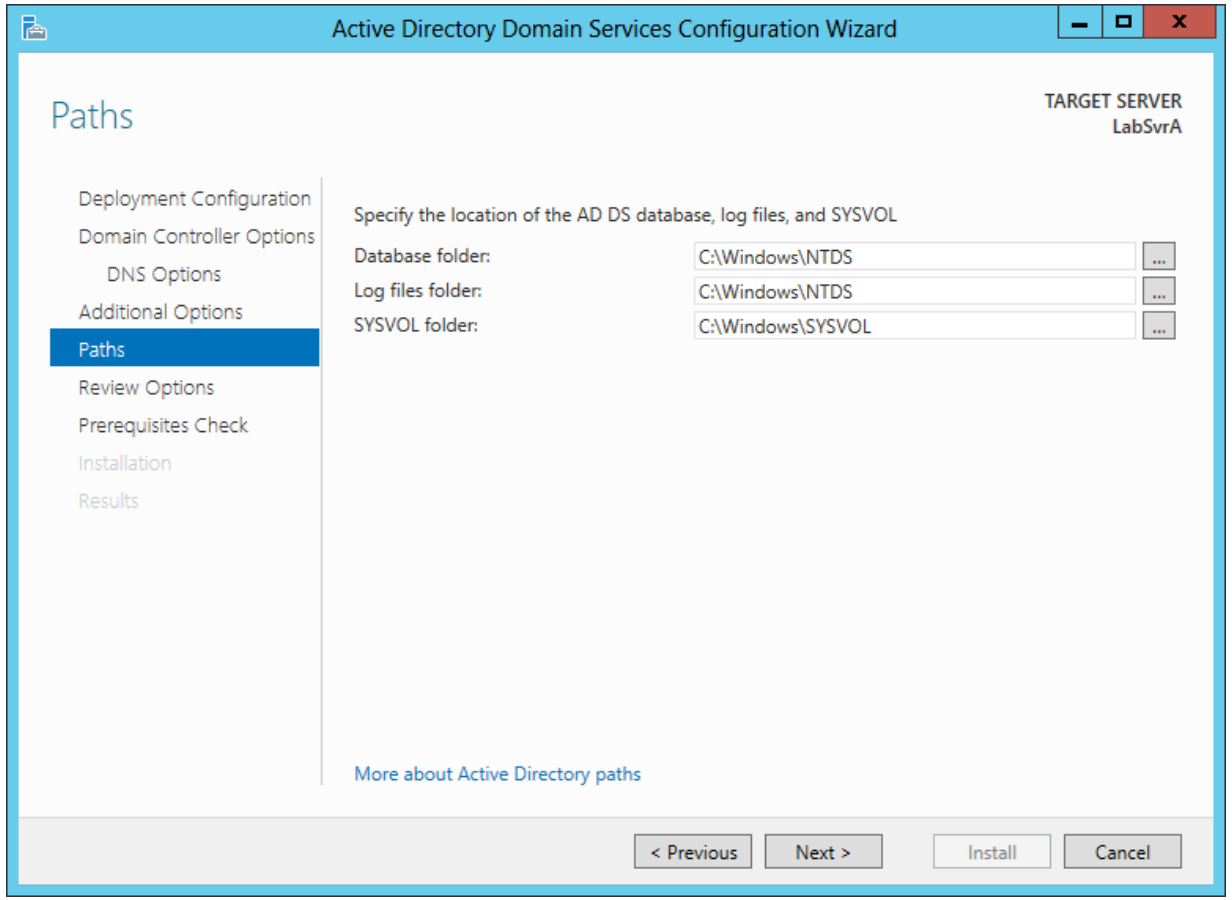
The Domain Controller Options page of the Active Directory Domain Services Configuration Wizard

Creating a New Forest



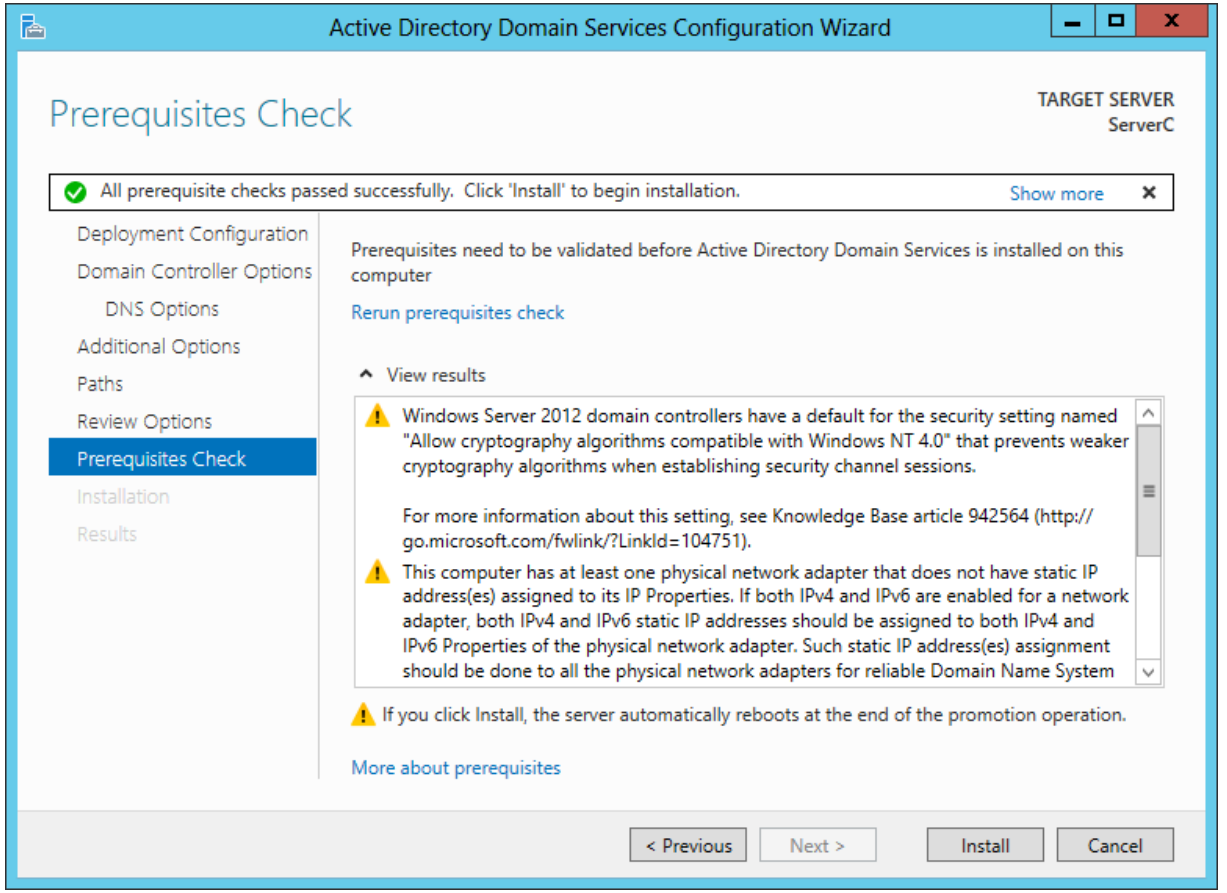
The Additional Options page of the Active Directory Domain Services Configuration Wizard

Creating a New Forest



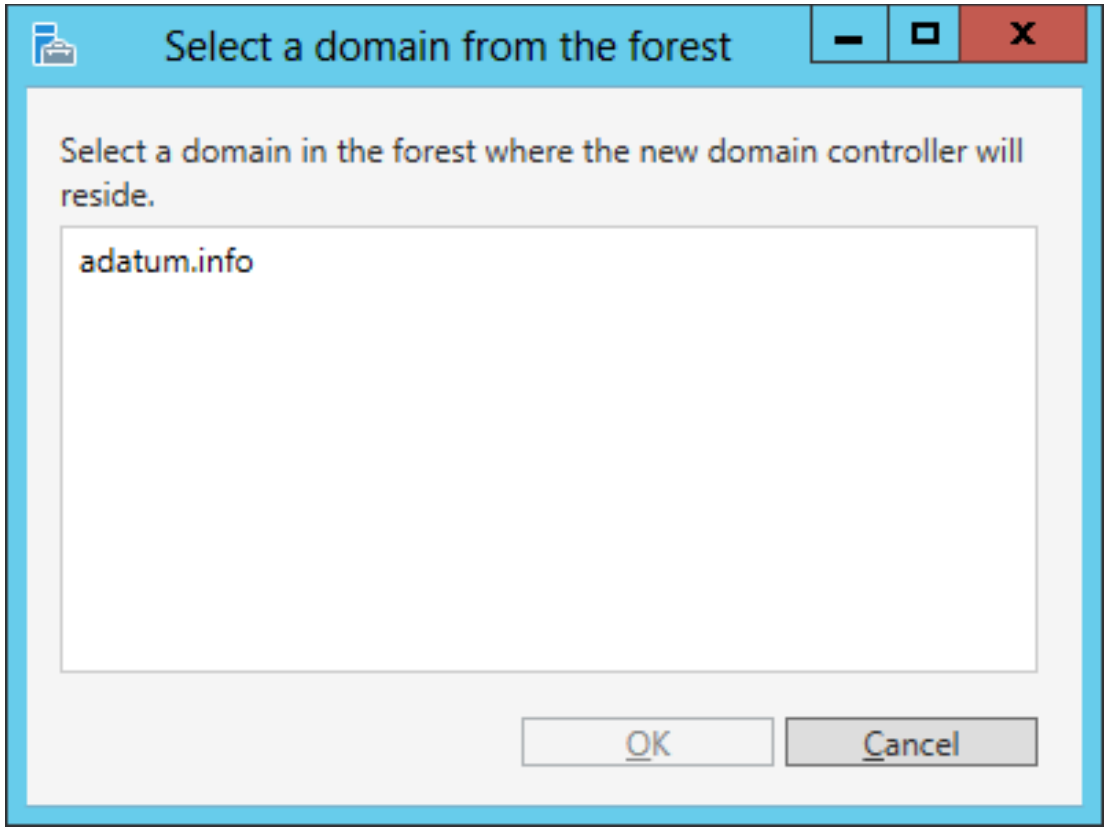
The Paths page of the Active Directory Domain Services Configuration Wizard

Creating a New Forest



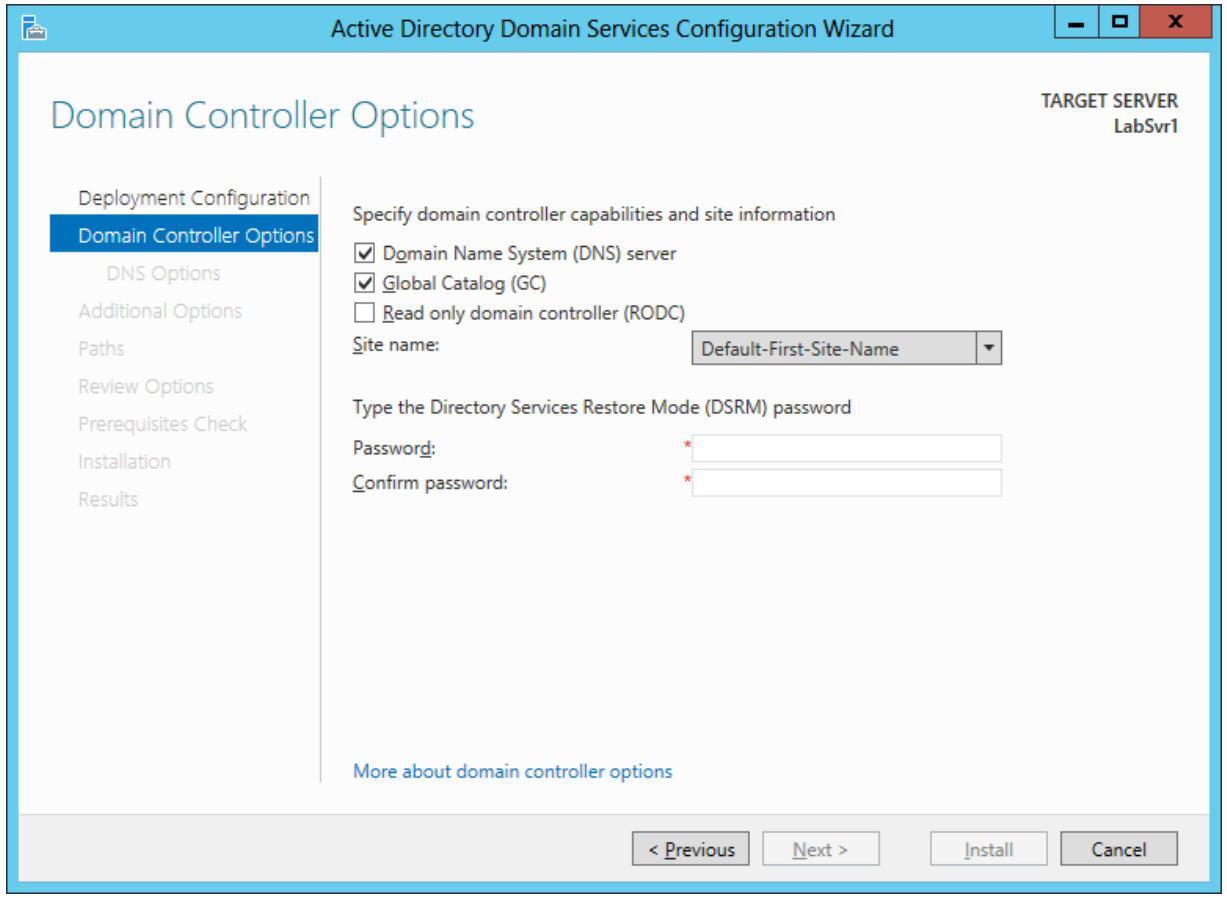
The Prerequisites Check page of the Active Directory Domain Services Configuration Wizard

Adding a Domain Controller to an Existing Domain



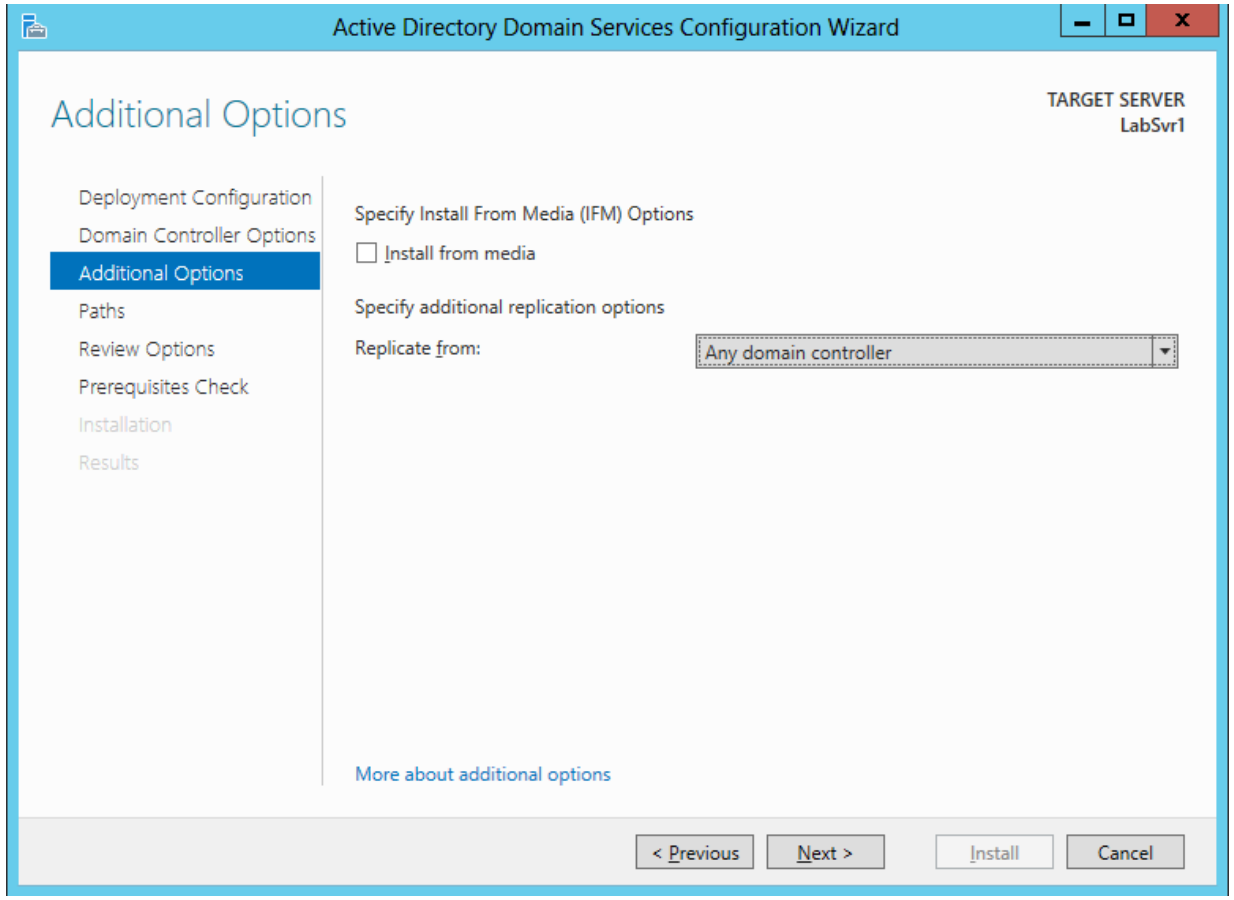
The Select a domain from the forest page of the Active Directory Domain Services Configuration Wizard

Adding a Domain Controller to an Existing Domain



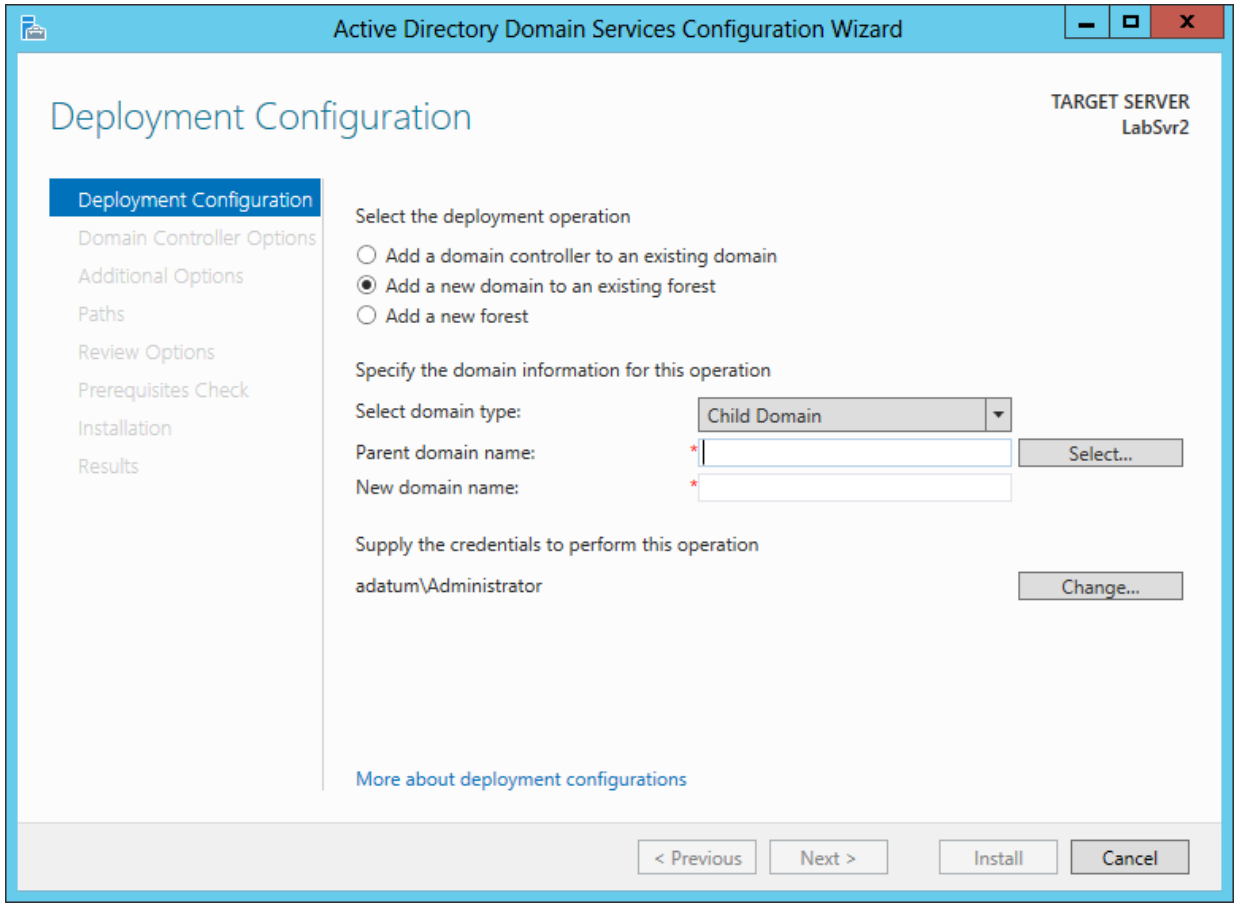
The Domain Controller Options page of the Active Directory Domain Services Configuration Wizard

Adding a Domain Controller to an Existing Domain



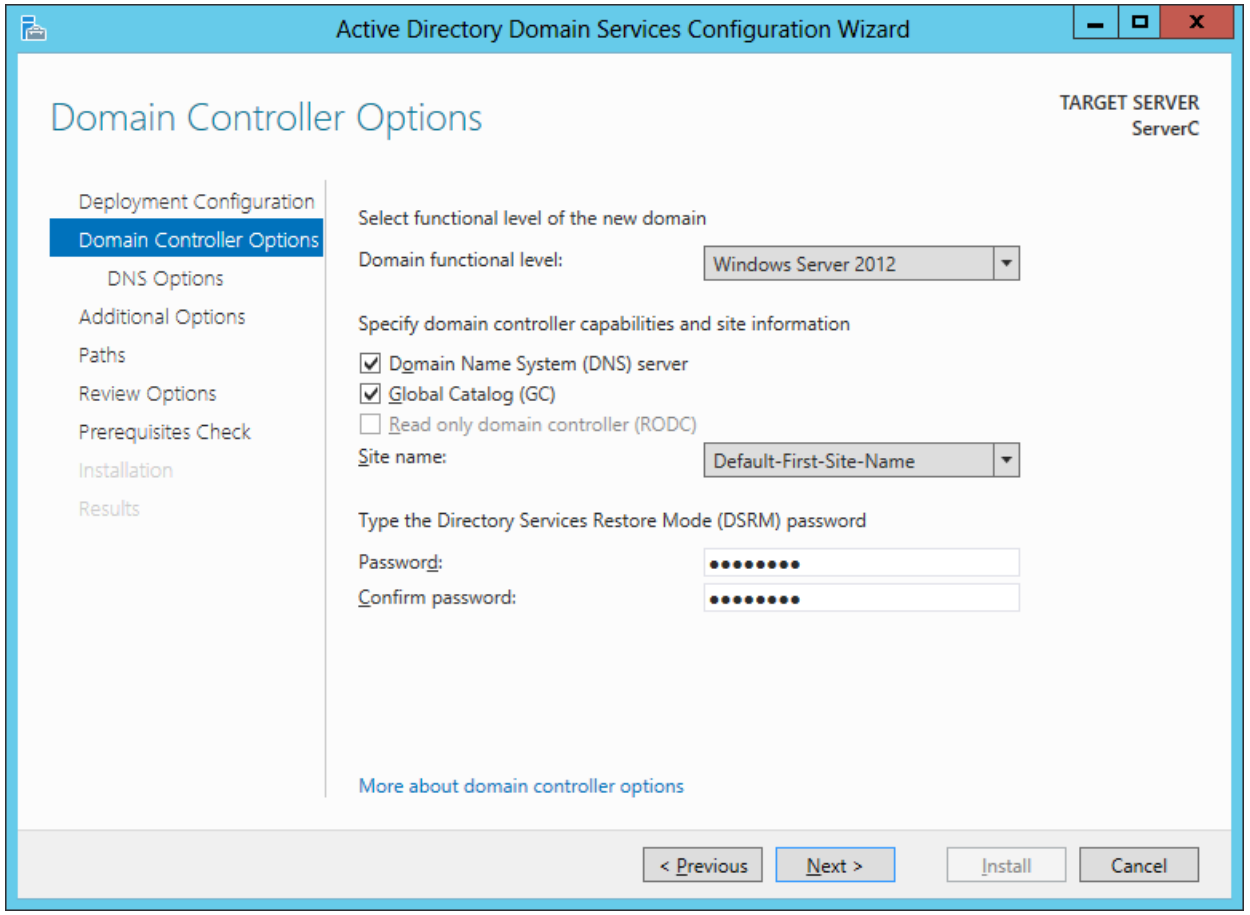
The Additional Options page of the Active Directory Domain Services Configuration Wizard

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 , 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
```

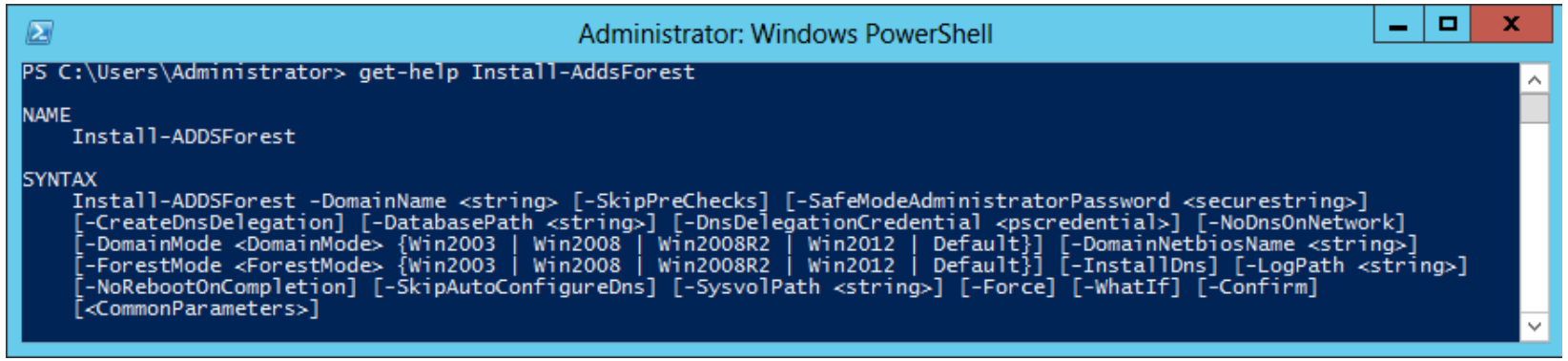
Installing AD DS on Server Core

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-AddsForest
- Install-AddsDomainController
- Install-AddsDomain

Installing AD DS on Server Core



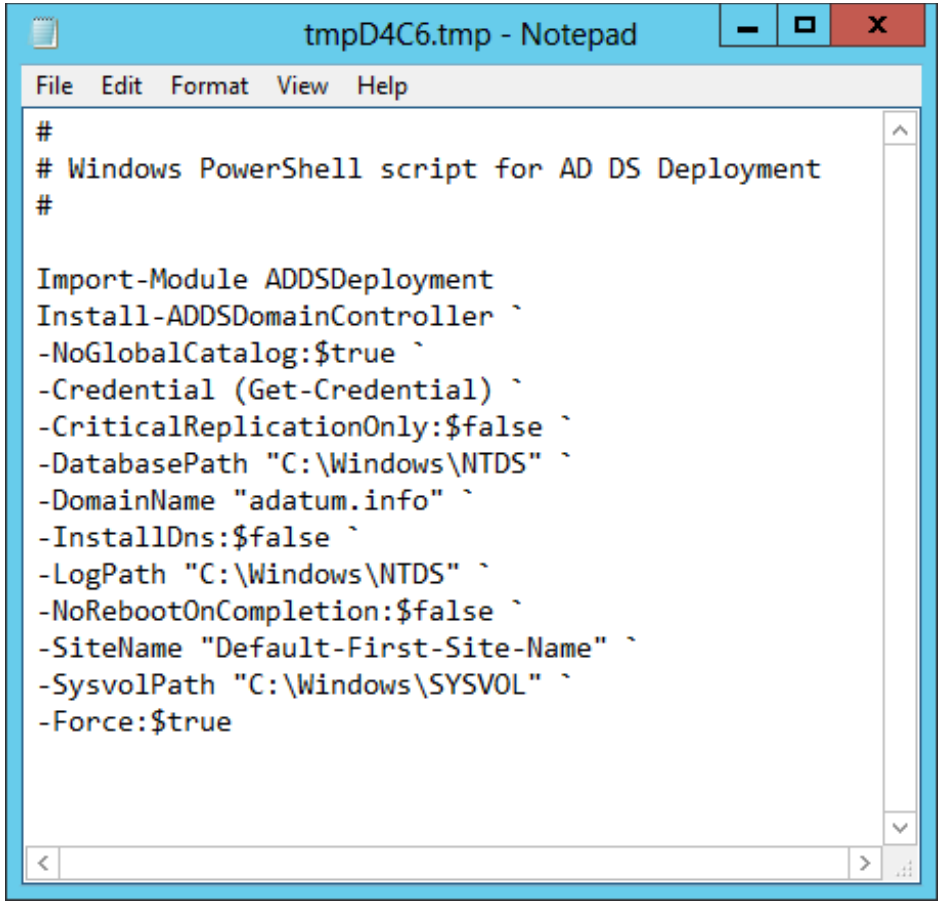
Syntax for the Install-AddsForest cmdlet in Windows PowerShell

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

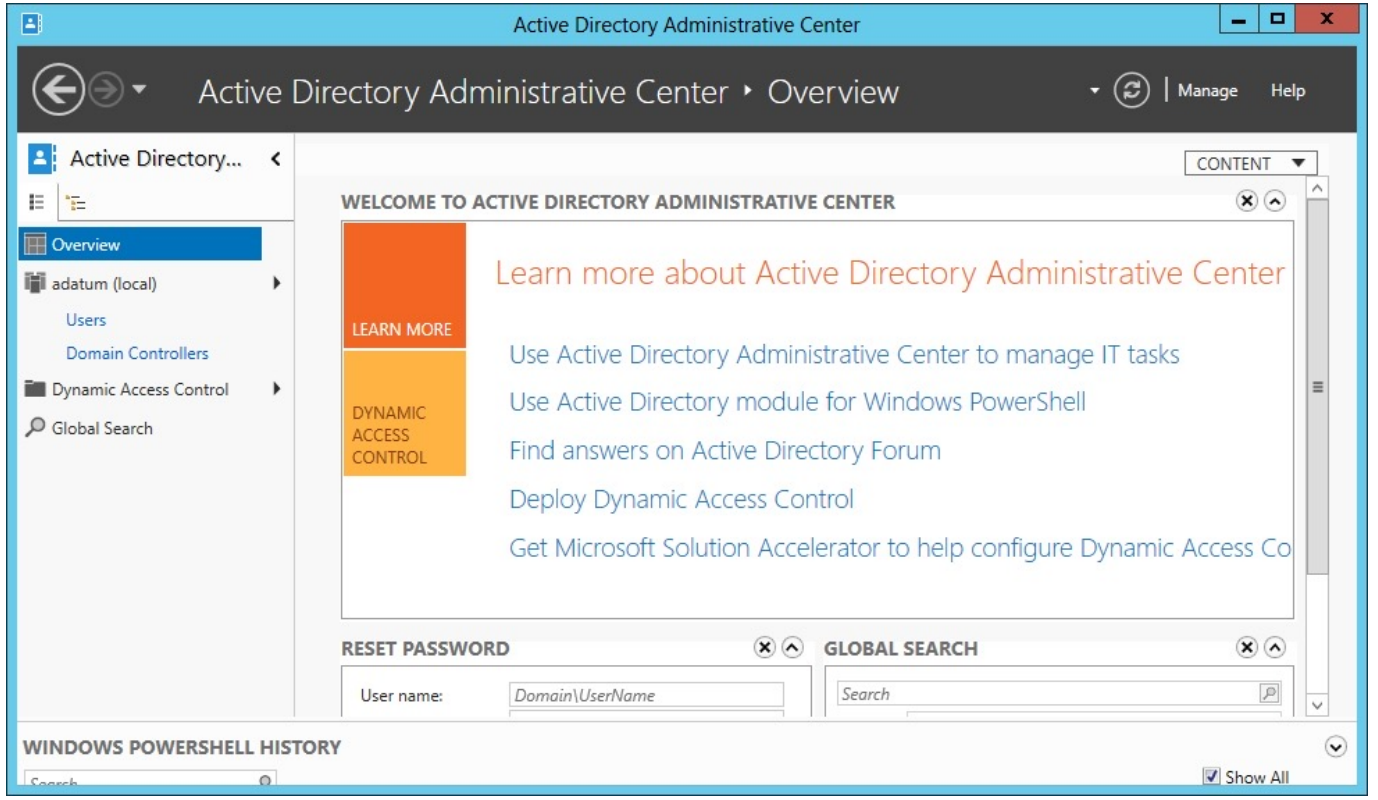
Creating User Objects

- The user account is the primary method for authentication on a network.
- Usernames and passwords are validated at log on by comparing entered information to the information stored in the AD DS database.

Types of Users

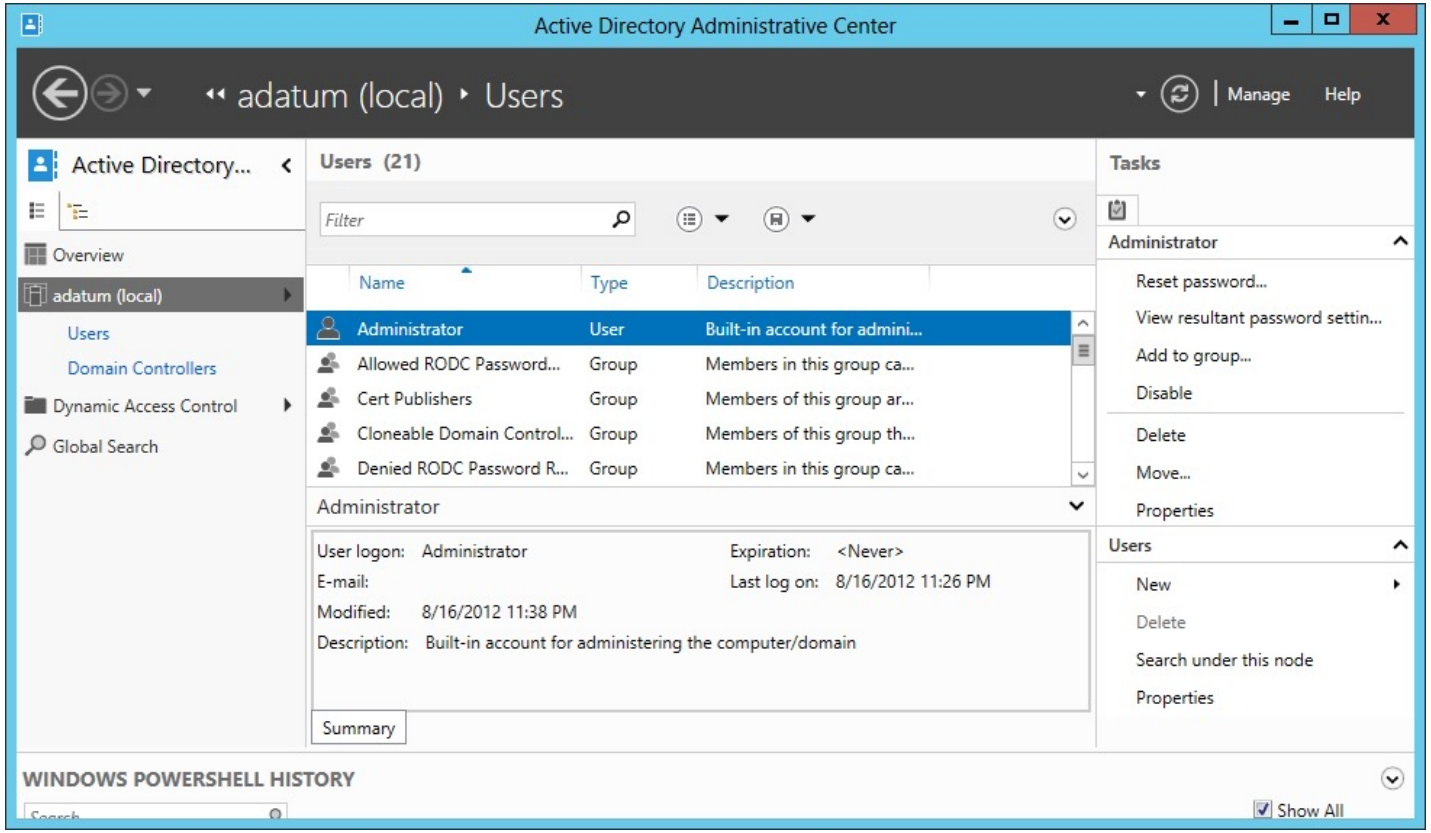
- **Local users:** These accounts can only access resources on the local computer and are stored in the local **Security Account Manager (SAM)** database on the computer where they reside.
- **Domain users:** These accounts can access AD DS or network-based resources, such as shared folders and printers.
  - Account information for these users is stored in the AD DS database and replicated to all domain controllers within the same domain.

Create a User with Active Directory Administrative Center



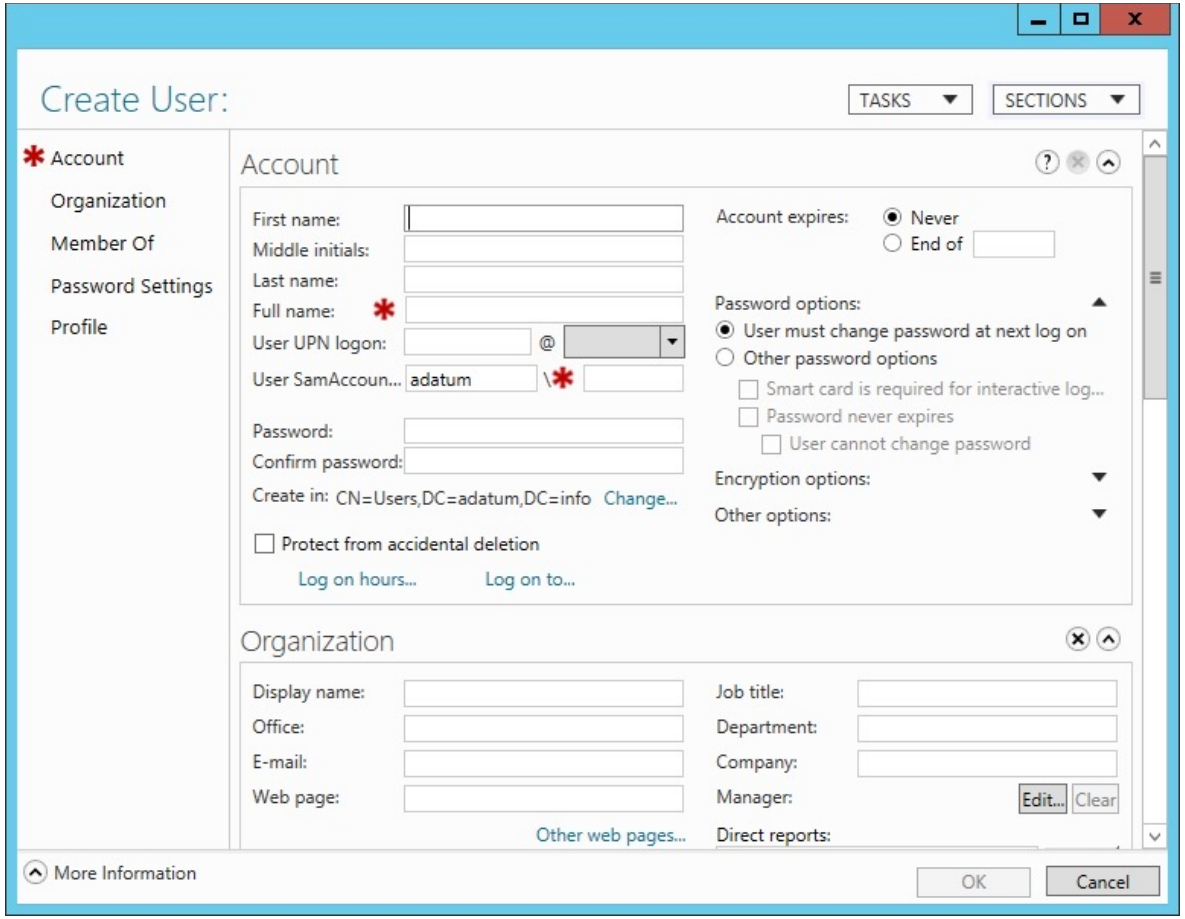
The Active Directory Administrative Center console

Create a User with Active Directory Administrative Center



A container in the Active Directory Administrative Center console

Create a User with Active Directory Administrative Center

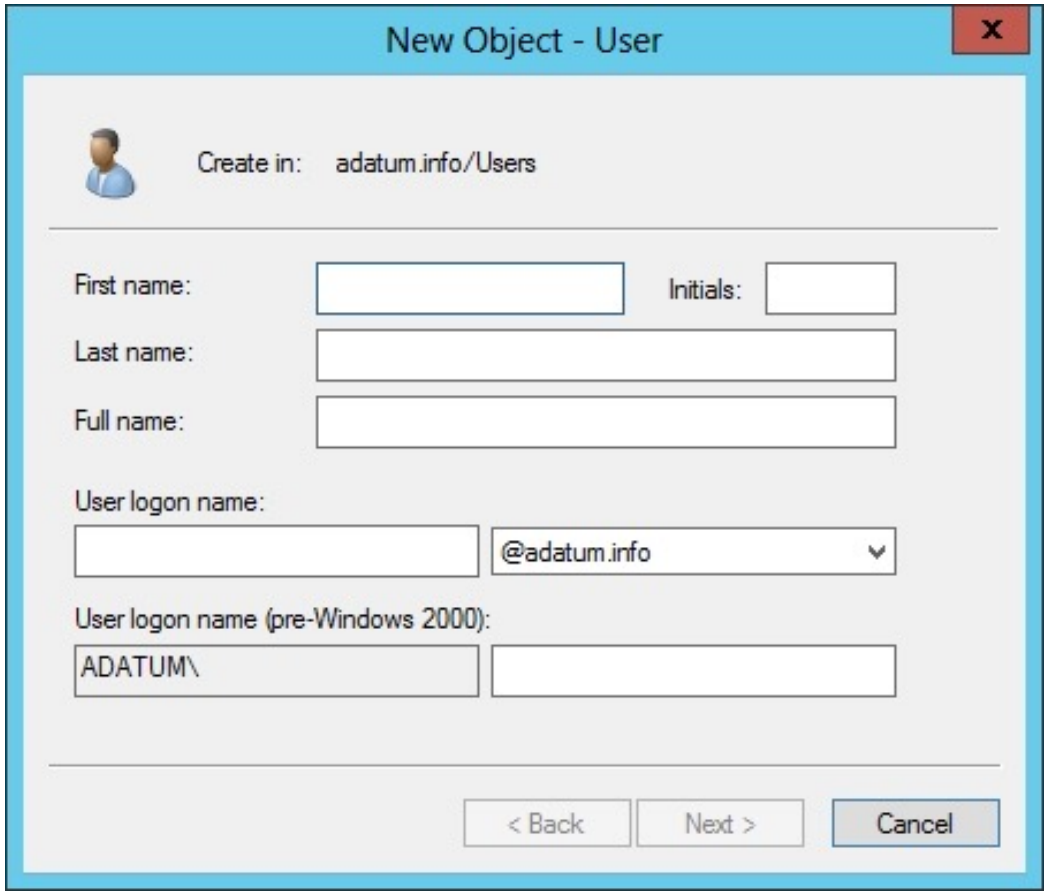


The Create User window in the Active Directory Administrative Center console

Create a User with Active Directory Users and Computers

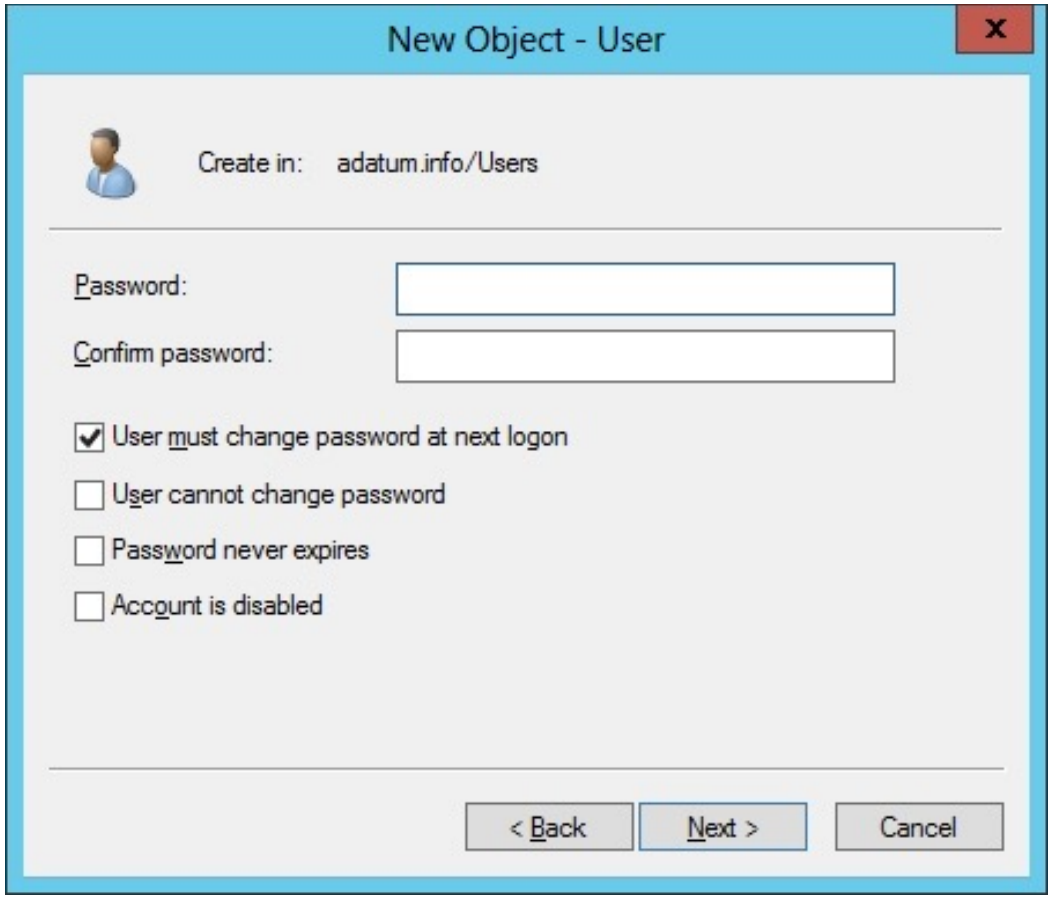
The Active Directory Users and Computers console

Create a User with Active Directory Users and Computers



The New Object - User Wizard

Create a User with Active Directory Users and Computers



The second page of the New Object - User Wizard

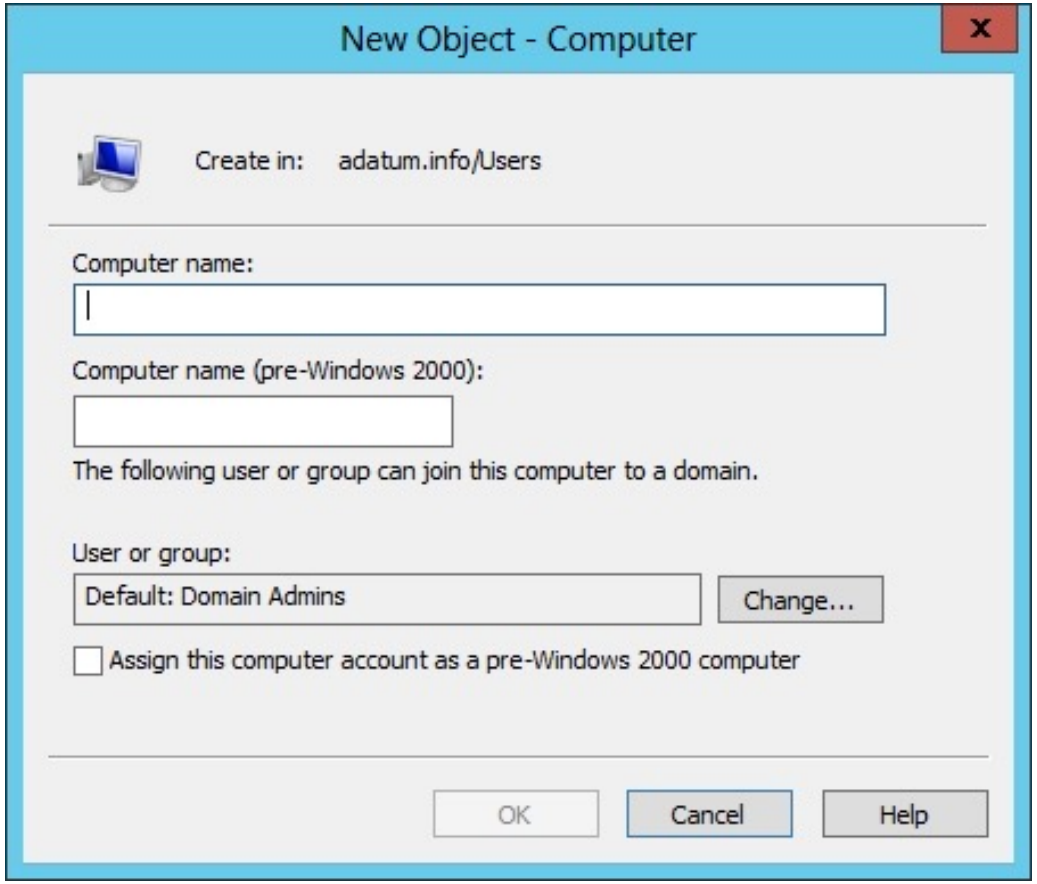
Using Windows PowerShell

Syntax of the New-ADUser cmdlet

Adding a Computer to a Domain

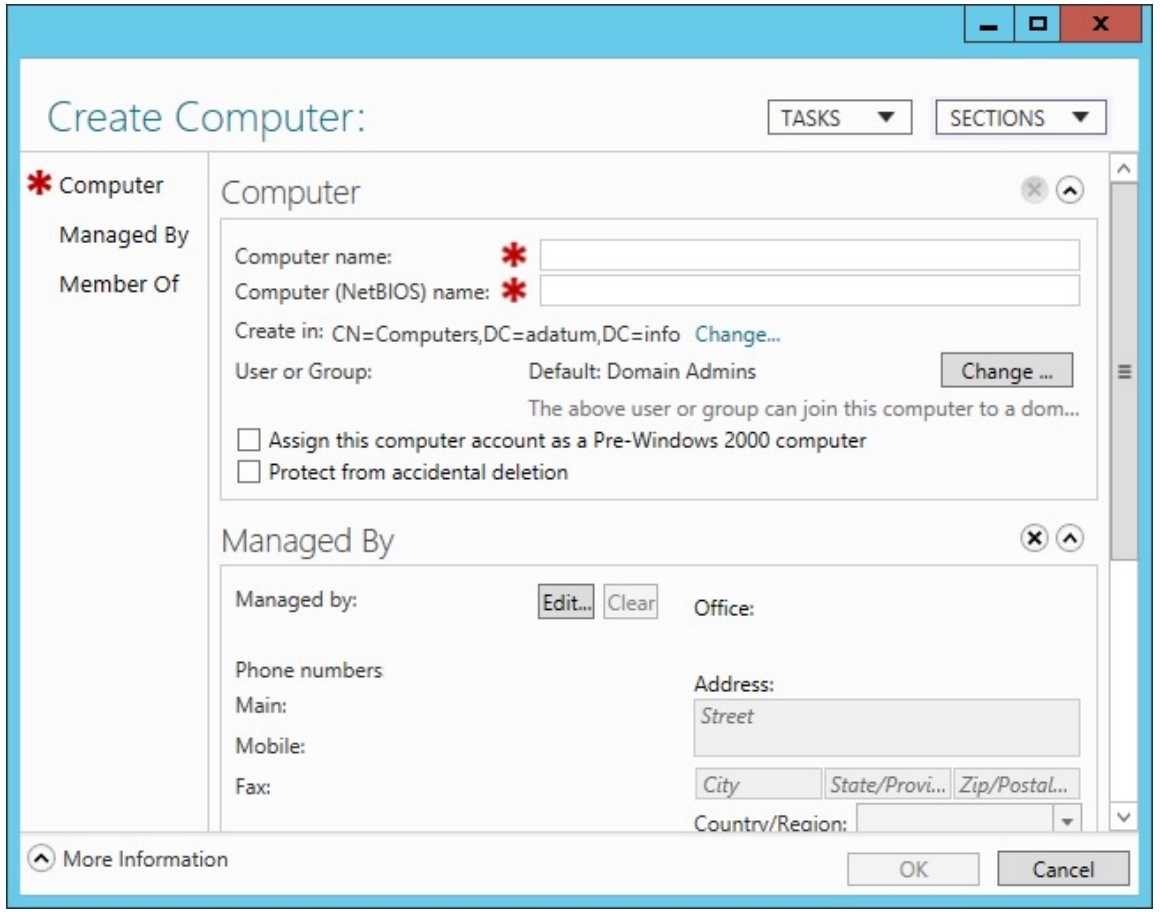
- **Creating a computer account:** Create a new computer object in Active Directory and assign the name of an actual computer on the network.
- **Joining the computer to the domain:** The system contacts a domain controller, establishes a trust relationship with the domain, locates (or creates) a computer object corresponding to the computer's name, alters its security identifier (SID) to match that of the computer object, and modifies its group memberships.

Creating Computer Objects Using Active Directory Users and Computers



The New Object – Computer wizard

Creating Computer Objects with Active Directory Administrative Center



The Create Computer dialog box

ISHIK UNIVERSITY
2008

Department of Information Technology

Lesson 4: Creating and Managing Active Directory Groups and Organizational Units

Server Management

Zina Yaaqub

Lesson 4: Creating and Managing Active Directory Groups and Organizational Units

MOAC 70-410: Installing and Configuring Windows Server 2012

Overview

- Create and Manage Active Directory Groups and Organizational Units (OUs)
- Designing an Internal Domain Structure
- Working with Organizational Units
- Working with Groups

Using Organizational Units

Reasons for creating an OU:

- **Duplicating organizational divisions**: The structure of OUs within your domains should be an extension of the model you used to design the Active Directory domain structure:
  - Geographical
  - Departmental
  - Political
- **Assigning Group Policy settings**: To assign different Group Policy settings to a particular collection of objects.
- **Delegating administration**: To grant certain individuals administrative responsibility for a portion of the Active Directory hierarchy, without giving them full access to the entire domain.

Using Group Objects

- Create a group when you want to grant a collection of users permission to access a network resource, such as a file system share or a printer.
- Groups are not part of the AD hierarchy.
- members of a group inherit any permissions that you assign to the group, but they do not inherit the Group Policy settings from the group's parent OUs and domain.

Working with Organizational Units

- OUs can be nested to create a design that enables administrators to take advantage of inheritance.
- Limit the number of OUs that are nested, because too many levels can:
  - Slow the response time to resource requests
  - Complicate the application of Group Policy settings

Working with Organizational Units

- There is only one built-in OU by default: the **Domain Controllers OU**.
- All other OUs must be created by the domain administrator.

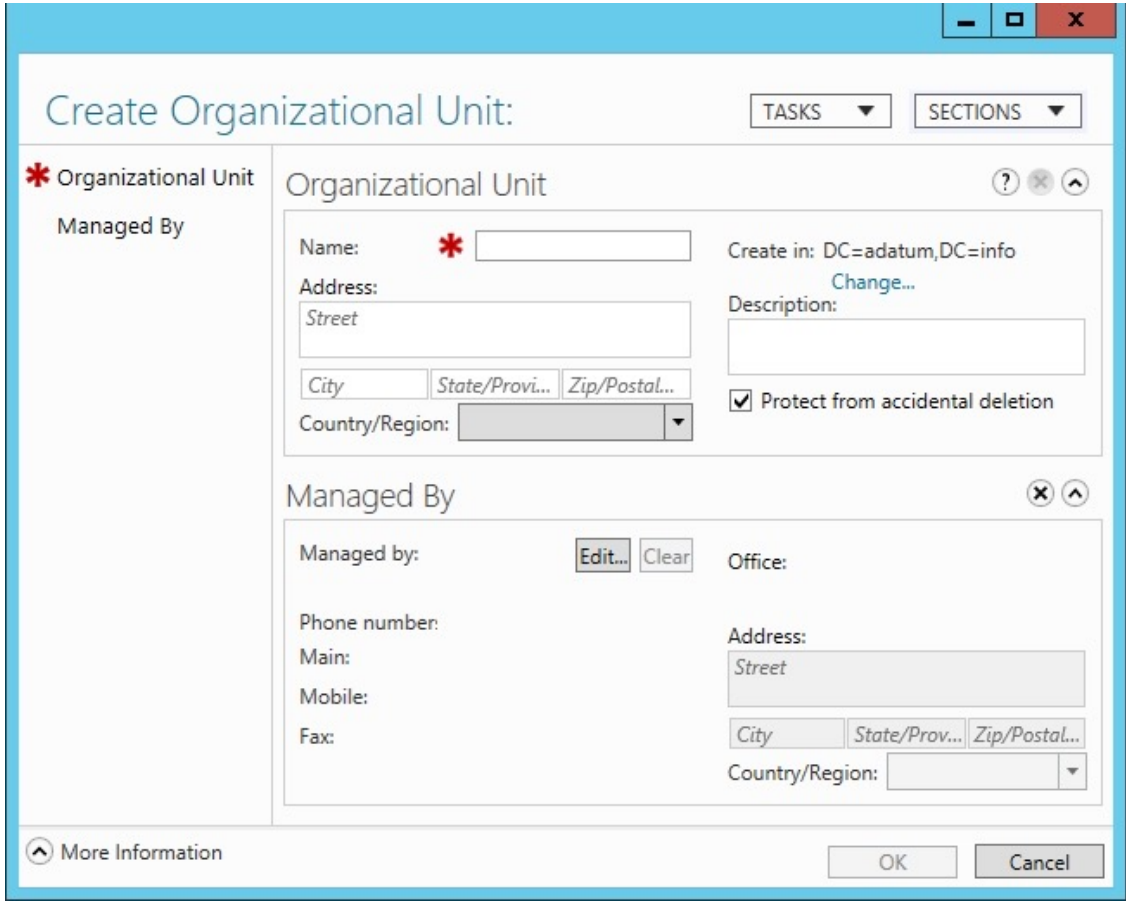
Containers

Default container objects:

- **Users:** Contains the domain's predefined users and groups.
- **Computer:** Contains computer objects in the domain.

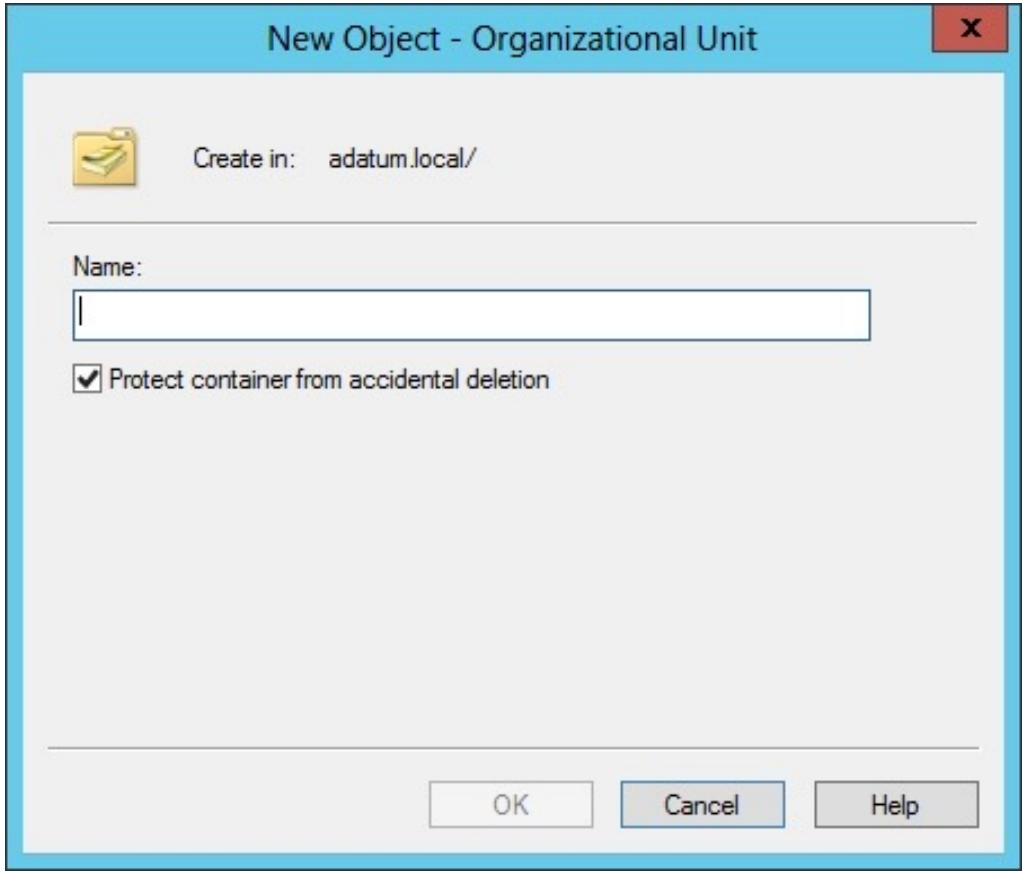
You cannot assign Group Policy settings to computer objects or delegate their administration.

Creating OUs



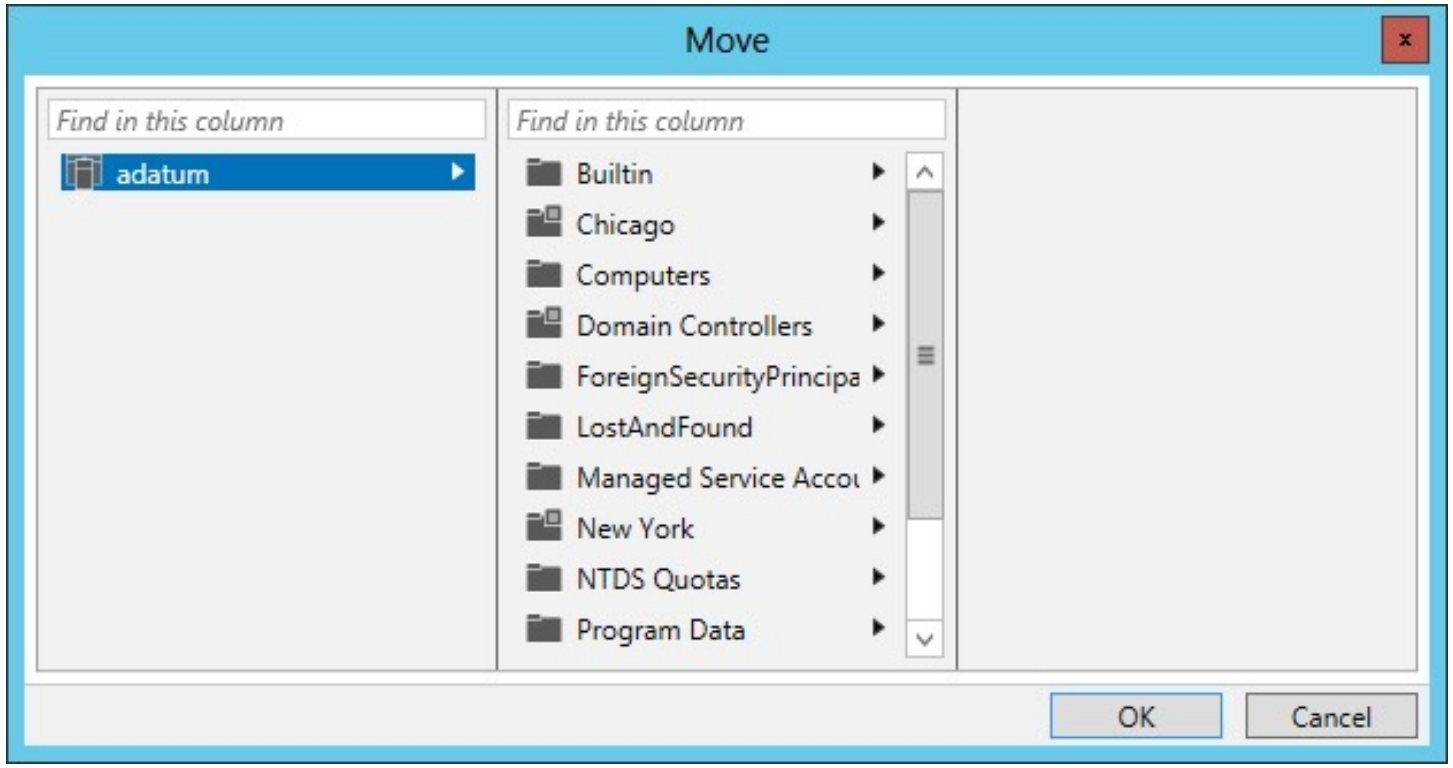
The Create Organizational Unit window in the Active Directory Administrative Center console

Creating OUs



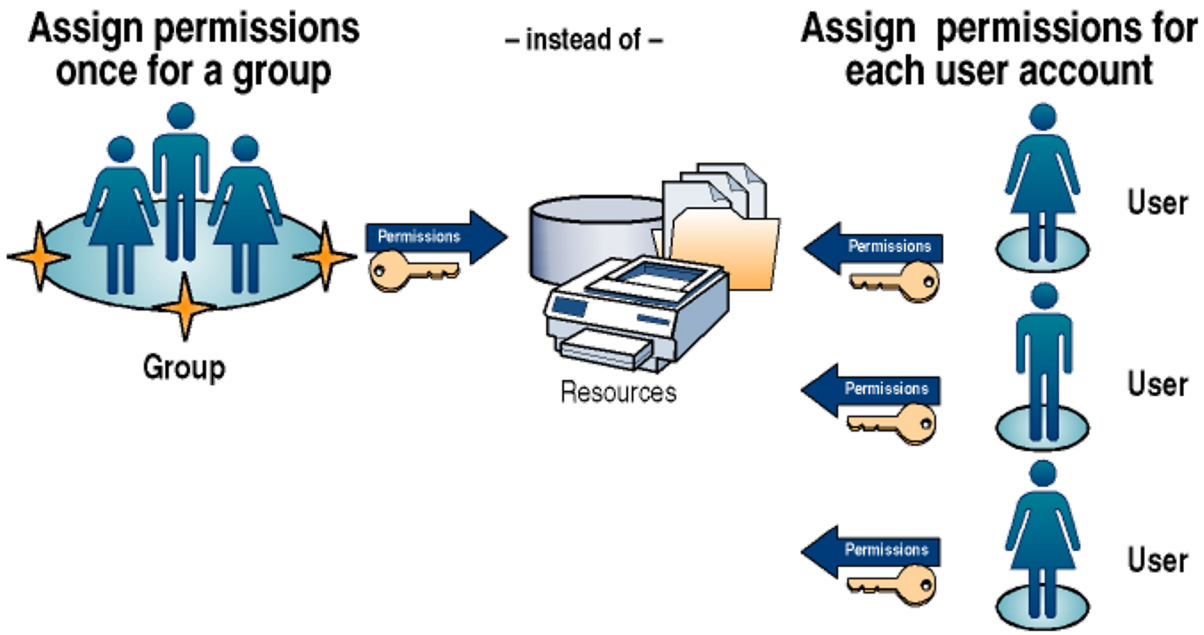
The New Object – Organizational Unit dialog box in the Active Directory Users and Computers console

Creating OUs



The Move dialog box in the Active Directory Administrative Center console

Working with Groups



- Groups are collections of user accounts.
- Members receive permissions given to groups.
- Users can be members of multiple groups.
- Groups can be members of other groups.

Group Types

There are two Windows Server 2012 group types:

- **Distribution groups:** Non-security-related groups created for the distribution of information to one or more persons.
- **Security groups:** Security-related groups created for purposes of granting resource access permissions to multiple users.

Group Scopes

- The **group scope** controls which objects the group can contain.
- Limits the objects to the same domain or permits objects from remote domains.
- Controls the location in the domain or forest where the group can be used.
- Group scopes available in an Active Directory domain include **domain local groups**, **global groups**, and **universal groups.**

Domain Local Groups

Domain local groups can have any of the following as members:

- User accounts
- Computer accounts
- Global groups from any domain in the forest
- Universal groups
- Domain local groups from the same domain

Global Groups

Global groups can have the following as members:

- User accounts
- Computer accounts
- Other global groups from the same domain

Universal Groups

Universal groups can contain the following members:

- User accounts
- Computer accounts
- Global groups from any domain in the forest
- Other universal groups

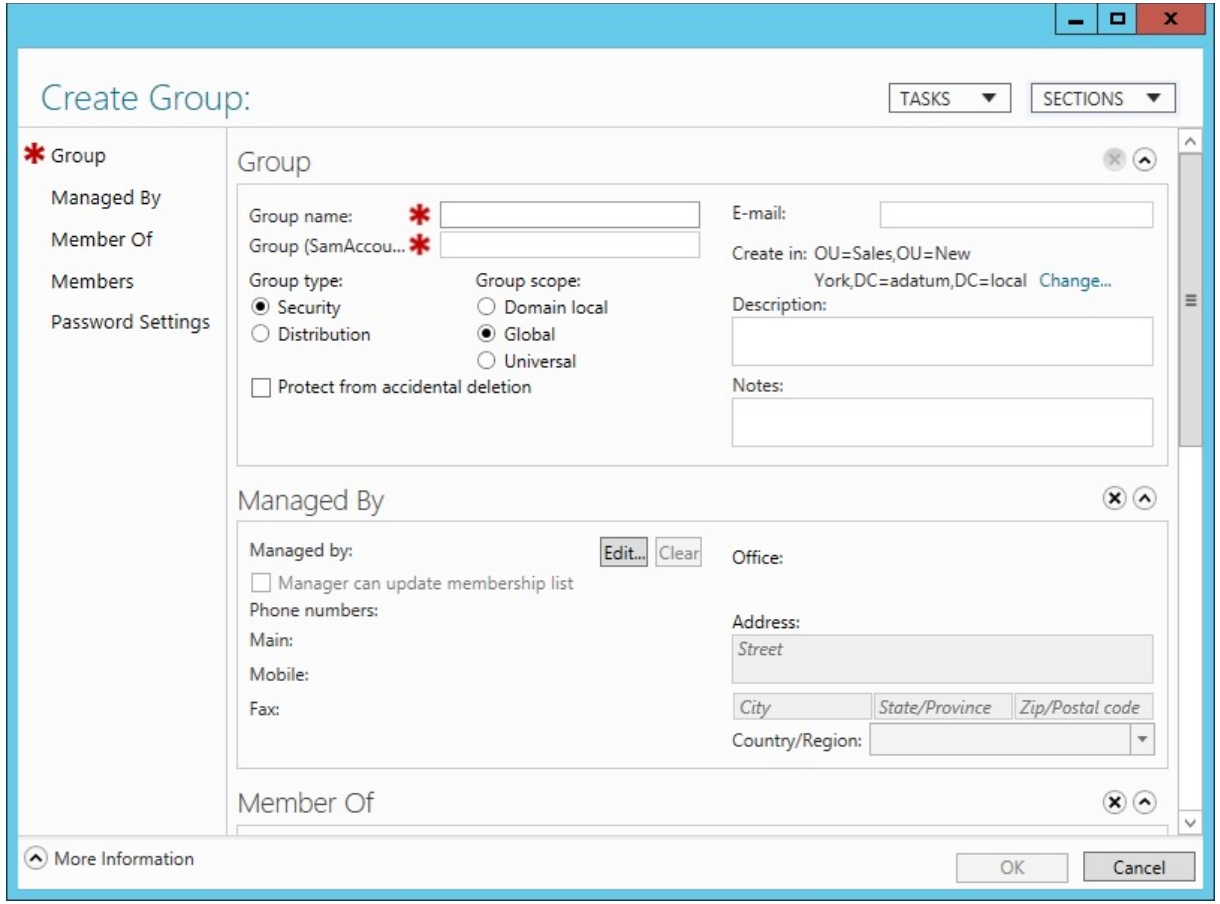
Nesting Groups

Group nesting is the term used when groups are added as members of other groups.

To allow users from multiple domains to access a resource in the parent domain:

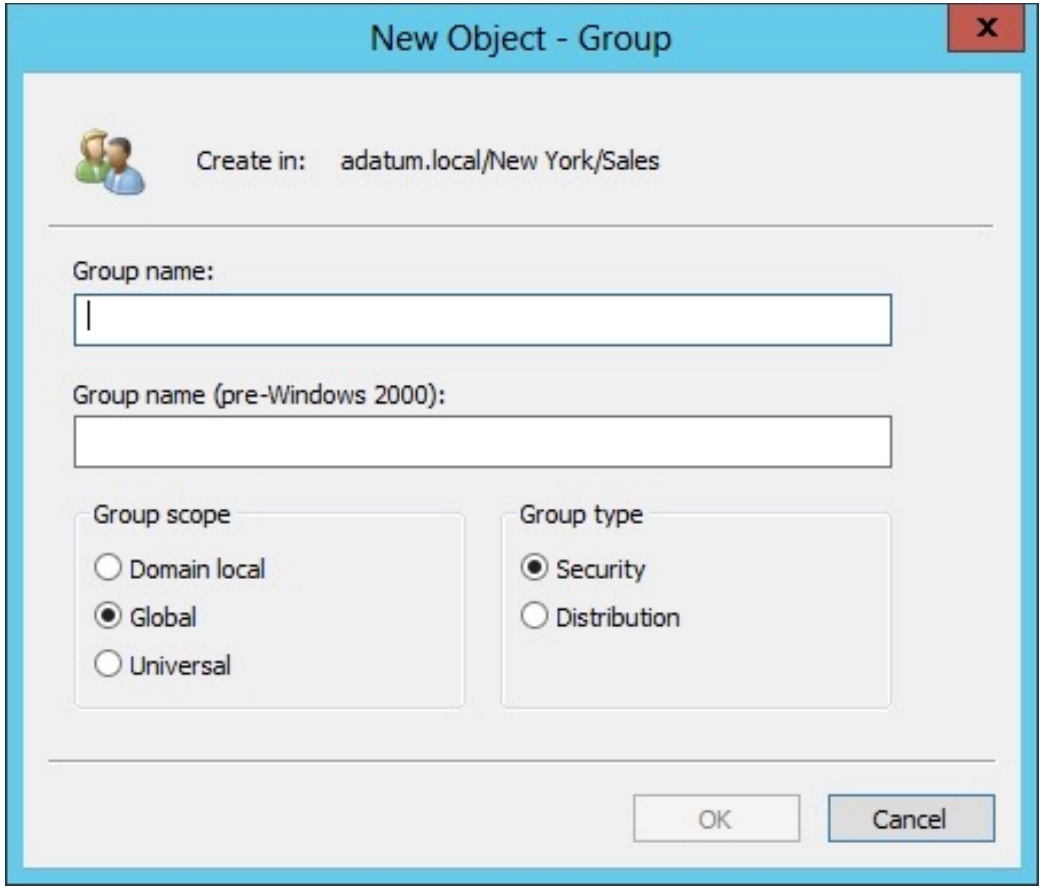
1. Create global groups in each domain that contain all users needing access to the enterprise database.
2. Create a universal group in the parent domain. Include each location's global group as a member.
3. Add the universal group to the required domain local group to assign the necessary permission to access and use the enterprise database.

Creating Groups



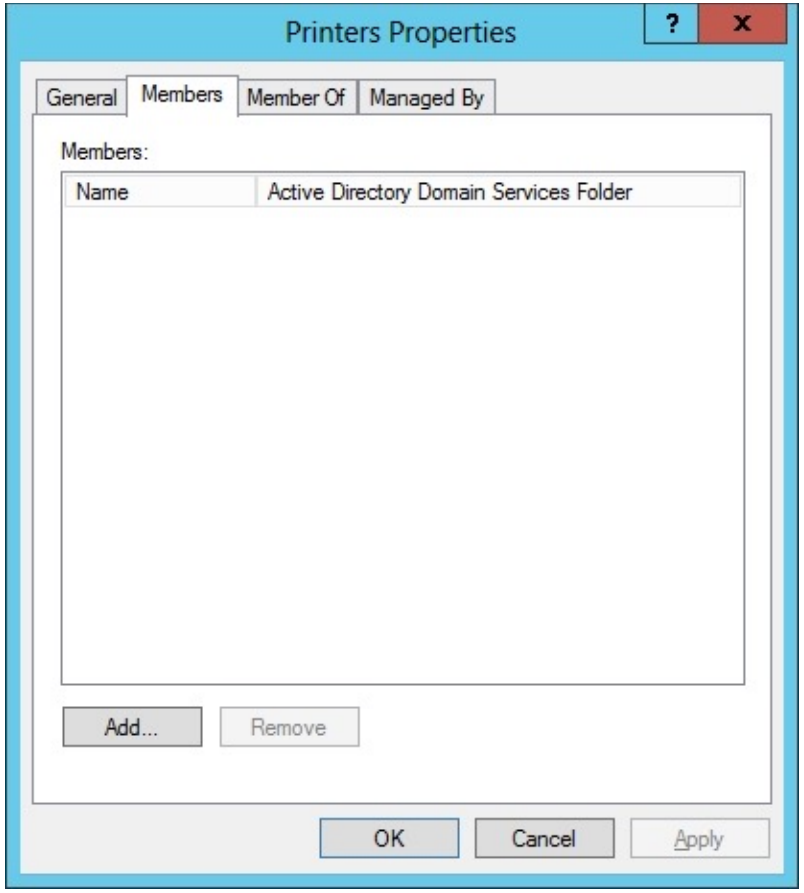
Creating a group in Active Directory Administrative Center

Creating Groups



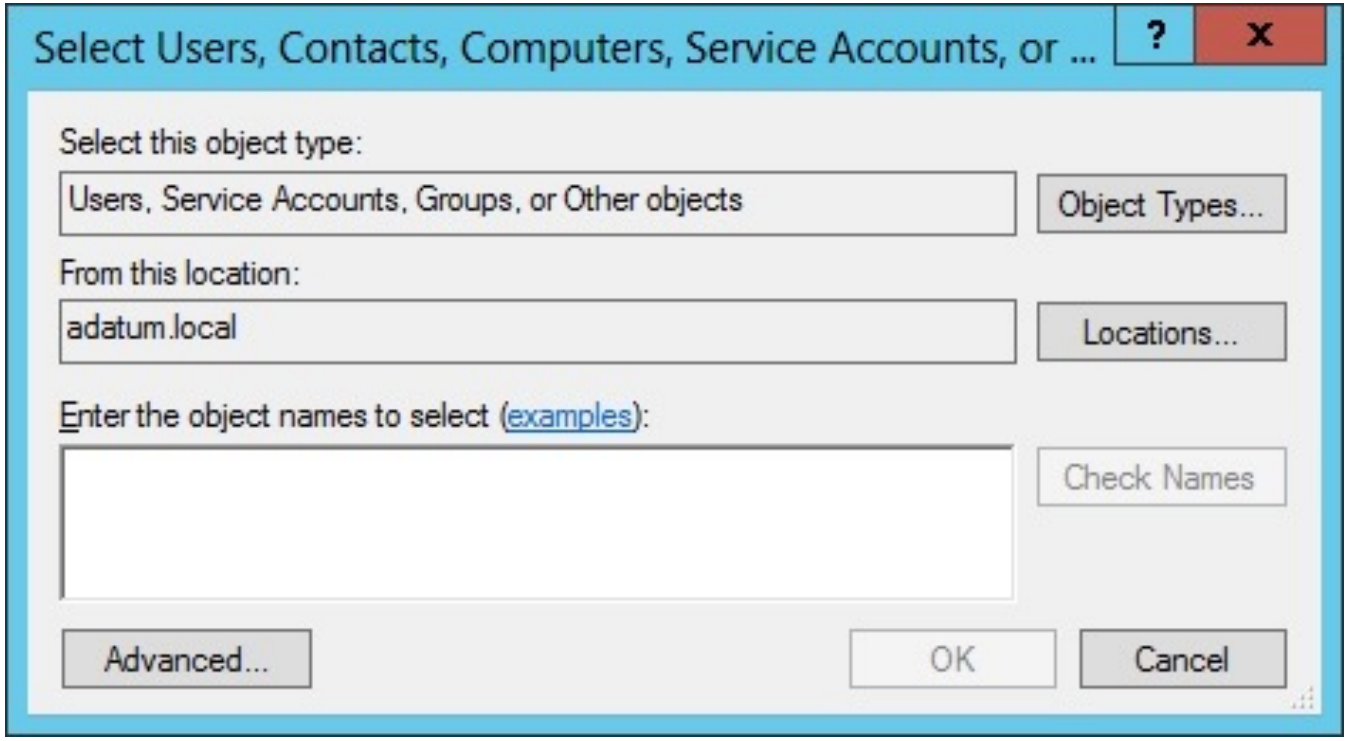
The New Object – Group dialog box

Managing Group Memberships



The Members tab of a group object's Properties sheet

Managing Group Memberships



The Select Users, Contacts, Computers, Service Accounts, or Groups dialog box

Questions

1. Compare the advantages and disadvantages of single-master replication versus multiple-master replication in a large enterprise.

2. In what situations would you choose a Read-Only Domain Controller (RODC) instead of a standard domain controller?

3. Analyze the risks of giving too many users Domain Admin privileges instead of delegating control through OUs.
4. How does hardware performance (CPU, RAM, storage) impact Active Directory efficiency?
5. What could happen if the Global Catalog server becomes unavailable in a forest?
6. Design a basic AD structure (domains, OUs, groups) for a company with three departments and two branch offices. Explain your reasoning.
7. A company has multiple branches connected by WAN links. What factors should be considered when deploying AD DS to ensure good performance?
8. Explain the difference between logical components and physical components in Active Directory.
9. Why is replication important in a domain environment?
10. What is the main function of a domain controller?What is the difference between a local user and a domain user?
11. Why are universal groups recommended when assigning permissions across multiple domains?