LONDON METROPOLITAN UNIVERSITY

Islington college
(इस्लिङ्टन कलेज)

Module Code & Module Title

Level 5 – Operating Systems

Assessment Type

Logbook 6

Semester

2025/26 Spring/Autumn

Student Name: Prabin Pradhan

London Met ID: 24046428

College ID: NP01NT4A240115

Assignment Due Date: Monday, December 1, 2025

Assignment Submission Date: Tuesday, December 2, 2025

Submitted To: Sarika Dahal

Word Count (Where Required): 2048

I confirm that I understand my coursework needs to be submitted online via Google Classroom under the relevant module page before the deadline in order for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a mark of zero will be awarded.

Table of Contents

Table of Figures

1 Introduction:

1.1 Active Directory:

Microsoft Active Directory is a proprietary directory service that gives administrators control over network resource permissions within Windows domain networks. Active Directory was first available in the Windows 2000 operating system but has expanded into a complete structure for the centralized management of various network elements such as users and computers, along with groups and other organizational resources. Active Directory functions as the core authentication and authorization system for Windows domain delivery environments through its organized hierarchical management system of network resources (Simiter, 2025).

To simplify and understand the concept of AD better, consider Active Directory as the “Contacts” application on your mobile phone (Simiter, 2025). The Contacts app itself acts as an Active Directory, while individual contacts in the app would be its “objects”. (Simiter, 2025) The values stored in each object, such as phone number, address, email, etc., would be your Active Directory (Simiter, 2025). The only difference is that objects like in the mobile app aren’t just limited to people, but AD may also contain group objects such as printers, computers, devices, etc (Simiter, 2025).

Key Features of Active Directory Domain Services

- **Lightweight Directory Services**: AD LDS is a Lightweight Directory Access Protocol (LDAP) directory service (Simiter, 2025). It provides only a subset of the AD DS features, making it more versatile in where it can be run (Simiter, 2025). For example, it can be run as a stand-alone directory service without needing to be integrated with a full implementation of Active Directory (Simiter, 2025).
- **Certificate Services**: You can create, manage, and share encryption certificates, which allow users to exchange information securely over the internet (Simiter, 2025).

- **Active Directory Federation Services**: ADFS is a Single Sign-On (SSO) solution for AD that allows employees to access multiple applications with a single set of credentials, thus simplifying the user experience (Simiter, 2025).
- **Rights Management Services**: AD RMS is a set of tools that assist with the management of security technologies that will help organizations keep their data secure (Simiter, 2025). Such technologies include encryption, certificates, and authentication, and cover a range of applications and content types, such as emails and Word documents (Simiter, 2025).

1.2 Domain Controller:

A domain controller is a server that processes authentication requests from users and computers within a computer domain (Simiter, 2025). Domain controllers are most commonly used in Windows Active Directory (AD) domains, but are also used with other types of identity management systems (Simiter, 2025).

Domain controllers restrict access to domain resources by authenticating user identity through login credentials and preventing unauthorized access to those resources (Simiter, 2025). Domain controllers apply security policies to requests for access to domain resources. For example, in a windows AD domain, the domain controller draws authentication information for user accounts from AD (Simiter, 2025).

A domain controller can operate as a single system, but is usually implemented in clusters for improved reliability and availability (Simiter, 2025). For domain controllers running under Windows AD, each cluster comprises a primary domain controller and one or more backup domain controllers (Simiter, 2025).

Insecure sites can use a read-only domain controller to speed up authentication (Simiter, 2025). In Unix and Linux environments, domain controllers can manage Lightweight Directory Access Protocol domains (Simiter, 2025).

1.3 Forest:

A forest is the highest level of organization within Active Directory and is used to group one or multiple domains together (cayosoft, 2022). An Active Directory forest simply refers to all domains within a single AD installation and represents the security boundary of Active Directory (cayosoft, 2022). Forests allow administrators to assign broad policies, while trees and individual domains allow for more granularity in access and security (cayosoft, 2022).

Enterprise networks can hold hundreds of users and individual trees, which can have one or more domains or subdomains starting from the first setup domain, called the root domain (cayosoft, 2022). All together, these trees are organized into a forest, establishing a security boundary for network objects (cayosoft, 2022). It contains all the users, domains, devices, policies, and network objects in the hierarchy underneath (cayosoft, 2022).

1.4 Workshop Task:

On this going workshop task is to Set up the Windows Server 2022 Active Directory Domain Services Role. Create a new forest and domain to elevate the server to the position of Domain Controller. Use PowerShell commands to confirm the Domain Controller configuration and make sure all services are operating as intended.

2 Aim and Objectives:

- The Aim is to set up a centralized domain controller for network resource management by installing and configuring Active Directory Domain Services (AD DS) on Windows Server 2022.

The main objectives of this workshop:

- Install a domain controller to verify computer identity across the network.
- Set up a fresh Active Directory domain and forest.
- Confirm that AD DS services have been successfully deployed.
- Allow for the central administration of user accounts, permissions, and network resources.
- Set and understand the purpose of the Directory Services Restore Mode (DSRM) password.
- Verify the health and status of AD DS, DNS, KDC, and Netlogon services using PowerShell.

3 Customization:

Customization is the process of making alterations to a product or service to meet the specific needs or desires of an individual or a group (storyly.com, 2025). It is a way to personalize an experience or item to align with the unique preferences, tastes, or requirements of a customer (storyly.com, 2025).

Install Active Directory Domain Services:

Step 1: Initial Server Access:

Open the Server Manager program after logging in with administrator credentials to Windows Server 2022. This serves as the main hub for controlling server features and roles. To continue with the installation, you need to have administrative rights.

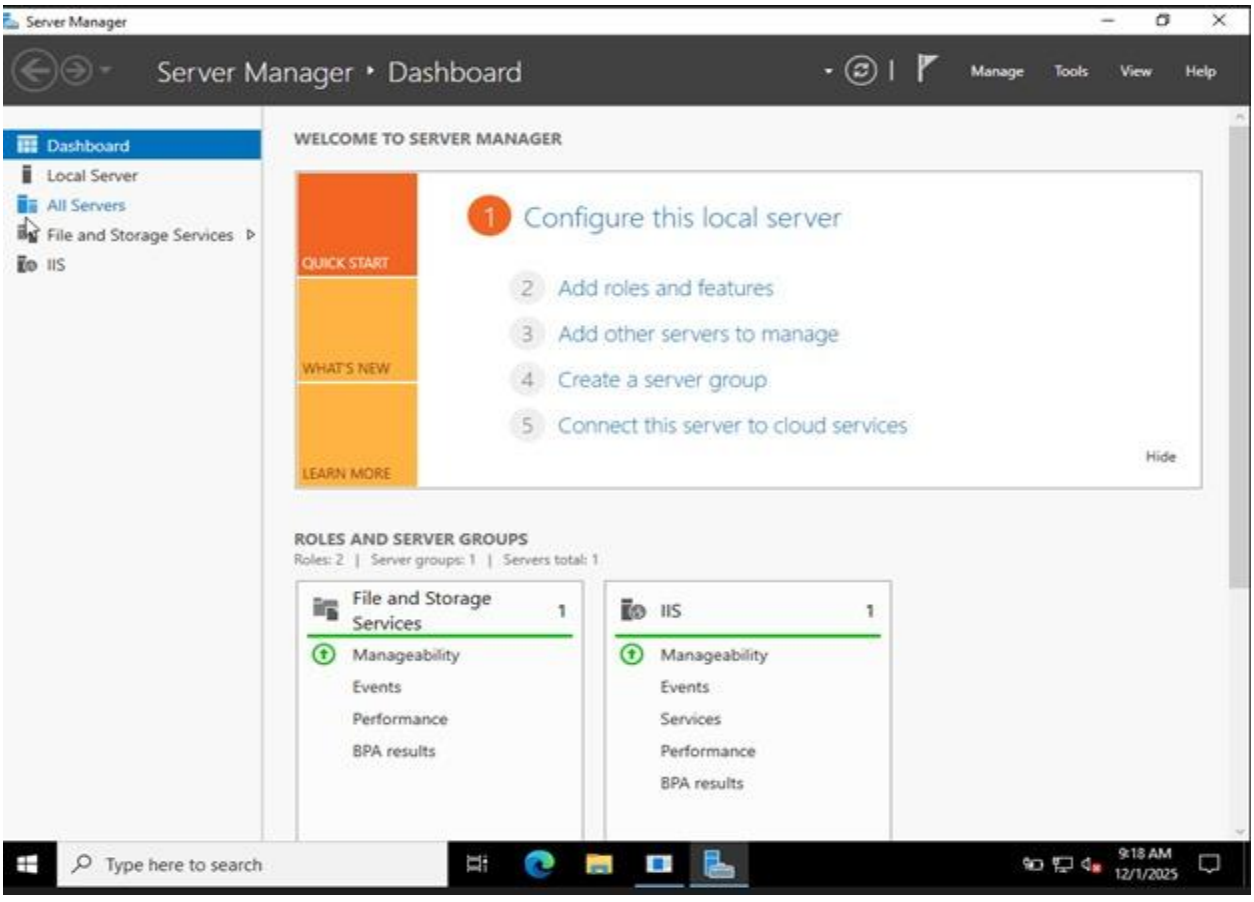

Figure 1: Initial Server Access

Step 2: Access Add Roles and Features:

To start the wizard, select "Add Roles and Features" from the Server Manager dashboard. A guided interface for installing server roles and features is offered by this wizard. A number of configuration pages will appear when the wizard opens.

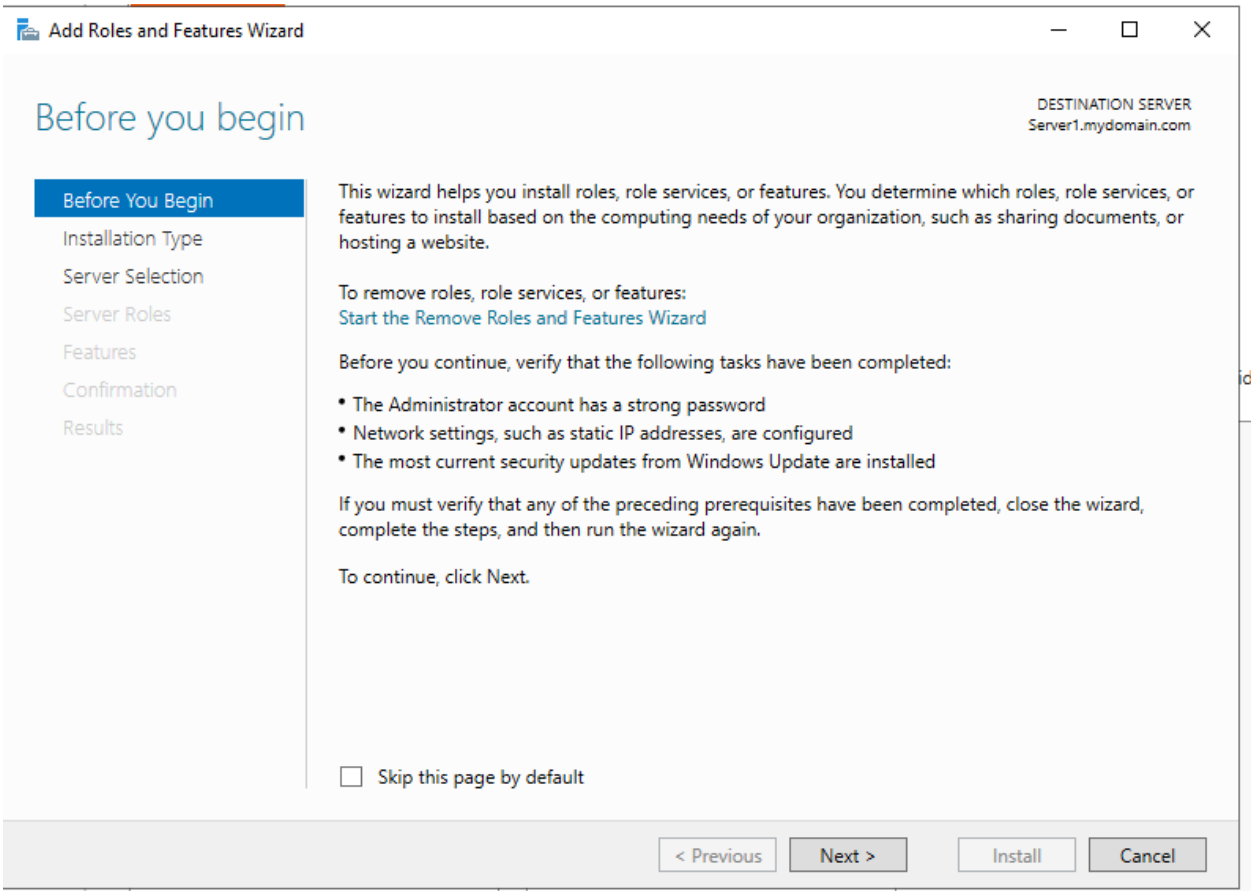

Figure 2: Add Roles and Features

Step 3: Select Installation Type:

To move on to the installation type selection screen, click the "Next" button. Depending on how your server is configured, you will see options for various installation types. The installation's course is decided by this step.

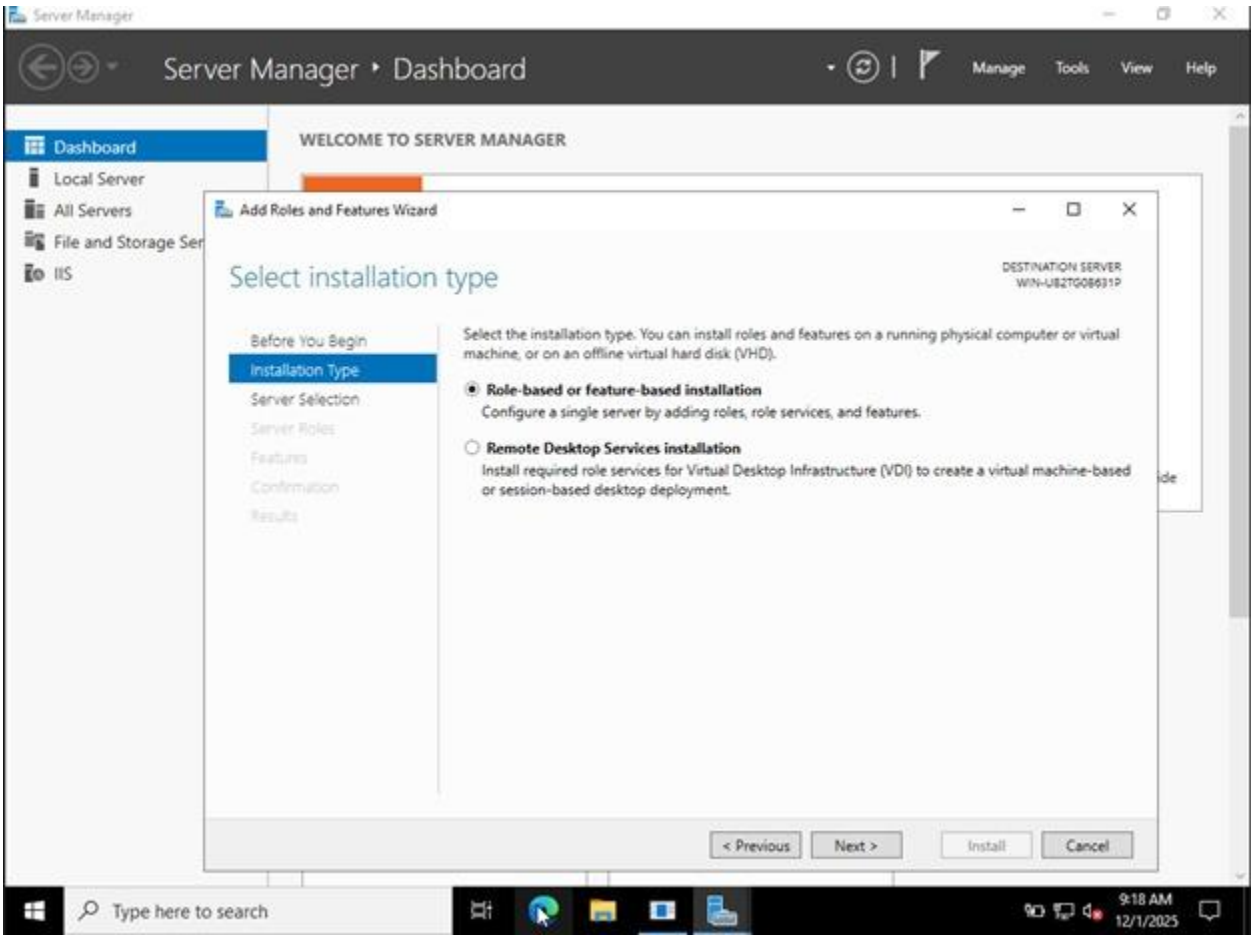

Figure 3: Select Installation Type

Step 4: Choose Add Roles and Features Wizard:

Click "Next" to proceed to the server selection after choosing the "Add Roles and Features" Wizard option. After that, you will be asked to select a destination server. Choose a server from the pool of available servers.

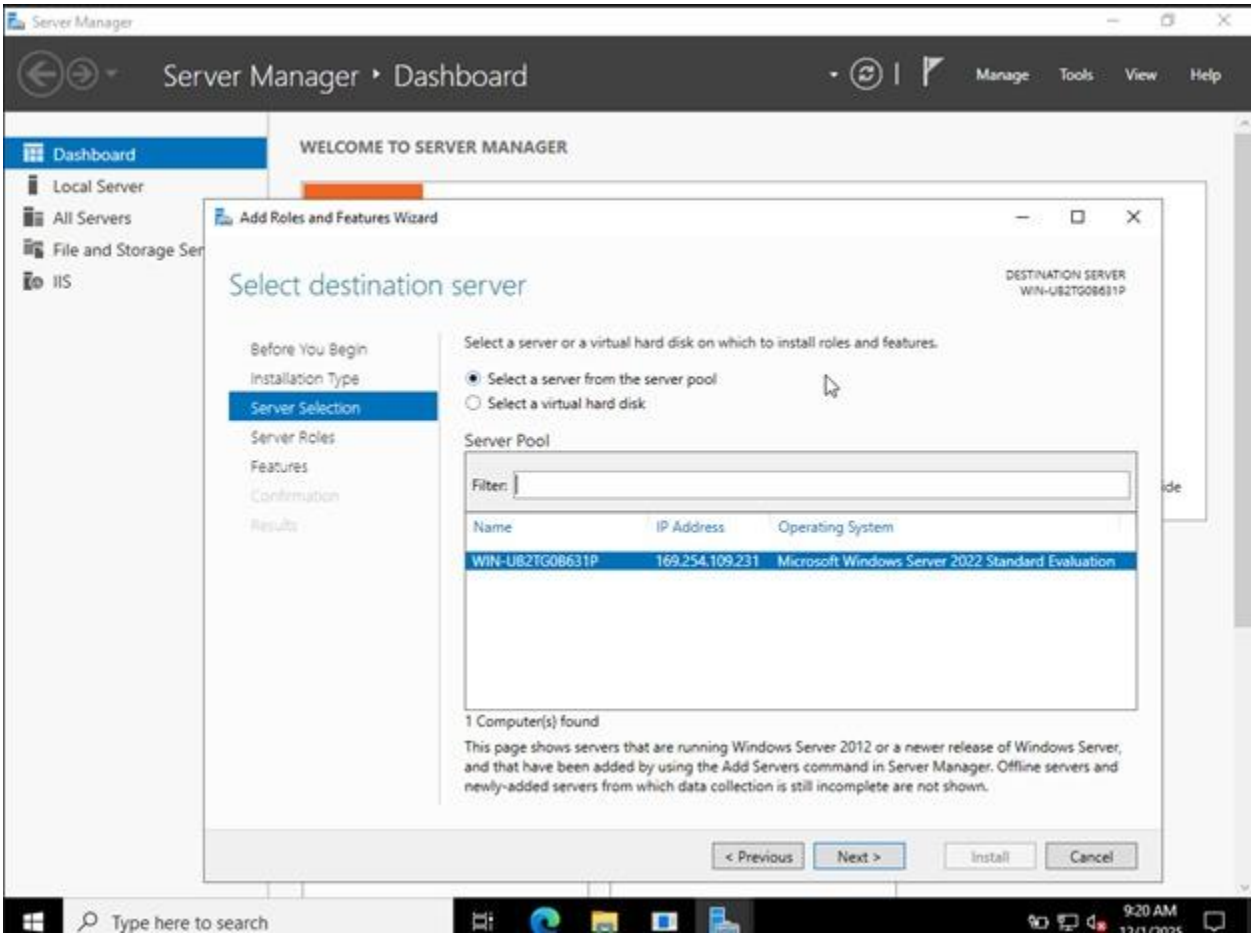

Figure 4: Choose Add Roles and Features Wizard

Step 5: Select Server from Pool:

Click "Next" after selecting "Select a server from the server pool" to move on to the role selection process. Your network's available servers will be shown for you to choose from. This guarantees that the role is set up on the appropriate server.

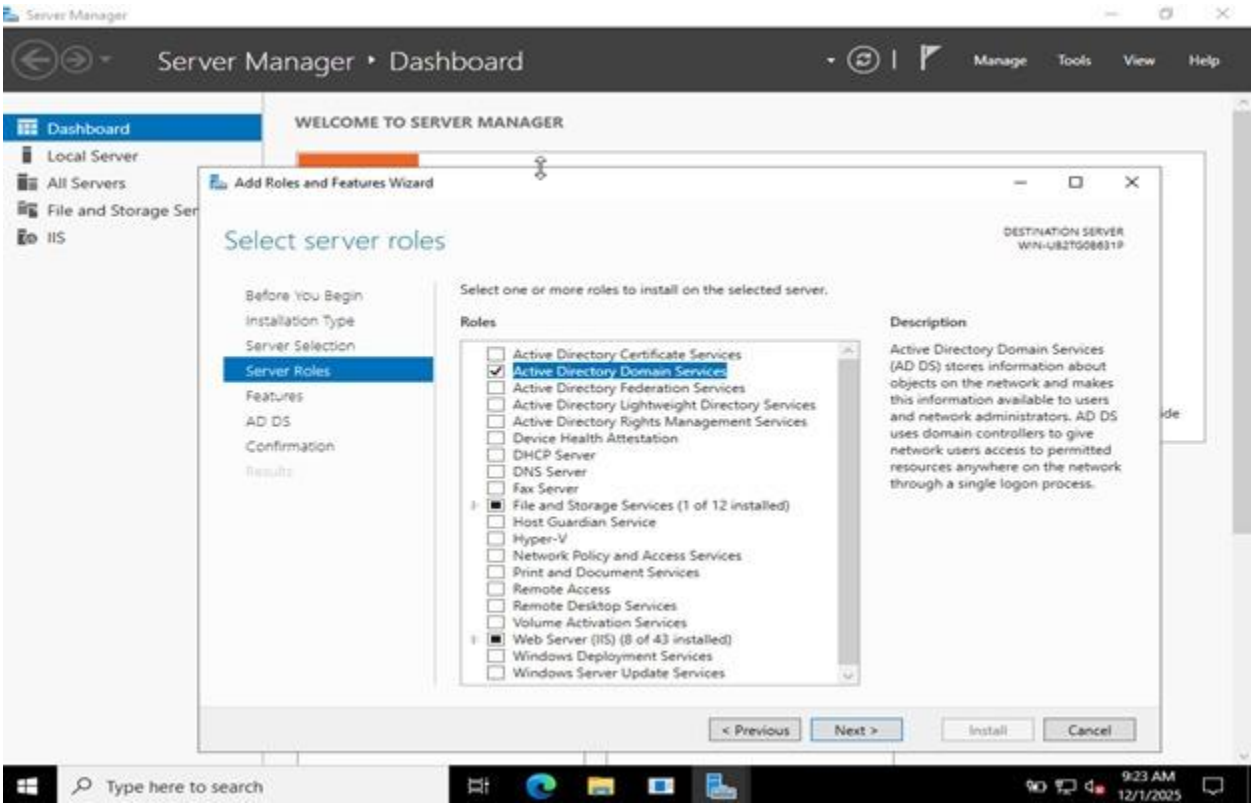

Figure 5: Select Server from Pool

Step 6: Select Active Directory Domain Services Role:

Choose "Active Directory Domain Services" as the necessary role from the list of server roles. This is the core component needed to establish a domain controller. Click "Next" to continue to the features selection page.

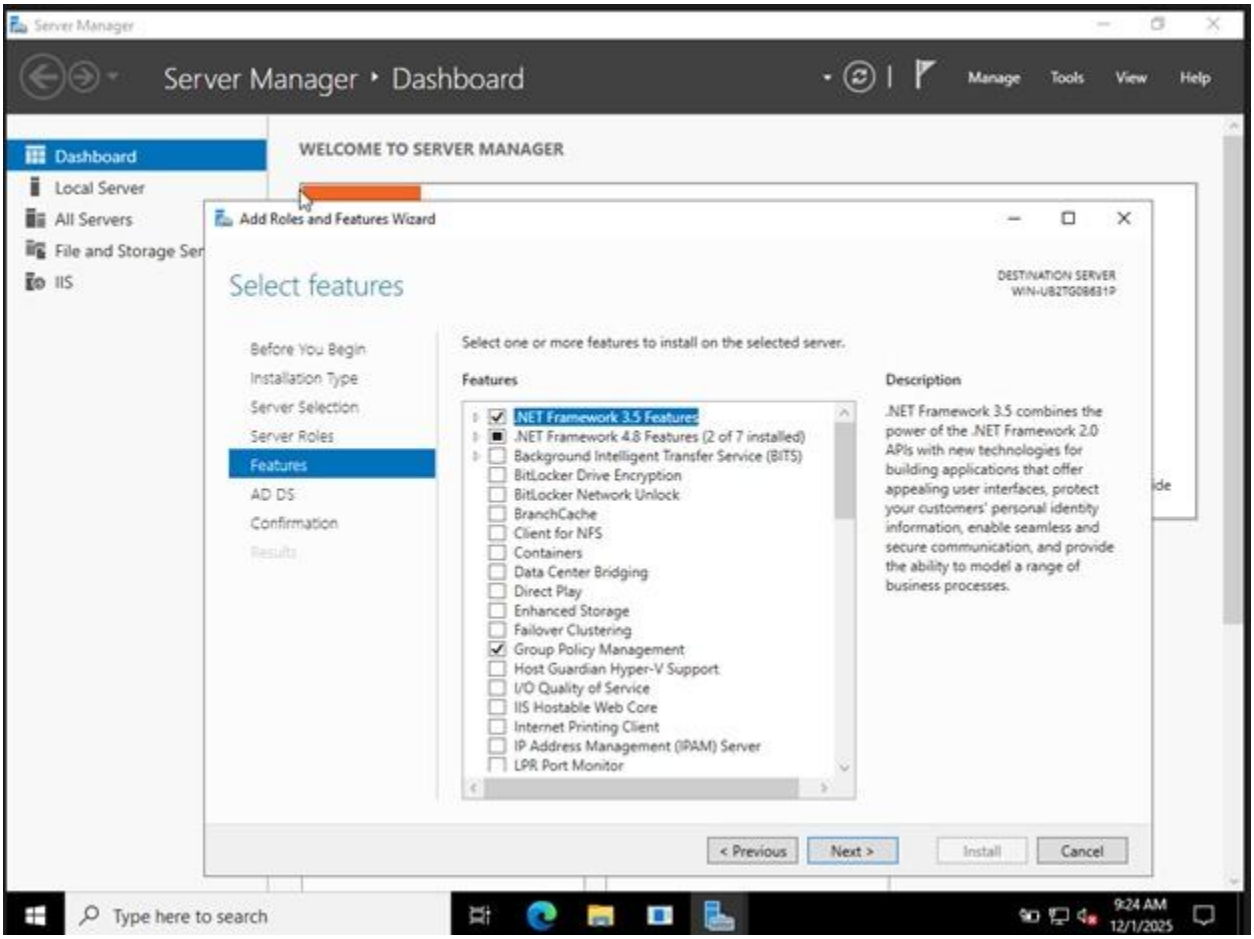

Figure 6: Select Active Directory Domain Services Role

Step 7: Confirm Default Features:

Leave all default feature settings as they are and click "Next" to proceed. The required dependencies and supporting features will be automatically chosen by the wizard. You will then see a confirmation page summarizing your installation choices.

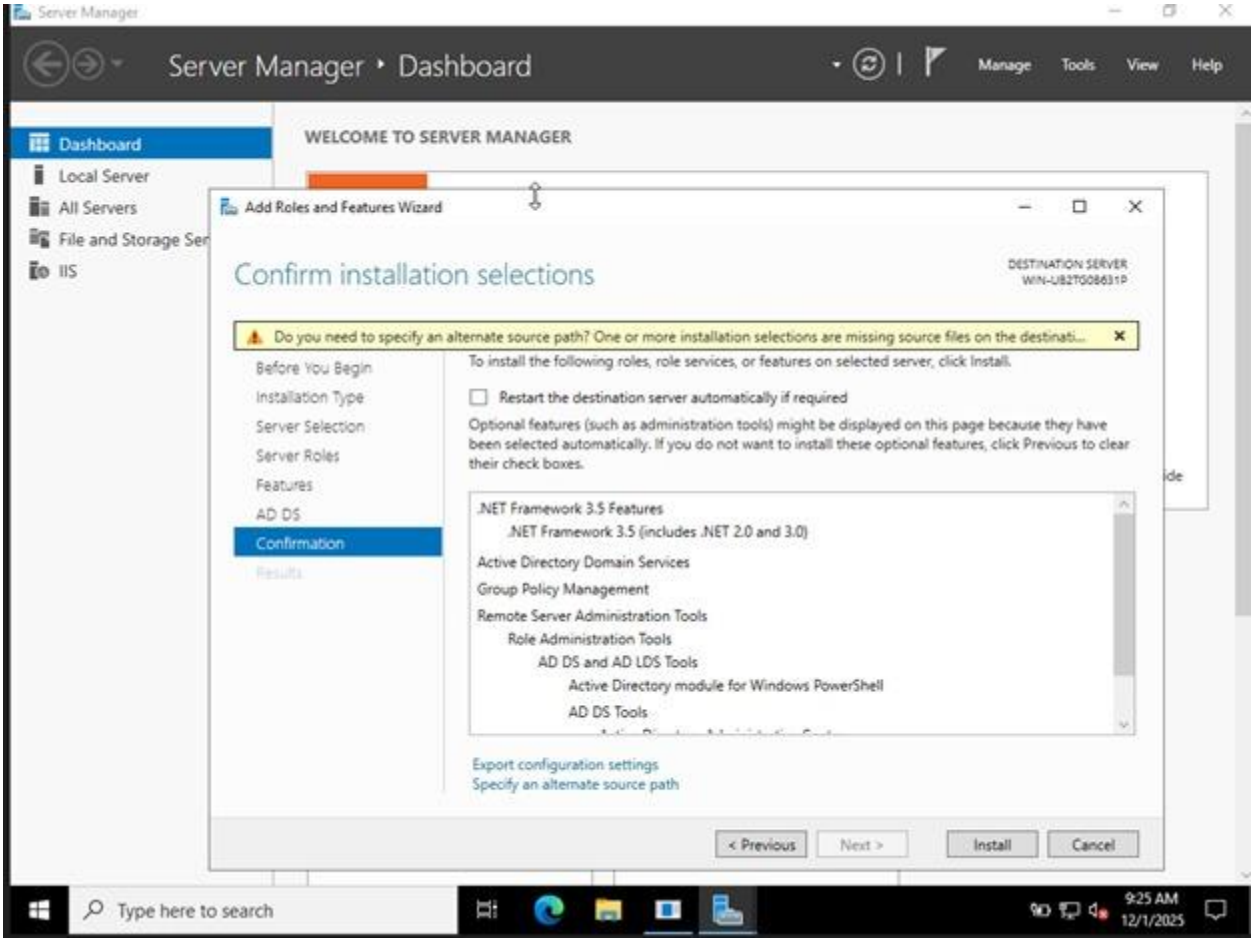

Figure 7: Confirm Default Features

Step 8: Begin Installation:

To begin installing AD DS on the chosen server, click the "Install" button. The installation progress will be shown by the wizard. After everything is finished, a confirmation message stating that the installation was successful will appear.

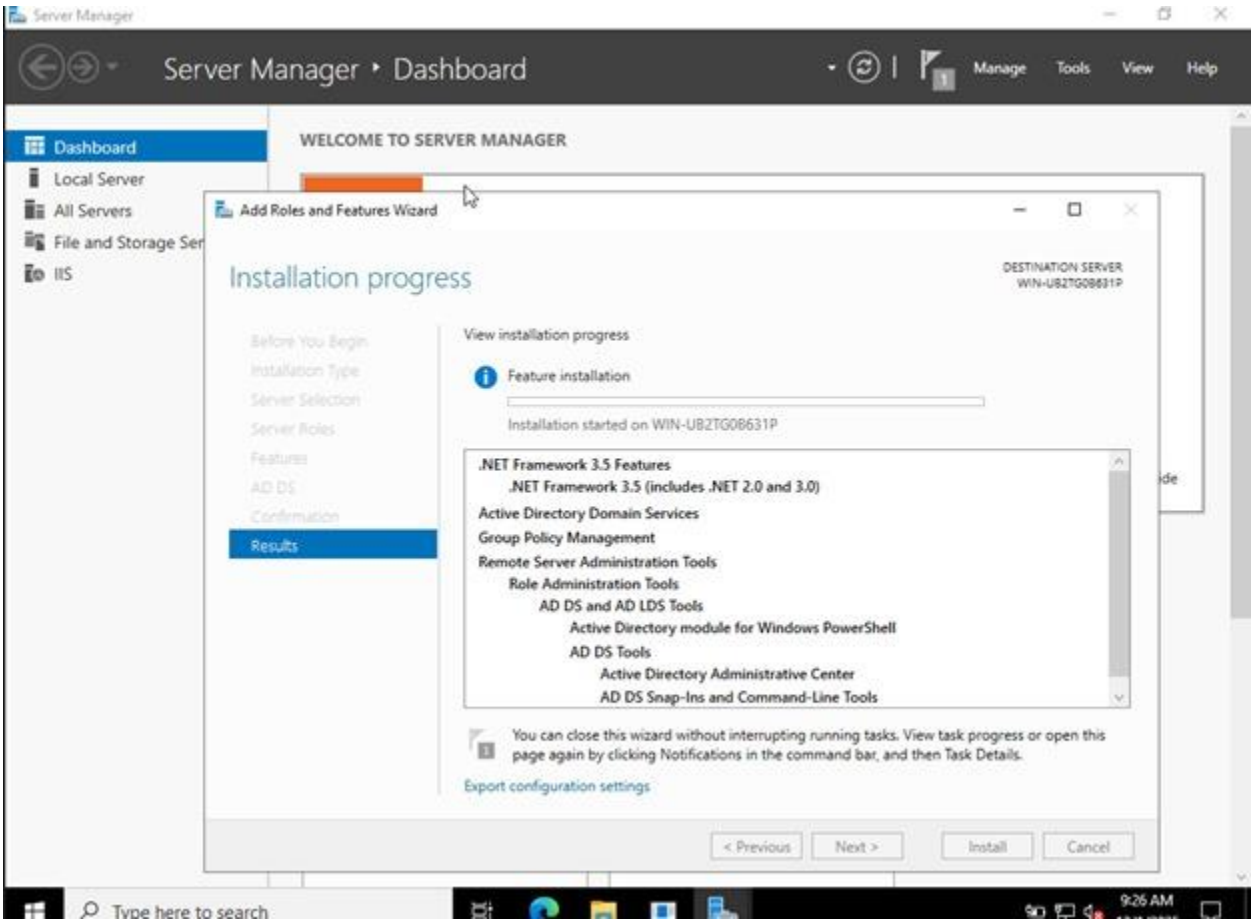

Figure 8: Installation Process

Step 9: Close Installation Wizard:

To close the initial installation wizard, click the "Close" button. The Server Manager interface will display a notification. This enables you to move on to the domain controller promotion phase.

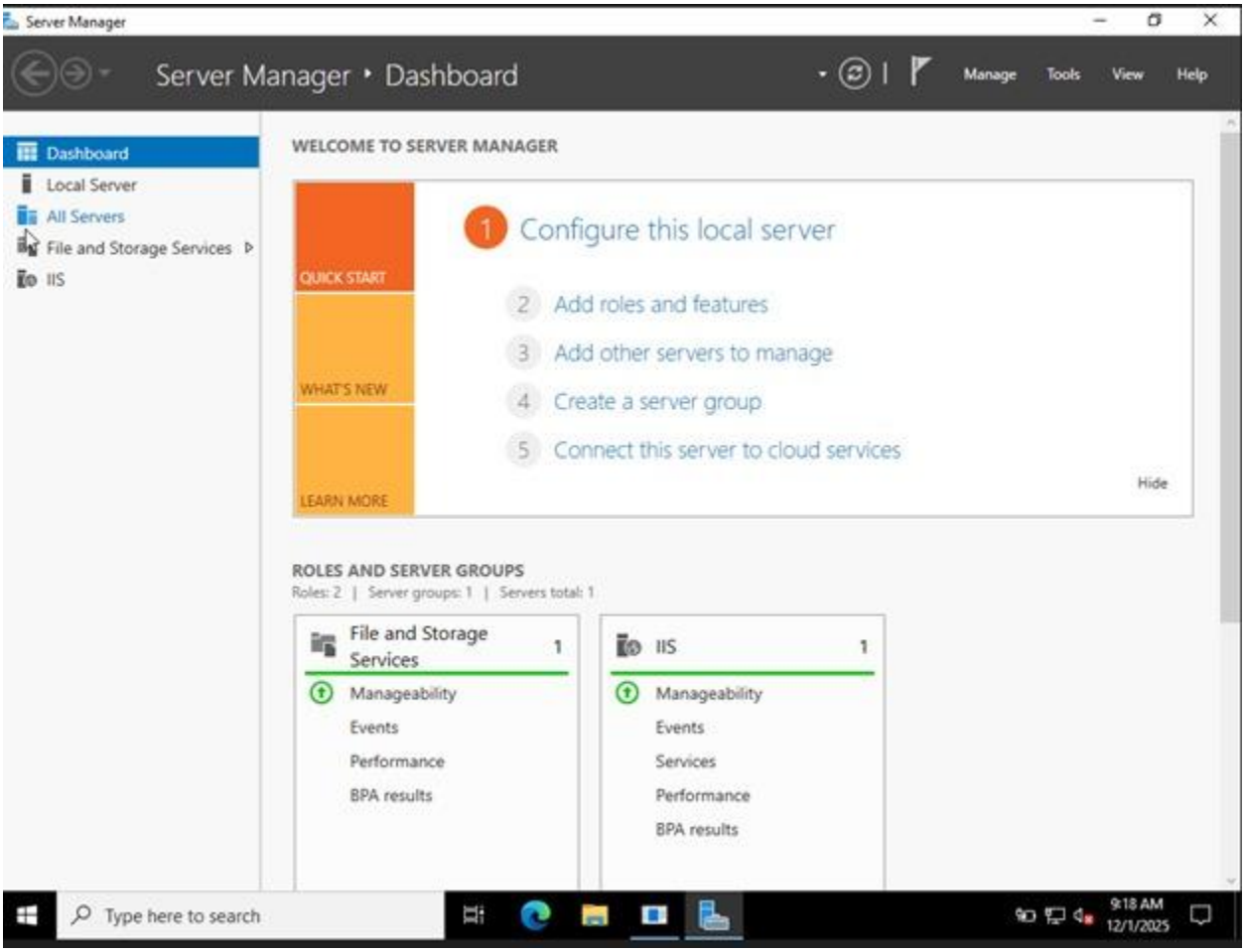

Figure 9: Close Installation

Step 10: Access Post-Deployment Configuration:

Click on the yellow notification icon in Server Manager to access post-deployment configuration options. This notification indicates that additional configuration is required to complete the setup. You will see the option to promote the server to a domain controller.

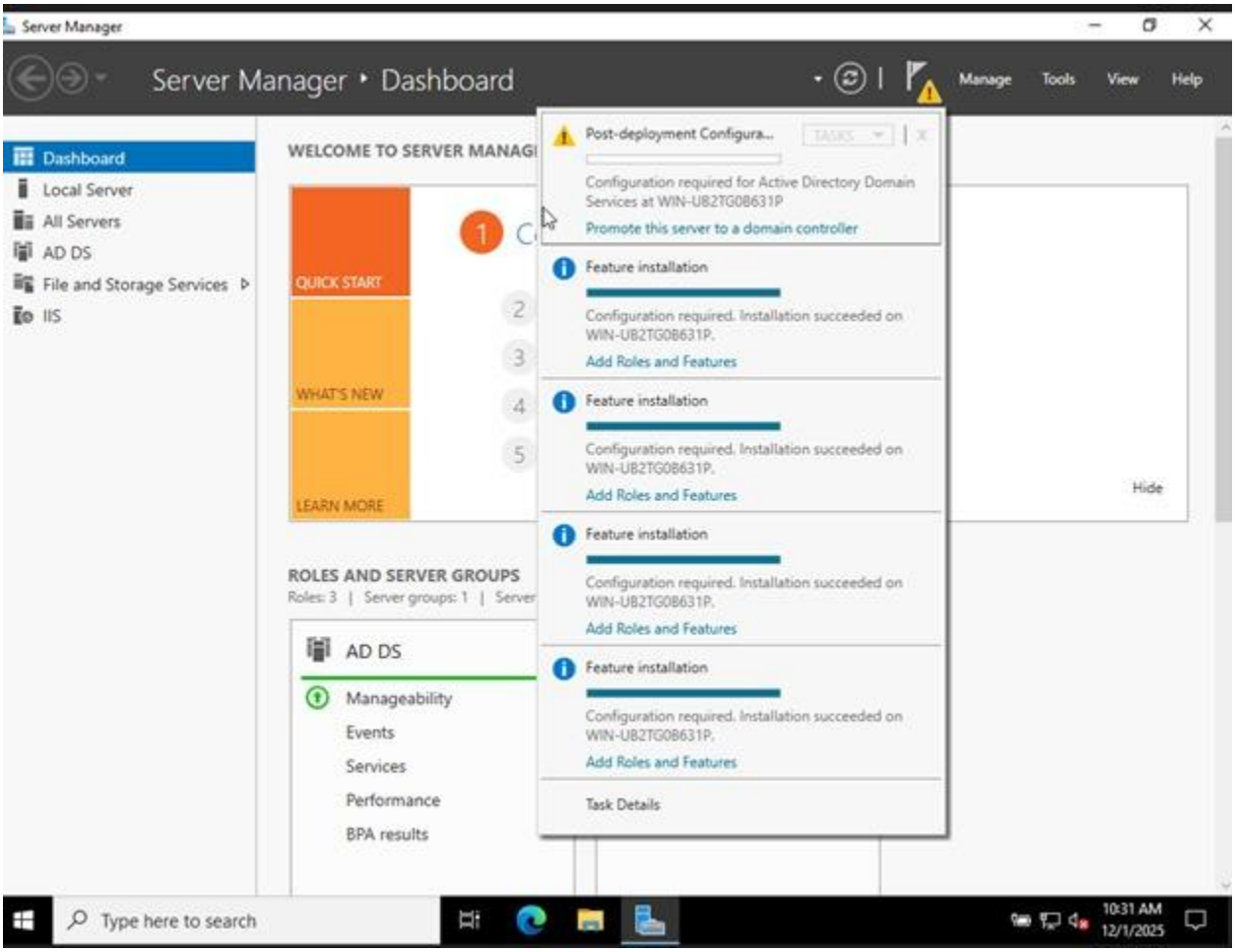

Figure 10: Access Post-Deployment Configuration

Step 11: Promote to Domain Controller:

Select "Promote this server to a domain controller" to launch the wizard for deployment configuration. This step transforms your server into an active domain controller within your network. Forest options will be displayed on the deployment configuration page.

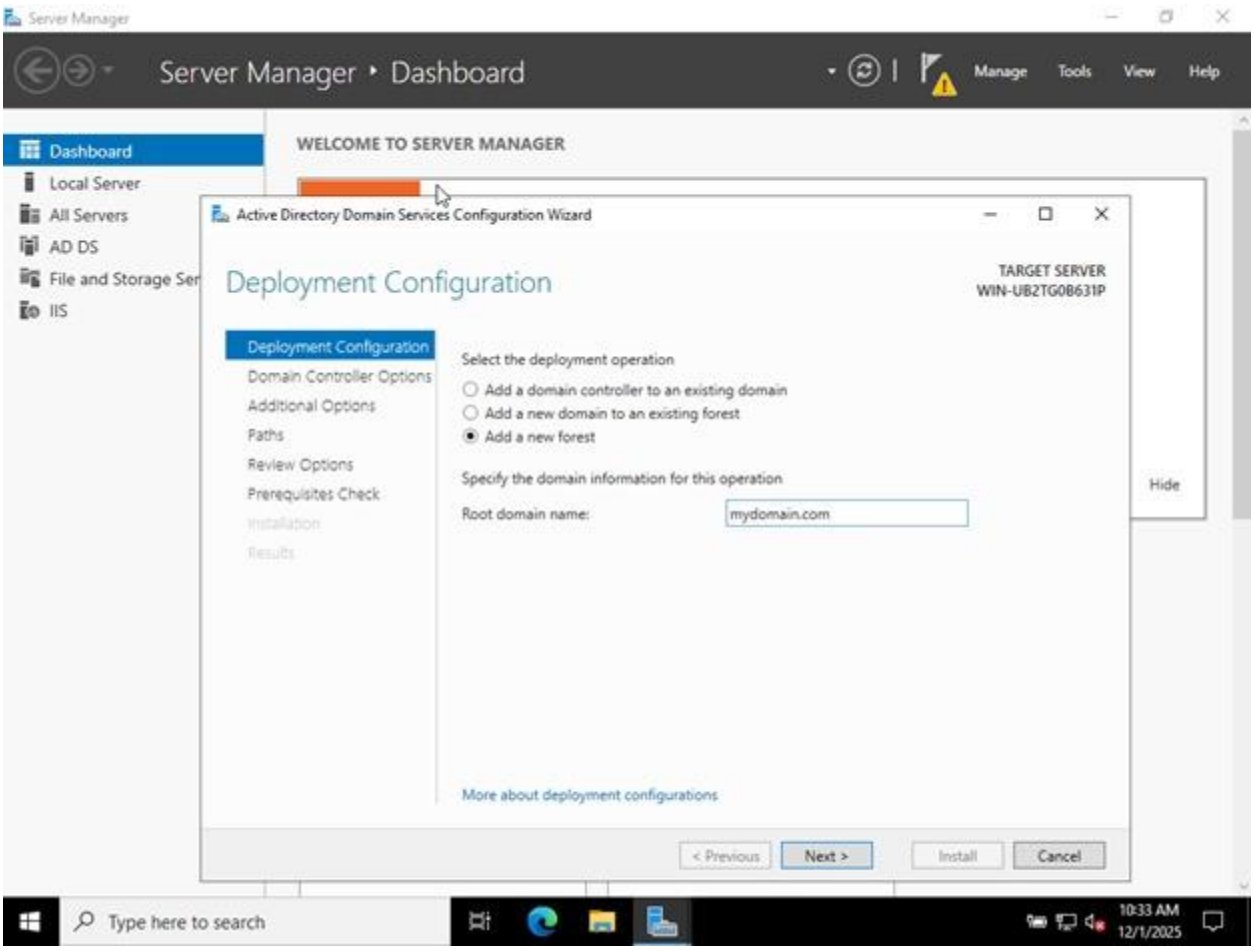

Figure 11: Domain Controller

Step 12: Create New Forest and Domain:

In the "Add a new forest" option, define your domain name, such as mydomain.com. This creates the first domain in your forest hierarchy and forms the root of your AD structure. Click "Next" to proceed to the domain controller options.

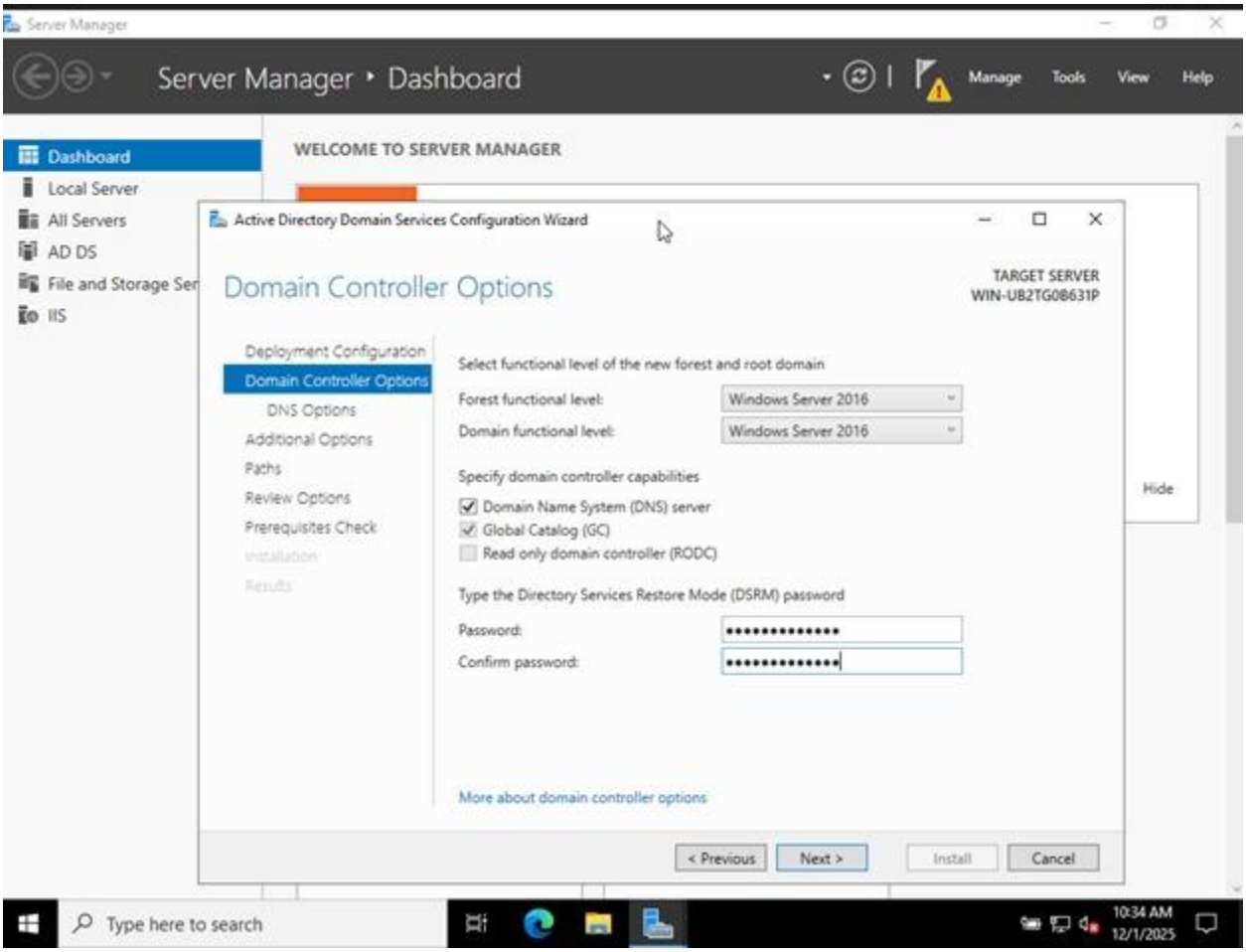

Figure 12: New Forest and Domain

Step 13: Set the Directory Service:

Restore Mode Password At the configuration page, define a secure password for DSRM, which is necessary for recovery and maintenance operations on servers. Click "Next" to proceed to the DNS configuration options.

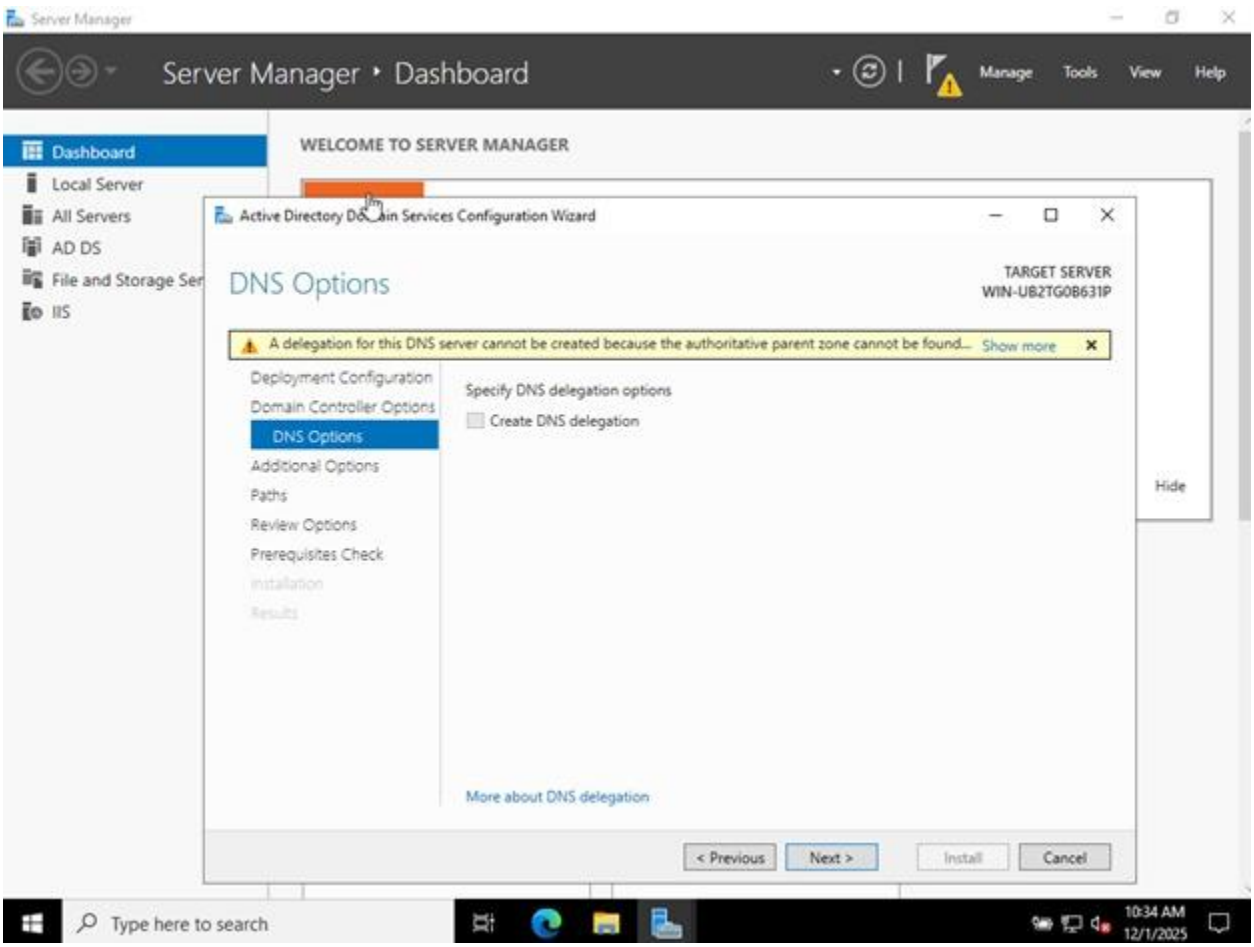

Figure 13: Set Directory Service

Step 14: Configure NetBIOS Name:

Configure the NetBIOS Name Leave the default configuration for DNS, then click "Next" when it asks for the configuration of the NetBIOS name. Set a NetBIOS name, typically 15 or fewer characters, to identify your domain to some legacy systems. This name ensures compatibility with older Windows systems.

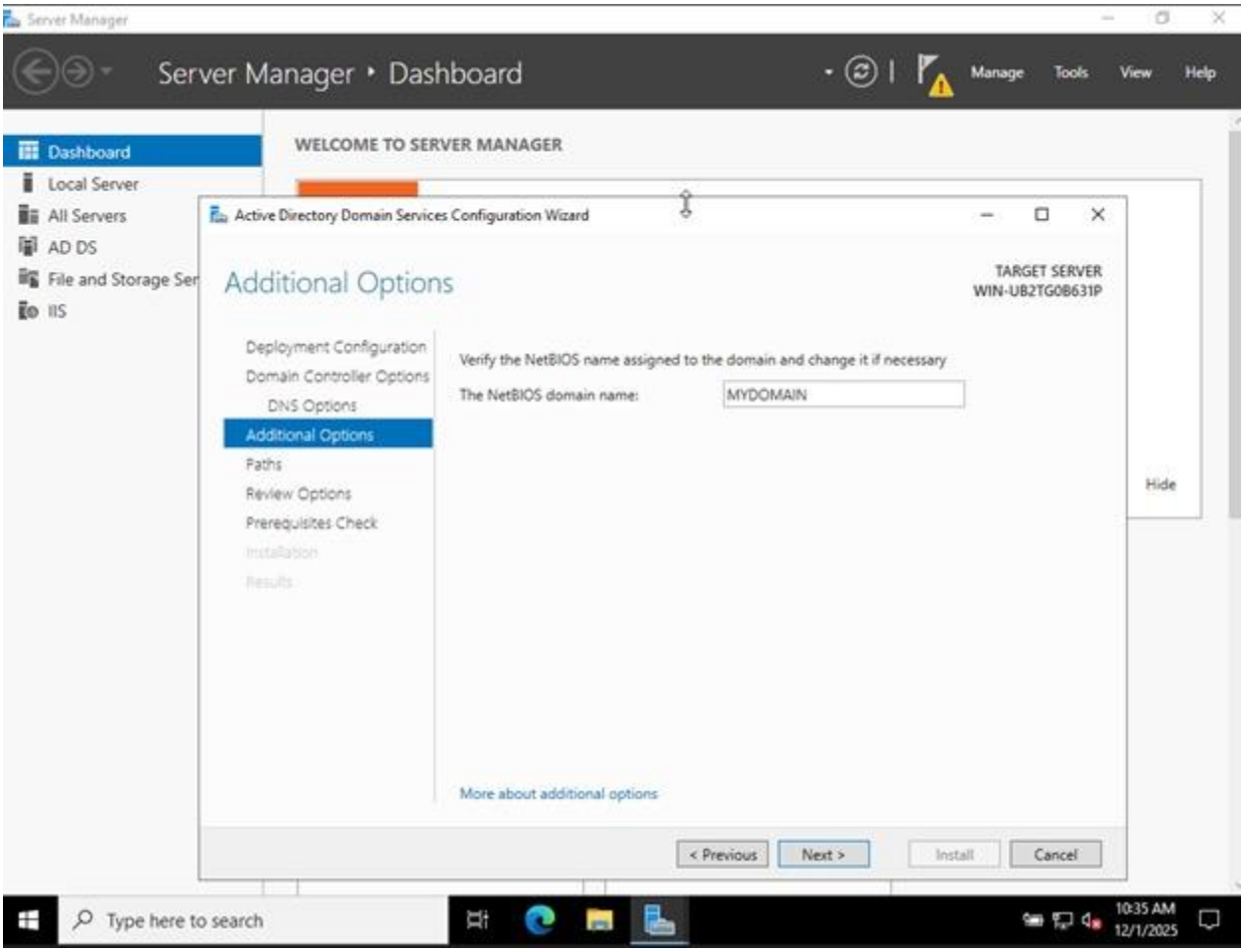

Figure 14: Configure NetBIOS Name

Step 15: Specify Database Paths:

Click Next and accept the defaults for the location of the Active Directory database and log files. These defaults are optimized for best performance and reliability. Click Next to open the review page.

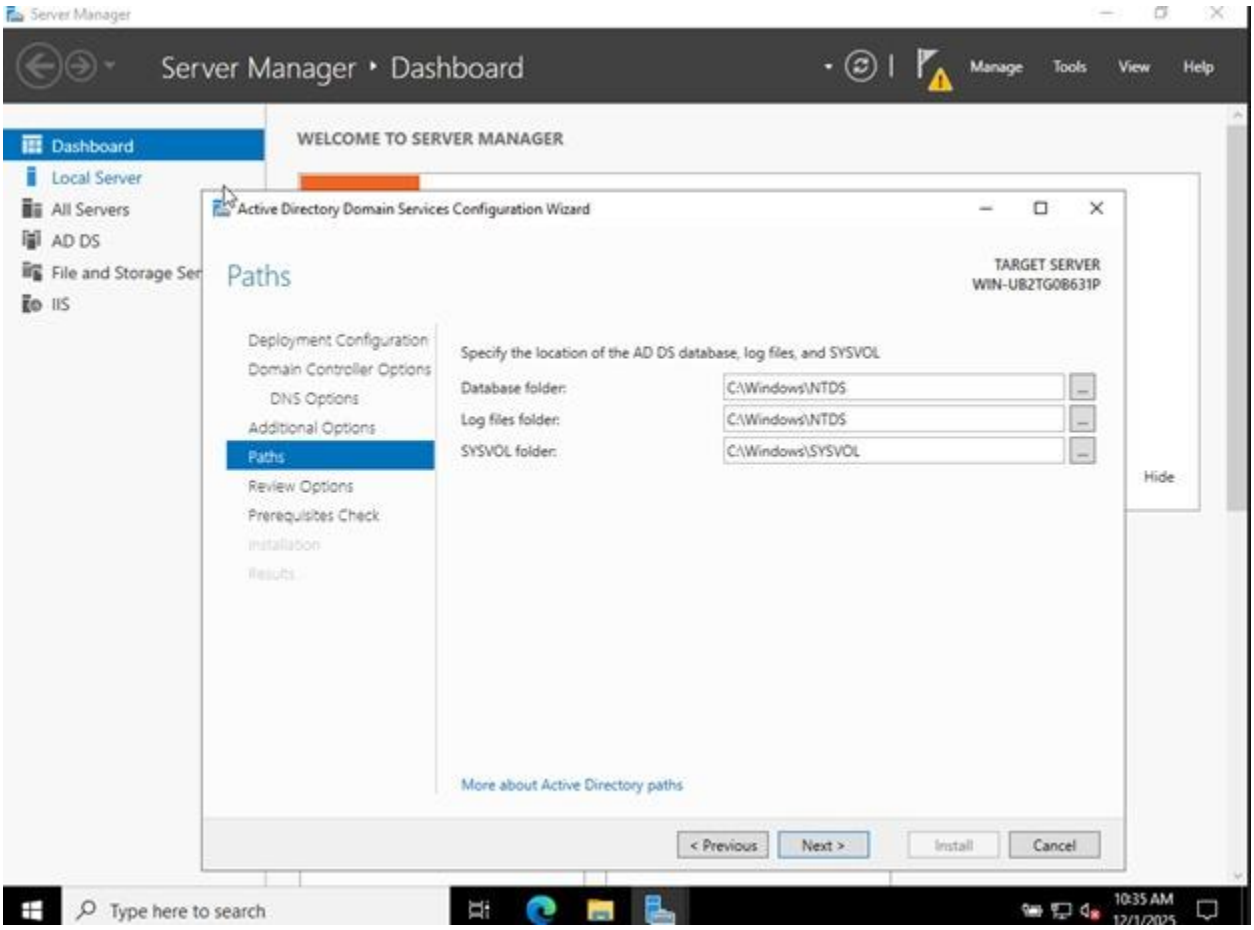

Figure 15: Specify Database Paths

Step 16: Review Configuration Settings:

Review all of the configuration settings you have provided throughout the wizard. Make sure the domain name, NetBIOS name, DSRM password, and paths are correct. This is your last chance to change the settings before installation.

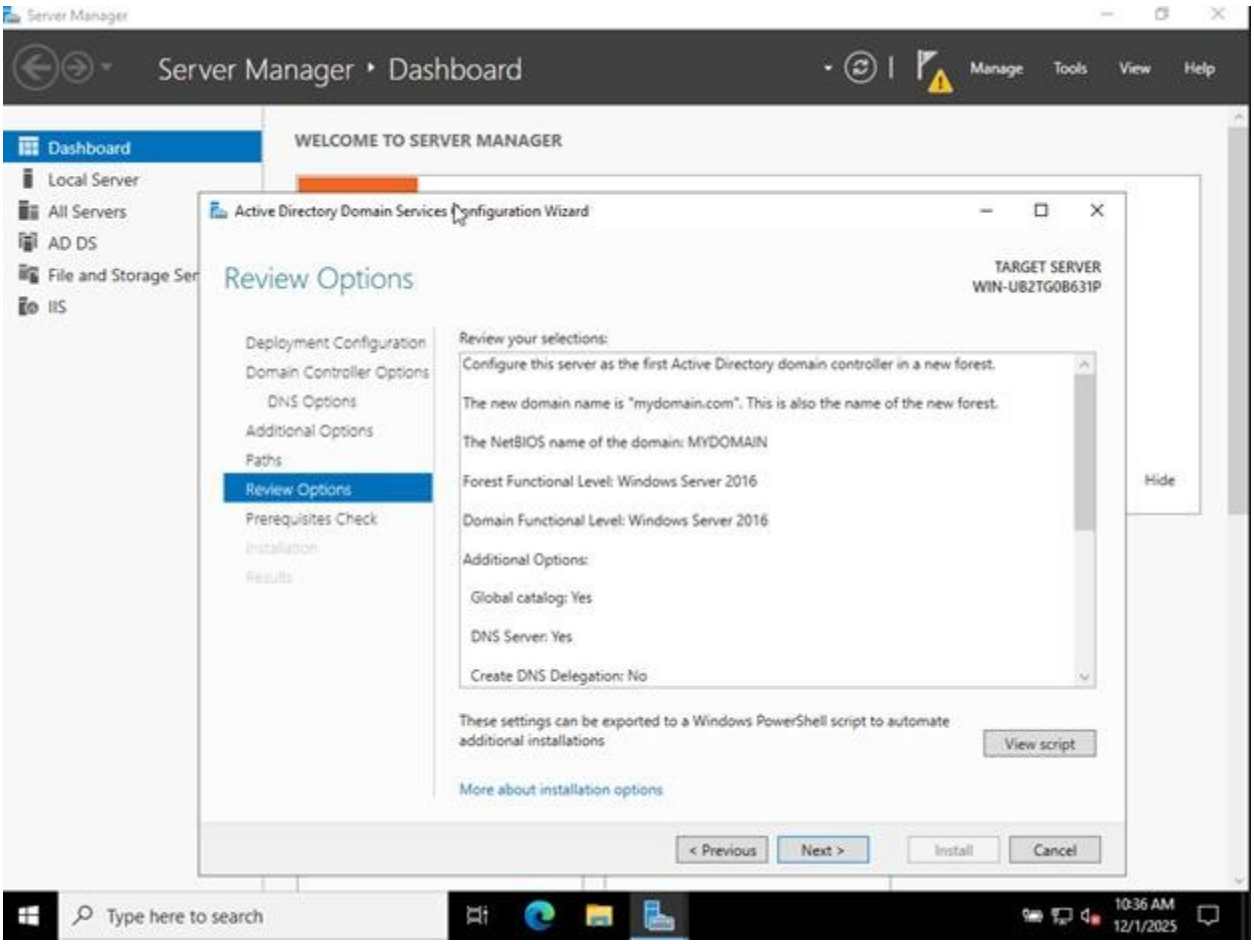

Figure 16: Review Configuration Settings

Step 17: Default Path:

Prerequisites Check The wizard will automatically check if all system prerequisites are met for the installation of AD DS. This validation ensures that your server meets all requirements for proper domain controller operation. Address any warnings or failures before proceeding.

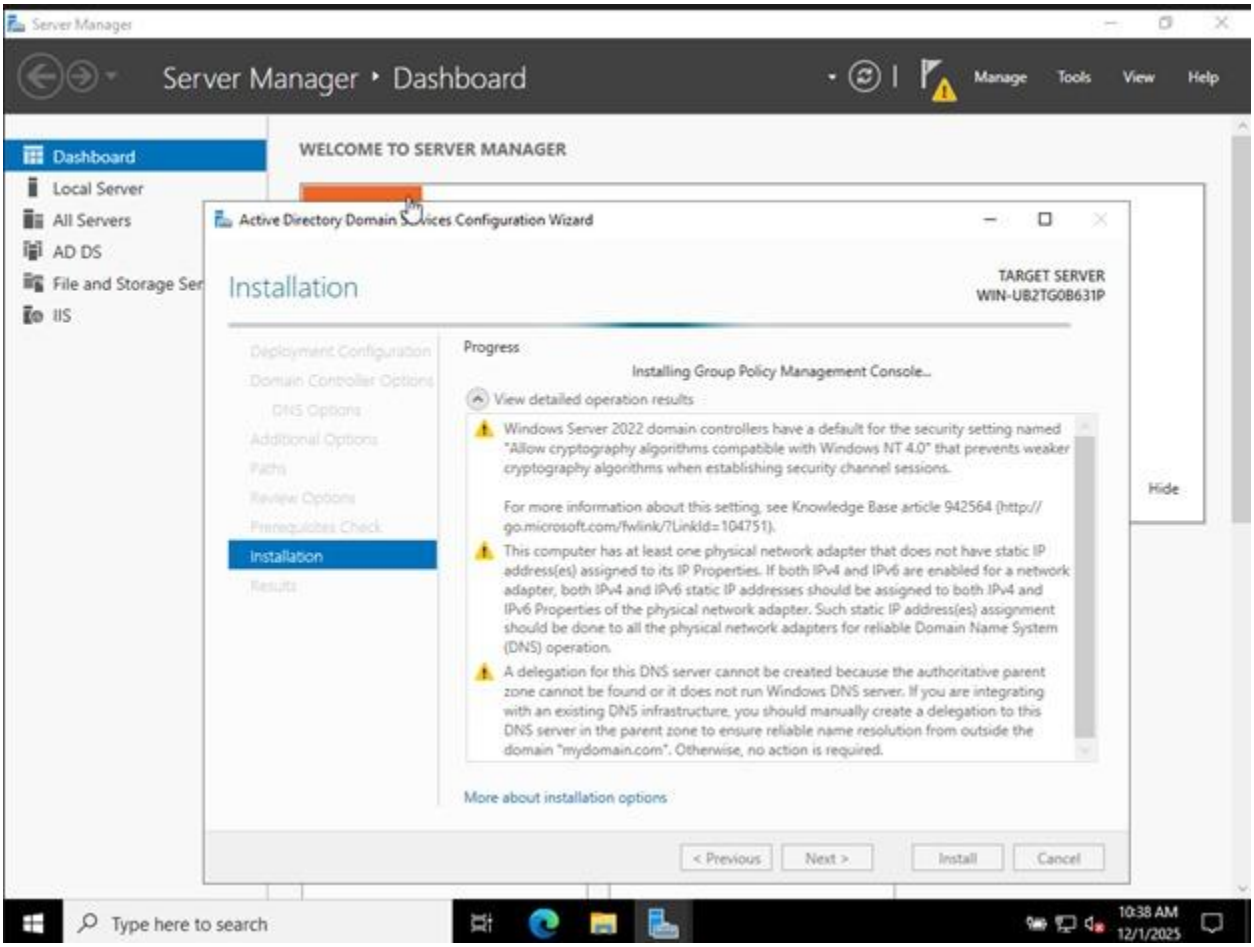

Figure 17: Prerequisites Check

Step 18: Complete Installation:

Click the "Install" button to complete the domain controller promotion. The system will automatically reboot after installation finishes. After the reboot, your server will be a full domain controller with all active AD DS services.

Next, you will need to verify whether the Domain Controller is adequately set up or not. Again, you can prove it from PowerShell.

To confirm the successful installation of the services, run the following command on Windows PowerShell.

Get-Service adws,kdc,netlogon,dns

You should see the status of all services on the following screen:

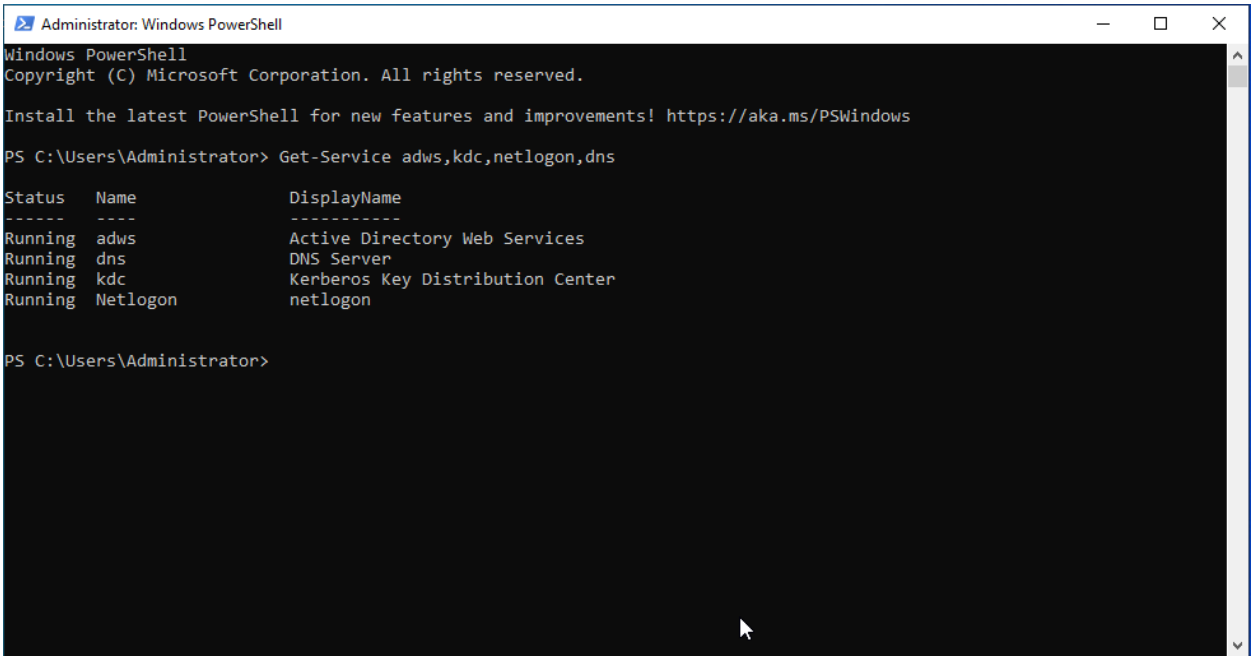

Figure 18: Successfully installed

Now, To display all the configuration details

of the domain controller, run the following command:

Get-ADDomainController

You should see all the information on the following screen:

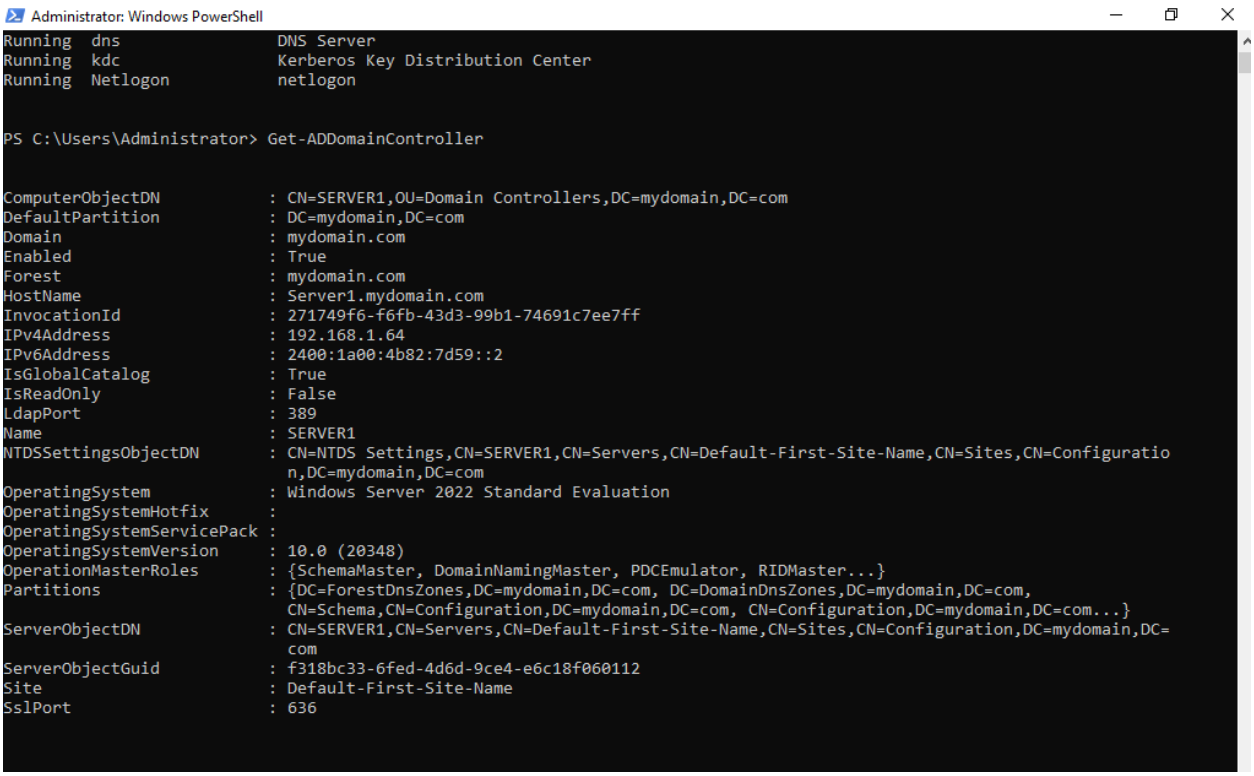

Figure 19: Configuration Details

To get detailed information about your domain, run the following command:

Get-ADDomain mydomain.com

You should see the next screen:

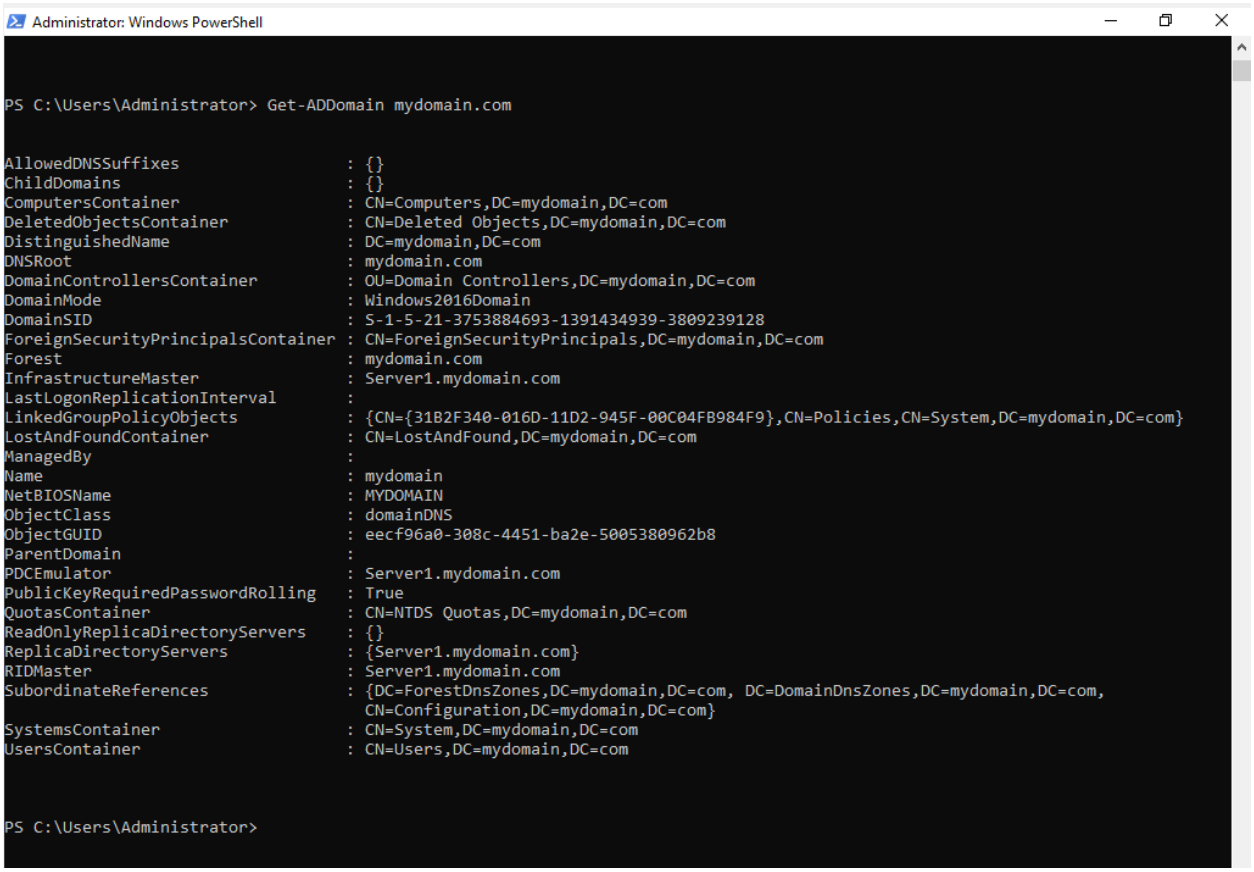

Figure 20: Domain Information

Again, to display your Active Directory Forest details, run the following command:

Get-ADForest mydomain.com

You should see the next screen:

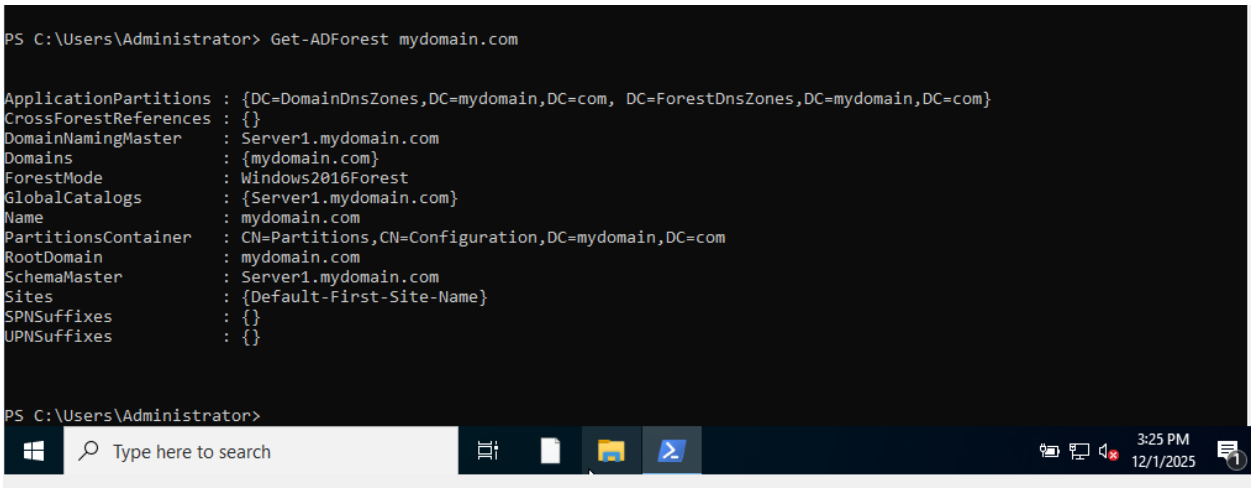

Figure 21: Active Directory Forest details

4 Conclusion:

This workshop task focuses on how to successful setup and verification of an Active Directory Domain Controller on Windows Server 2022 build up an integral infrastructure for centralized management in your network. From installation in 18 steps to post-deployment configuration, your server is now empowered to work as a domain controller in authenticating users, managing resources, and implementing security policies across the entire network.

Verification steps through PowerShell commands establish that all important services to keep your domain controller running (ADWS, KDC, Netlogon, and DNS) are up and running, ensuring that your domain controller is prepared to efficiently manage user accounts, computers, printers, and other network resources. The basis hereby formed is considered essential for providing centralized access control, user authentication, and group policy management within an organization.

References:

Lepide (2025) *What is Active Directory and How It Works?* [online].

Available at: https://www.lepide.com/blog/what-is-active-directory/

(Accessed: 1 December 2025).

Cayosoft (n.d.) *What Is an Active Directory Forest?* [online].

Available at: https://www.cayosoft.com/what-is-an-active-directory-forest/

(Accessed: 1 December 2025).

Storyly (n.d.) What is *Customization and how its done* [online].

Available at: https://www.storyly.io/glossary/customization (Accessed: 1 December 2025).