

Implementation of Active Directory Domain Services for Centralized Identity Management

By: Lloyd Ensor Azumah

Overview

This project demonstrates the implementation of Microsoft Active Domain Services (AD DS) to centralize user authentication, access control and resource management within a simulated enterprise network. The goal is to enhance security, improve administrative efficiency and establish a foundation for identity management in a Windows environment.

Objectives

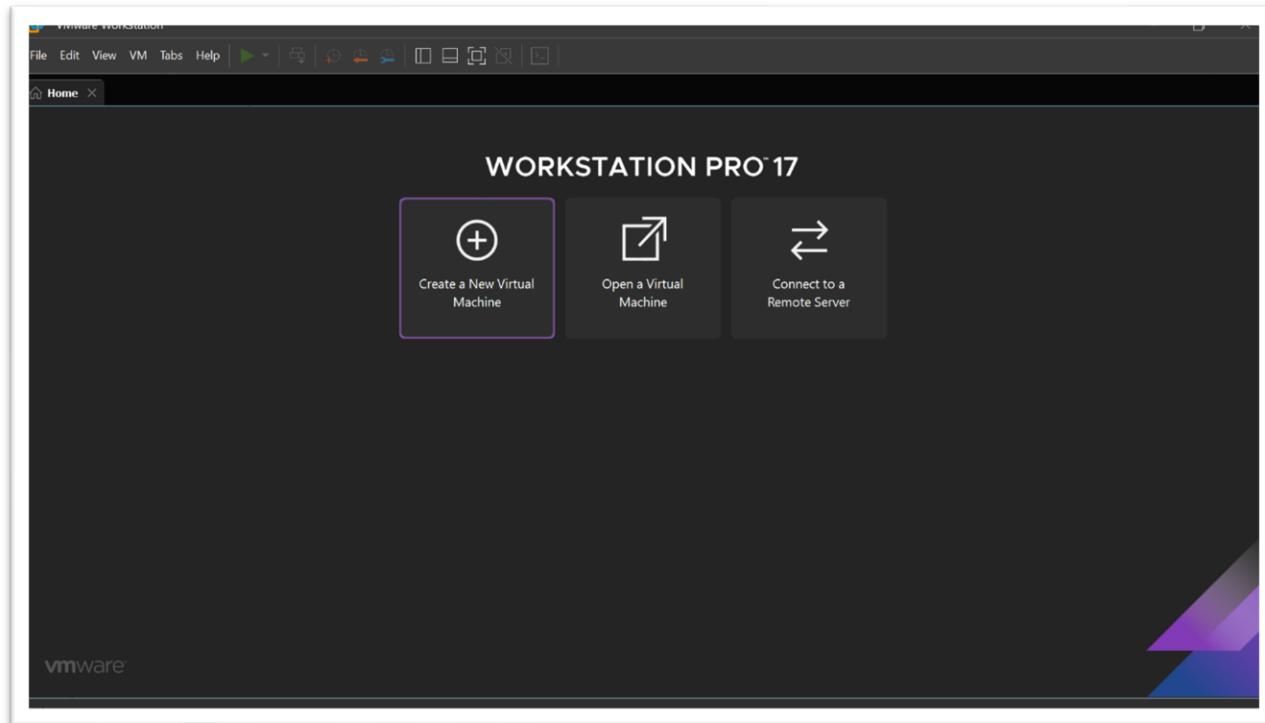
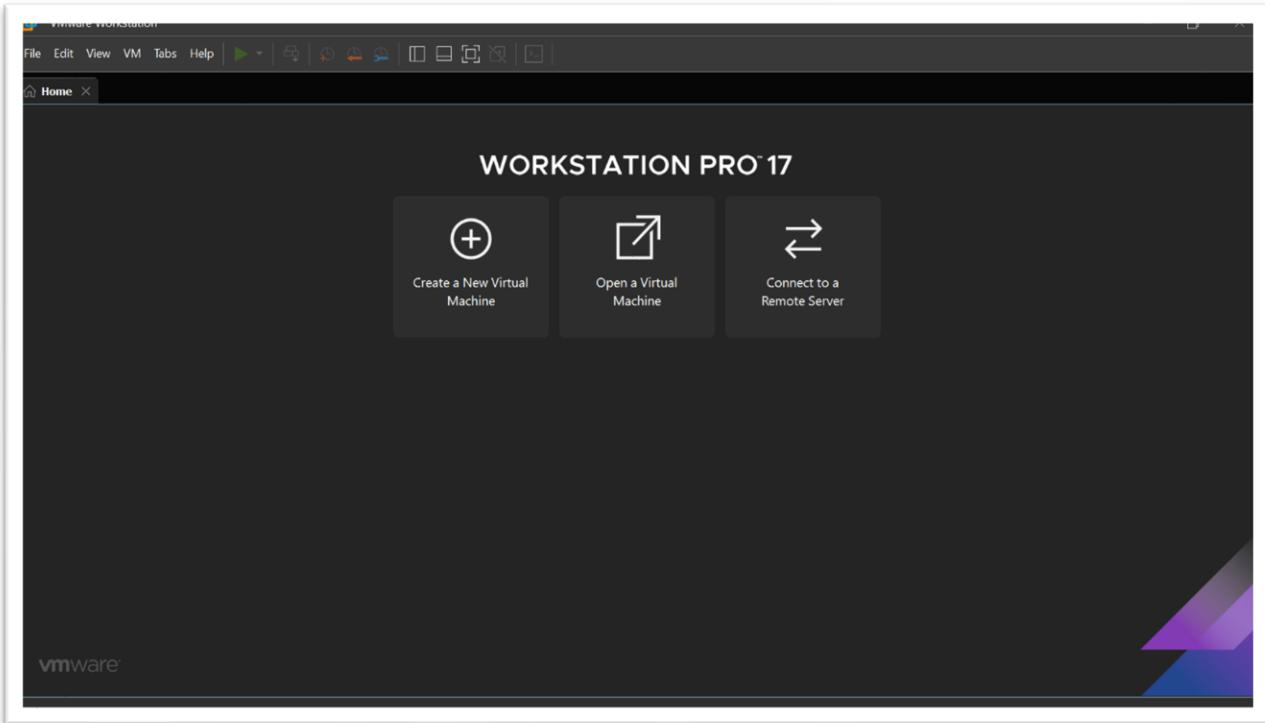
- Deploy a Windows Server and configure it as a Domain Controller.
- Create and organize users, groups and organizational units (OUs).
- Implement Group Policy Objects (GPOs) for centralized security and system configuration.
- Demonstrate access control using permissions and group memberships

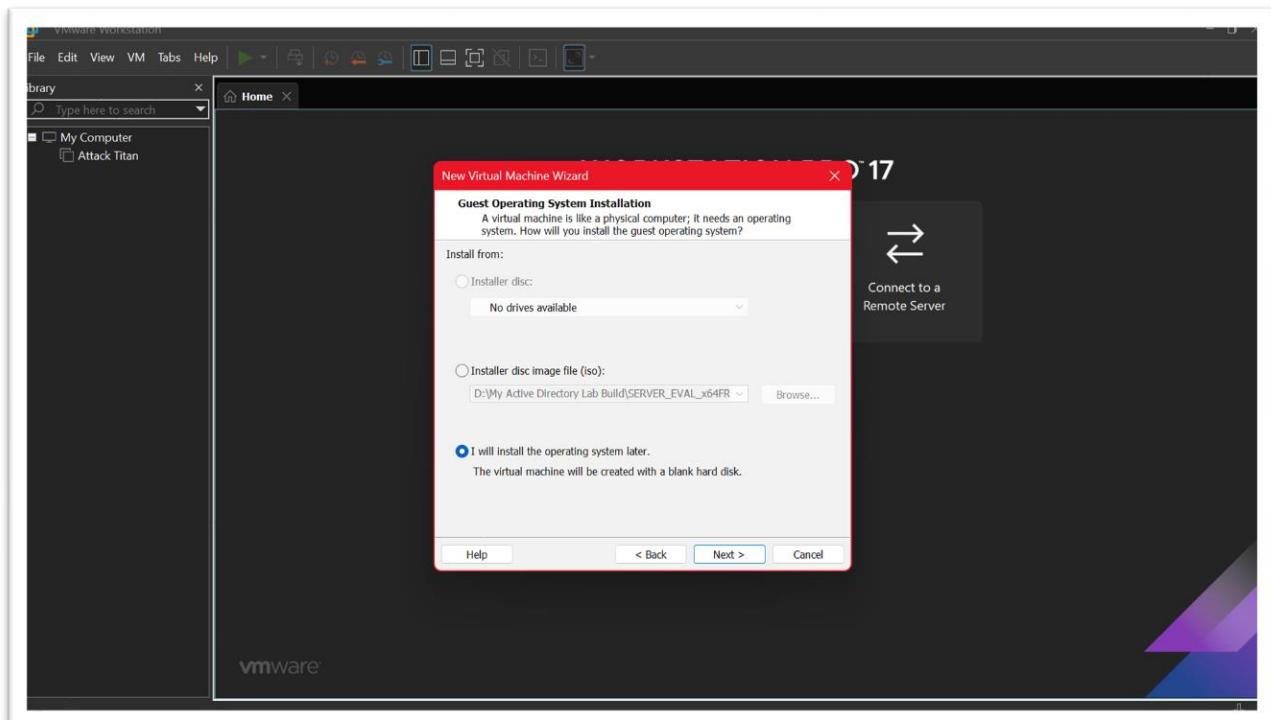
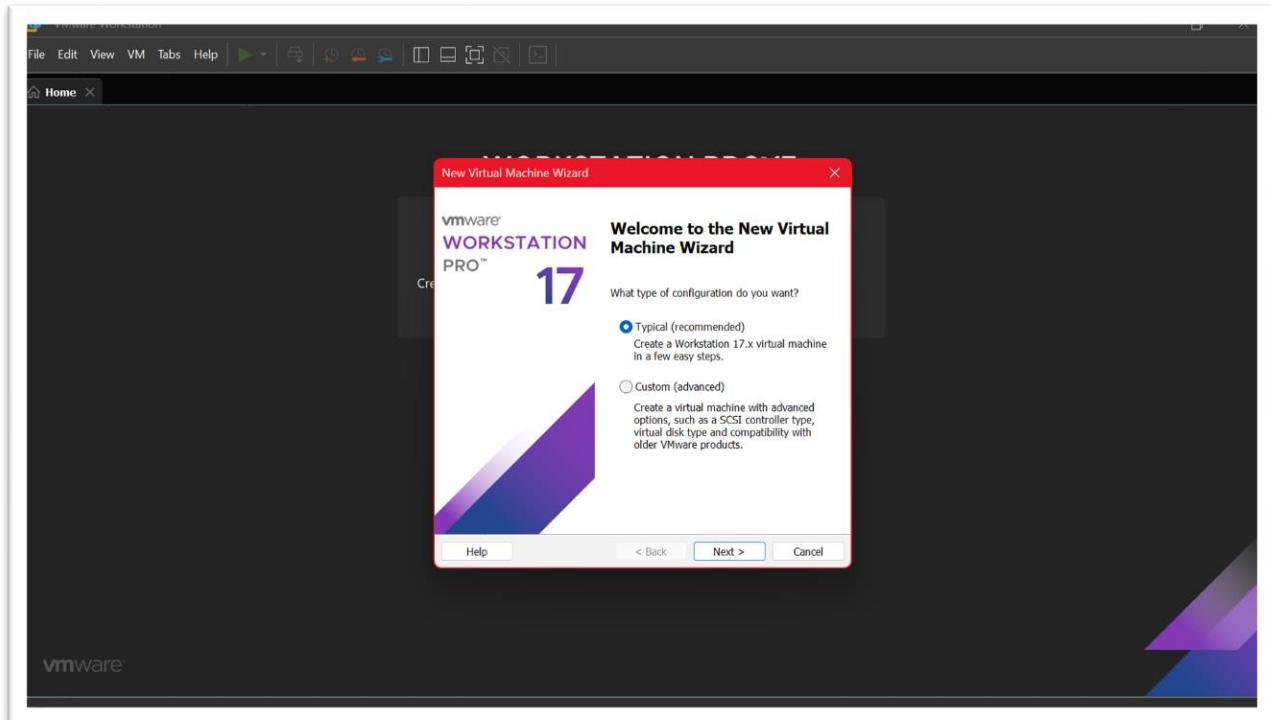
Tools and Technologies

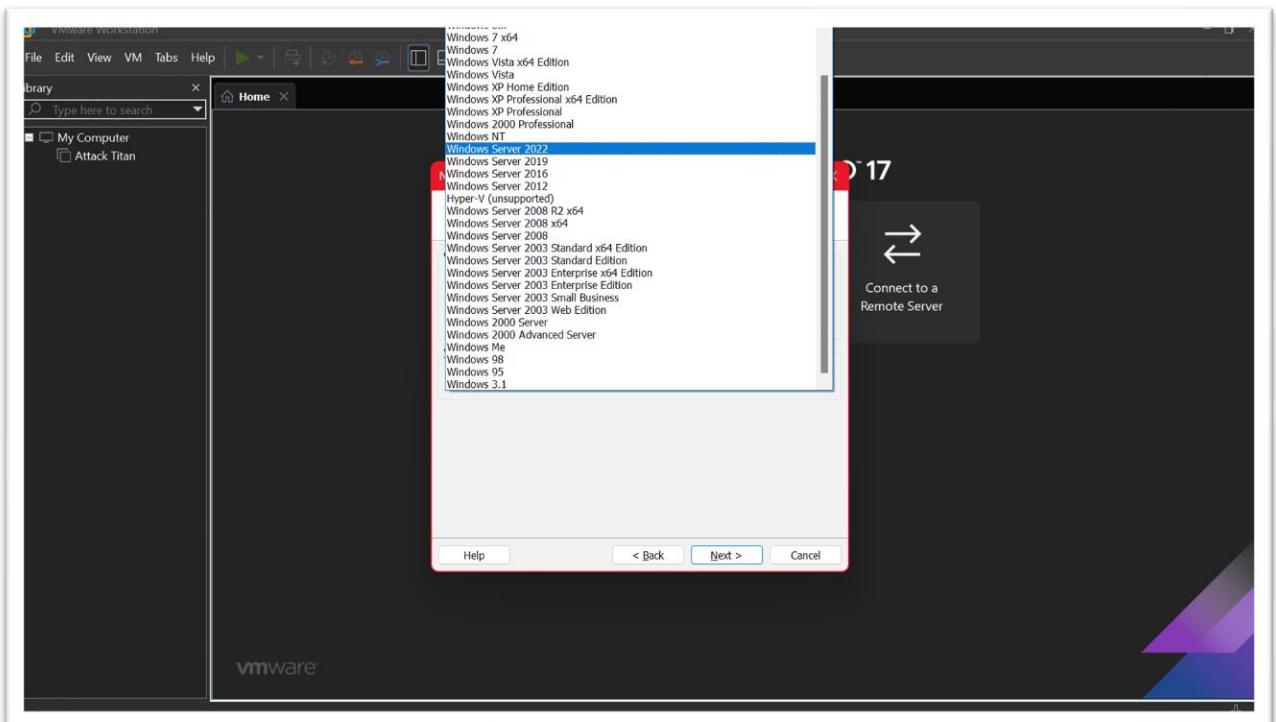
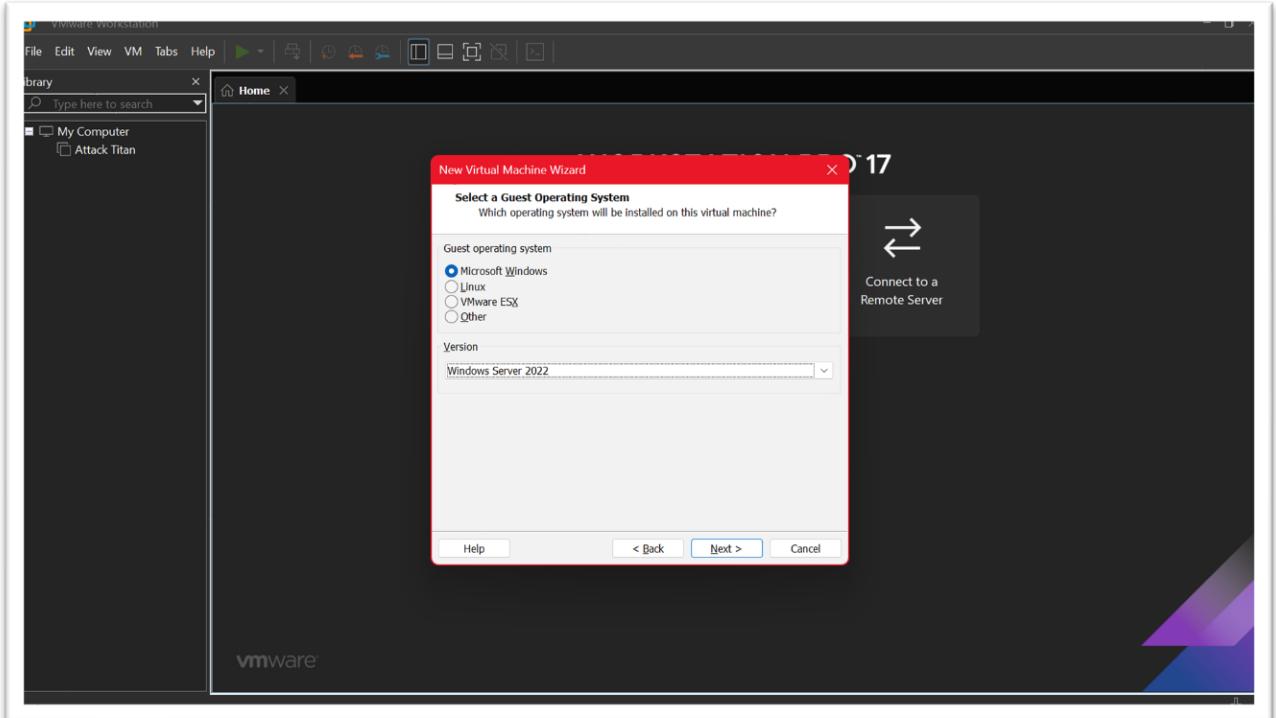
- Operating System: Windows Server 2022
- Windows 11
- Virtualization: VMware Workstation
- Network Configuration: NAT/Internal Network
- Admin Tools: Active Directory Users and Computers (ADUC), Group Policy Management Console (GPMC)
- Automation tool: PowerShell

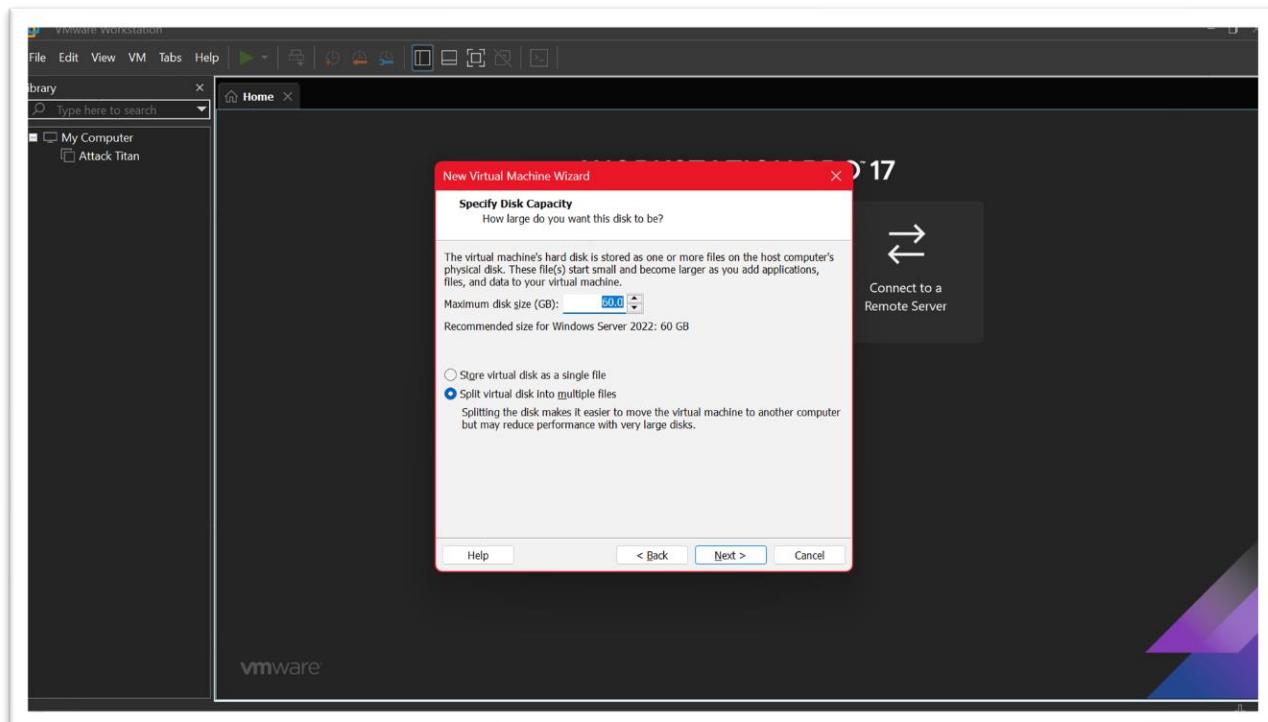
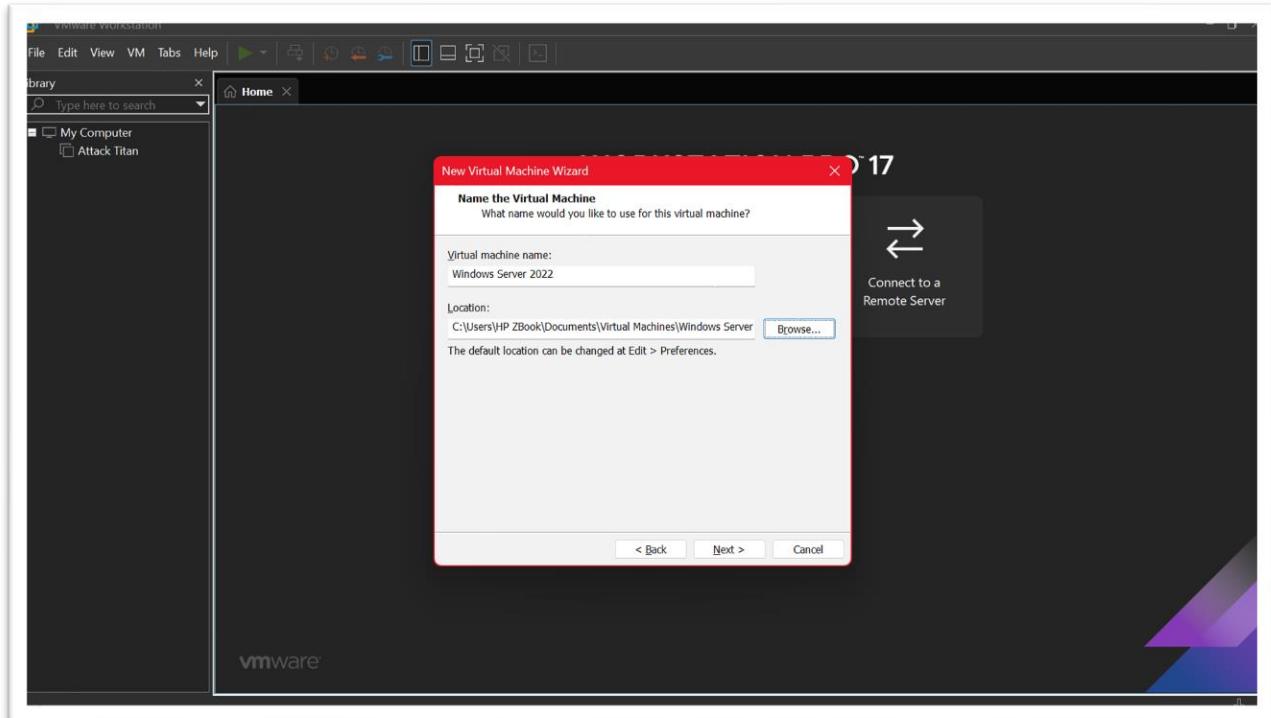
IMPLEMENTATION STEPS

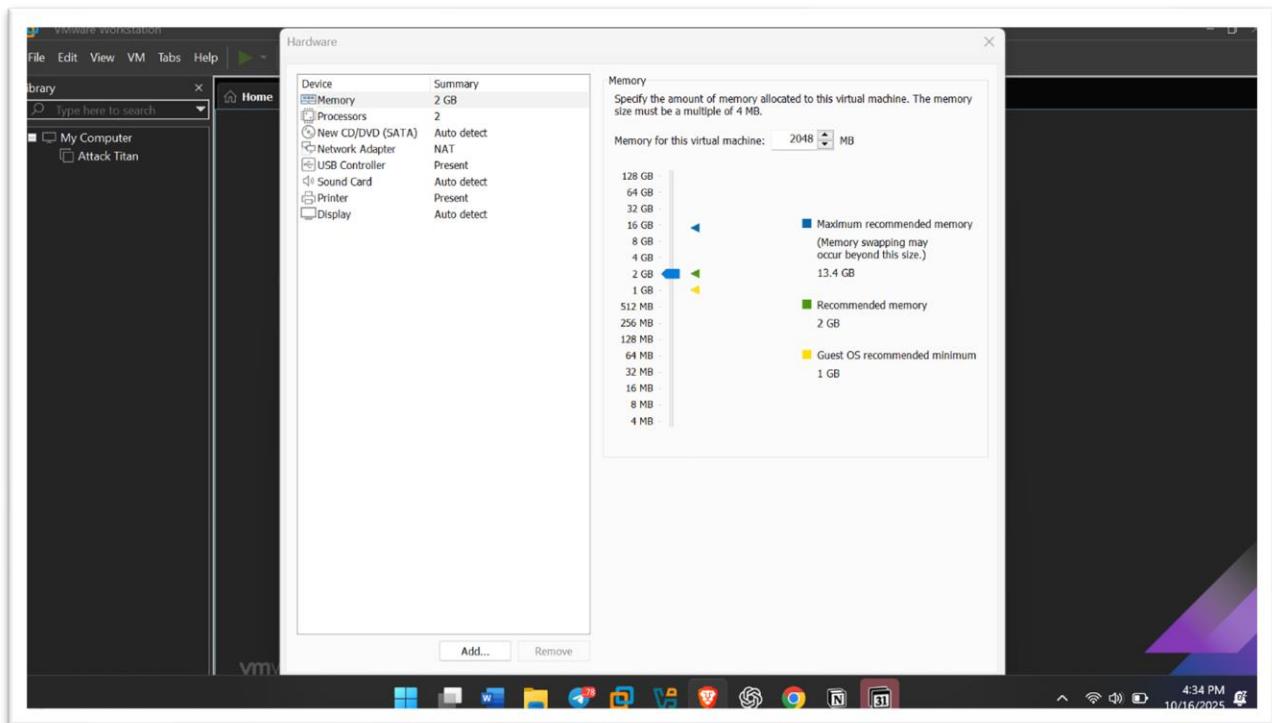
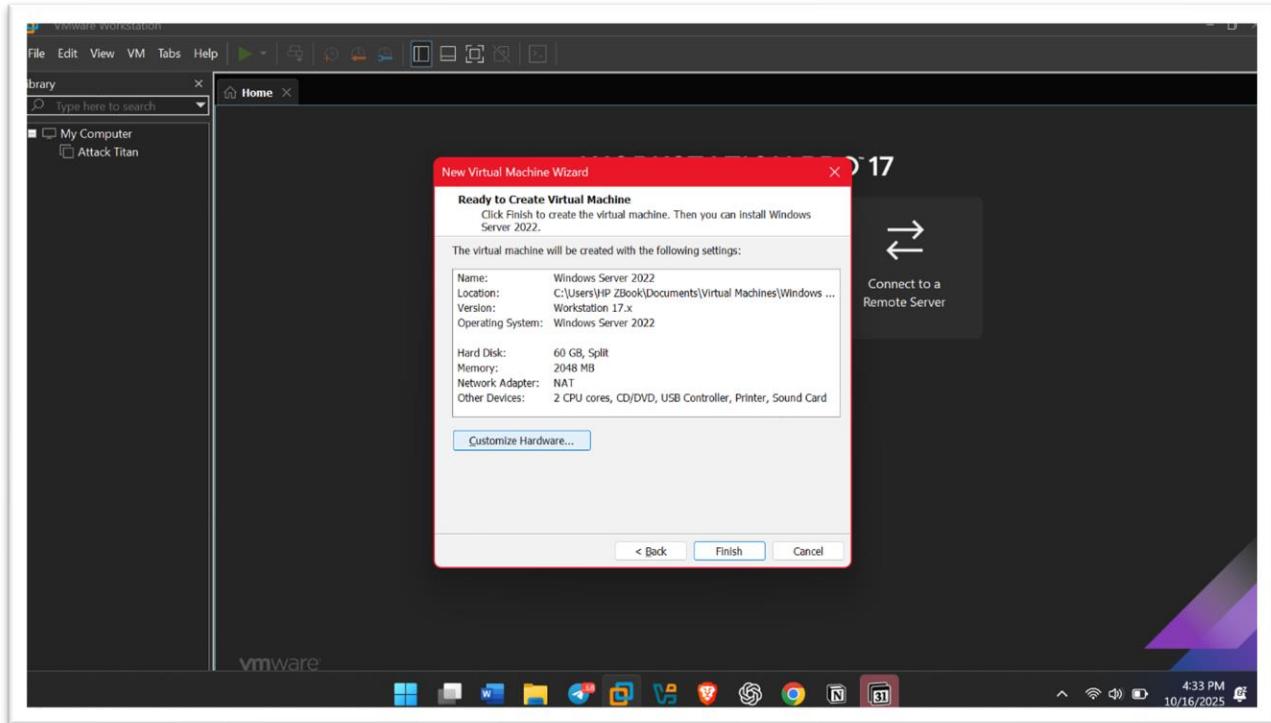
Step 1: *Install and configure Windows Server 2022 as a virtual machine (VM)*

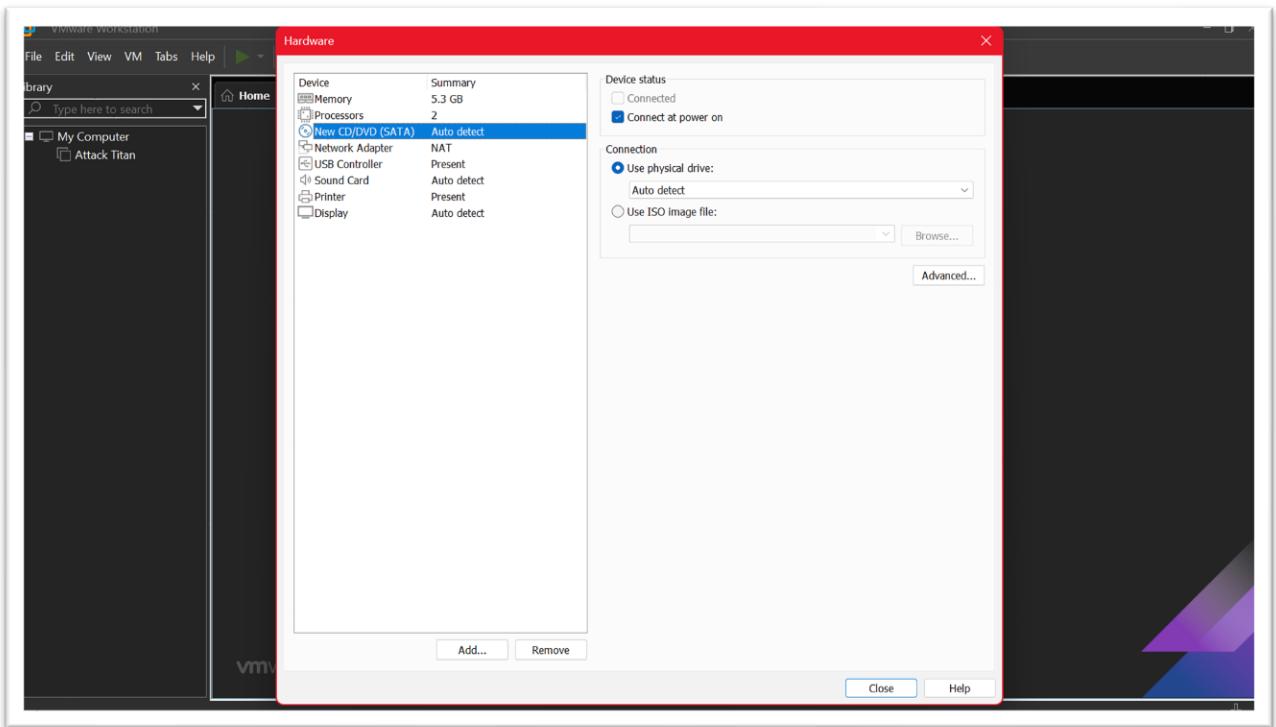
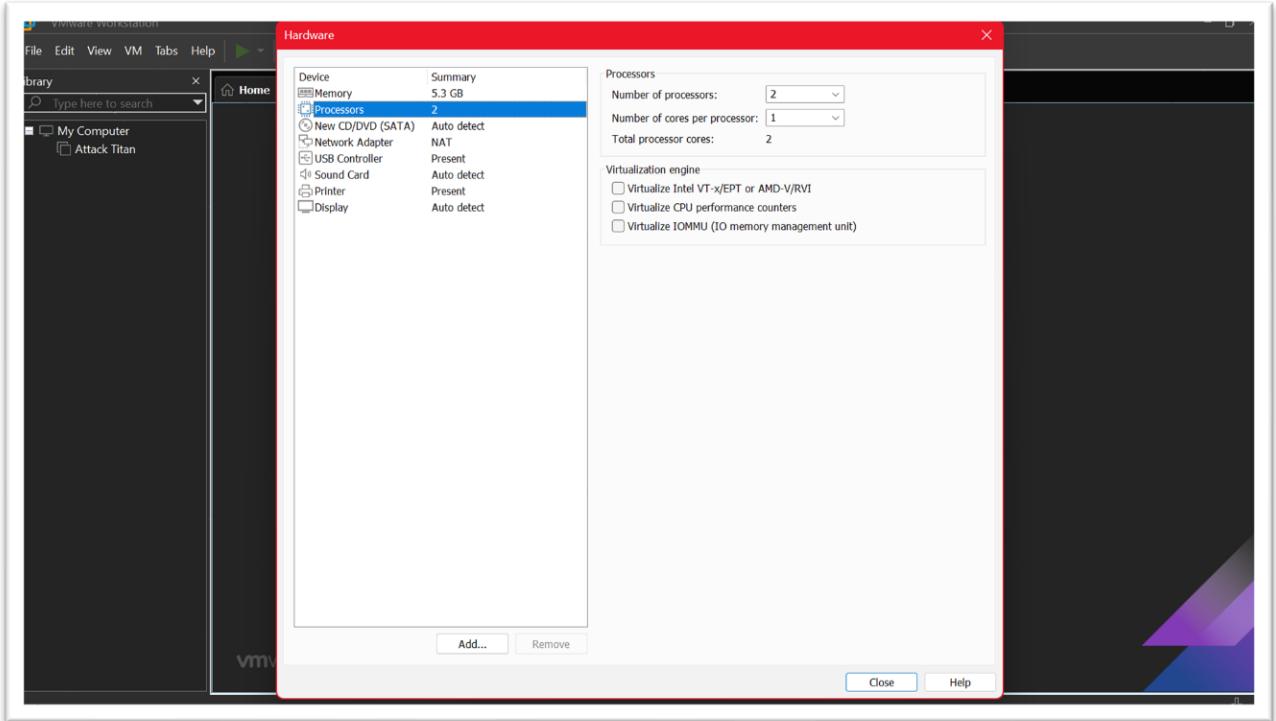


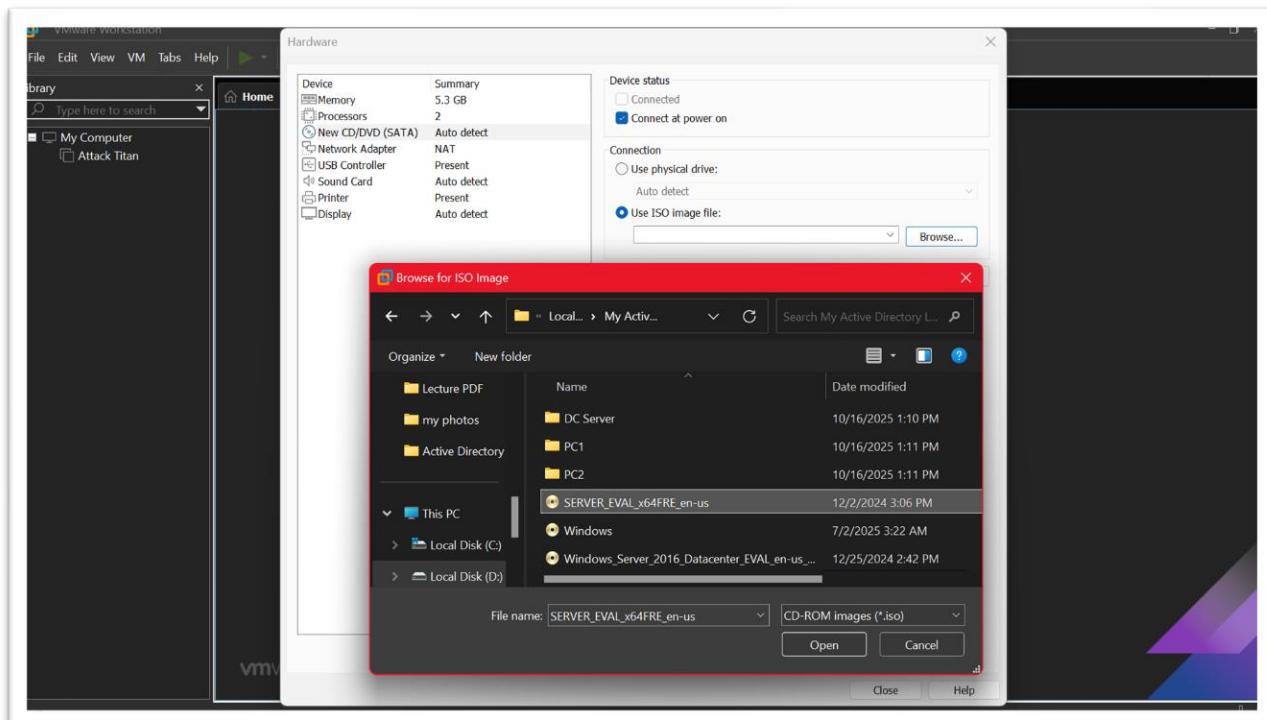
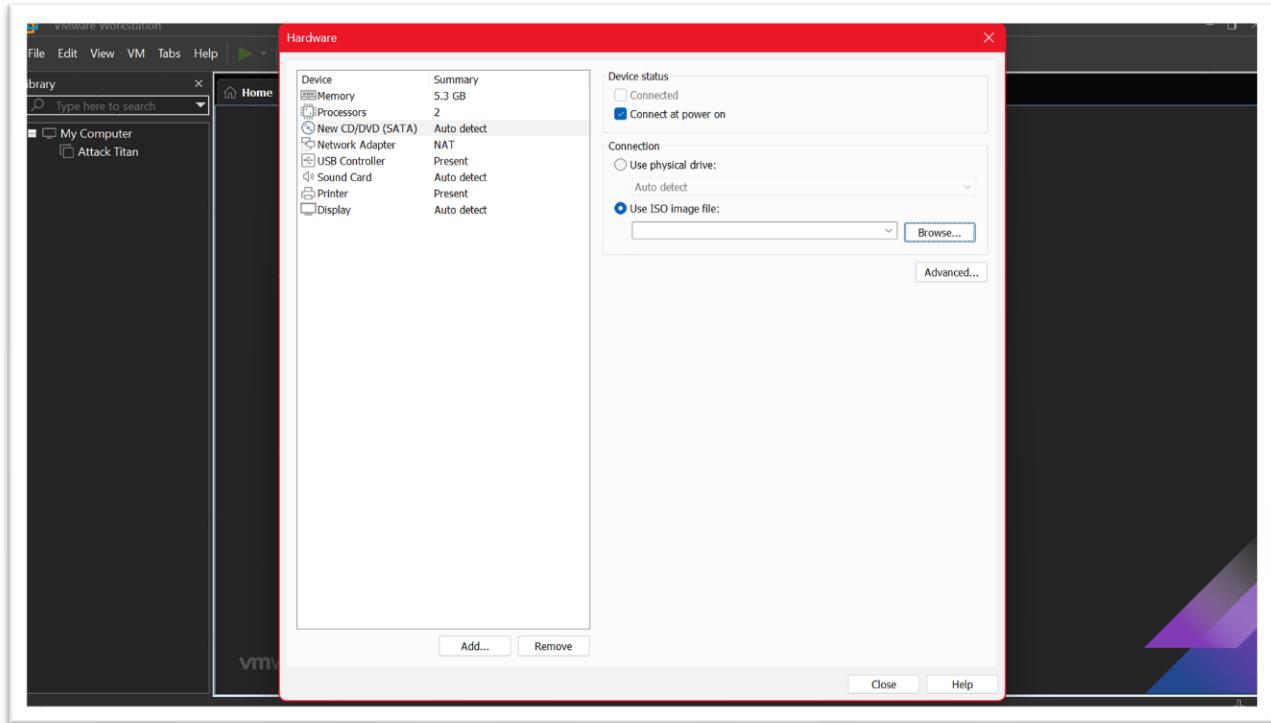


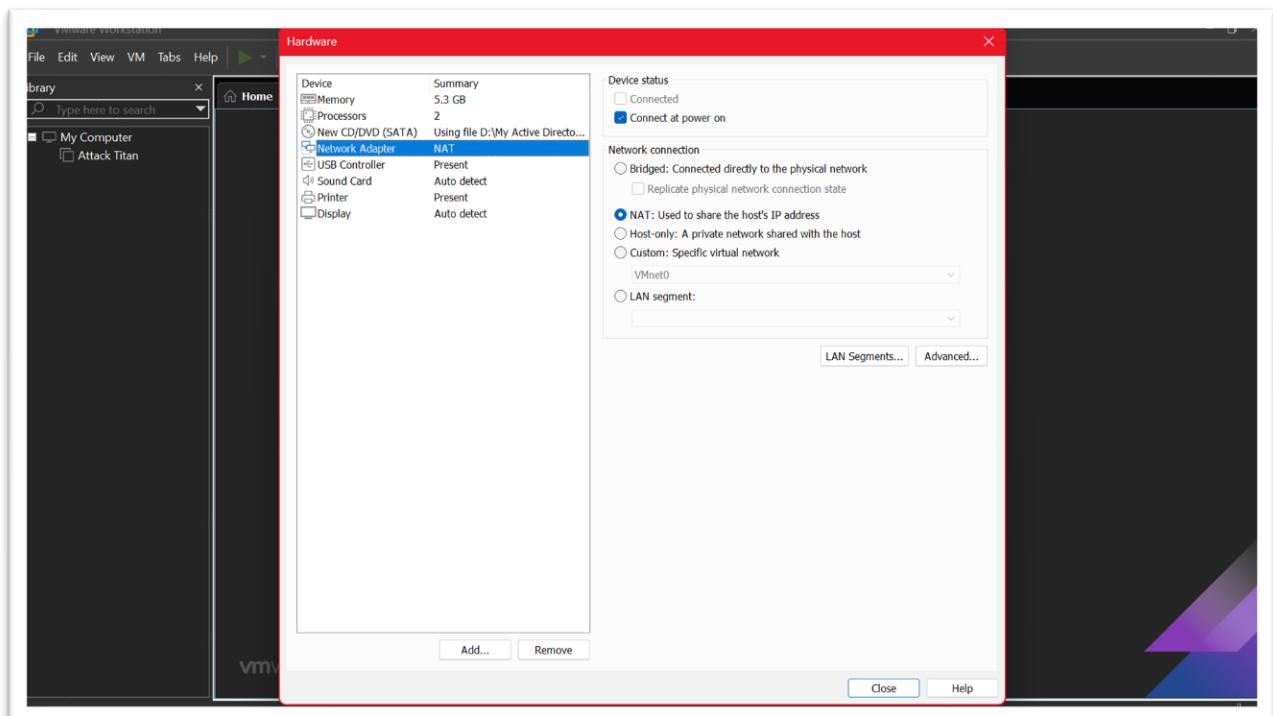
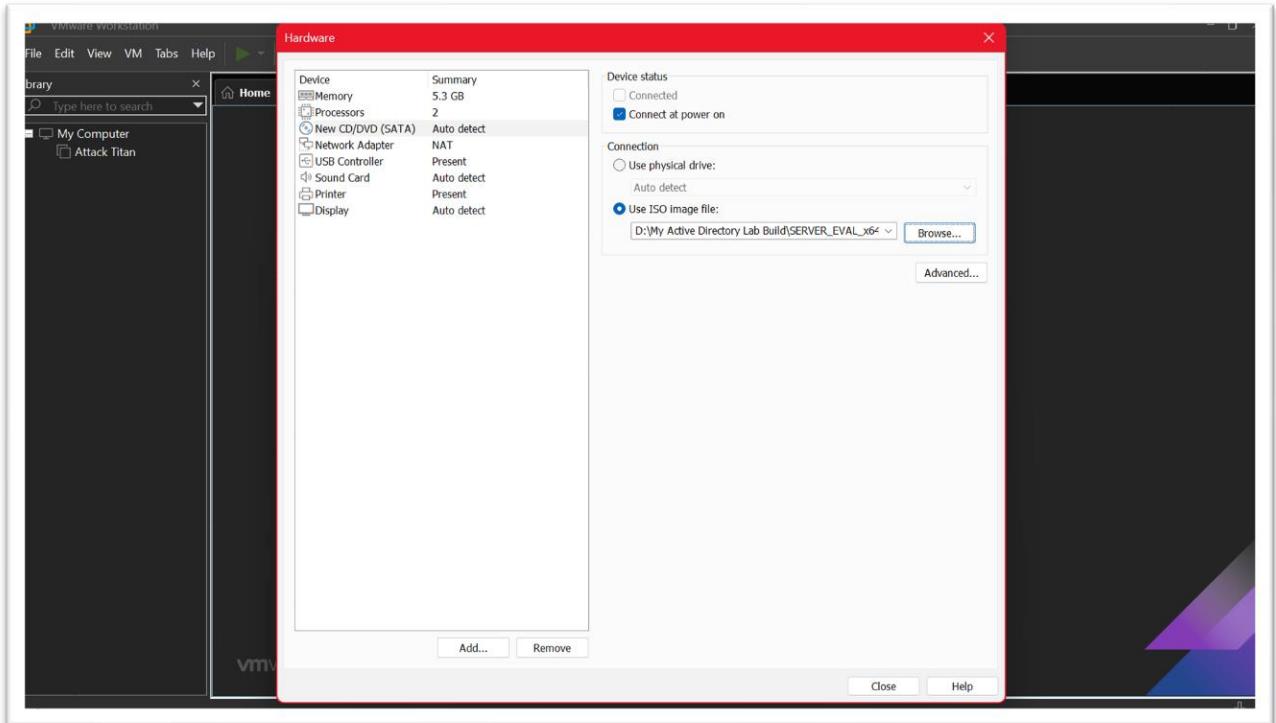


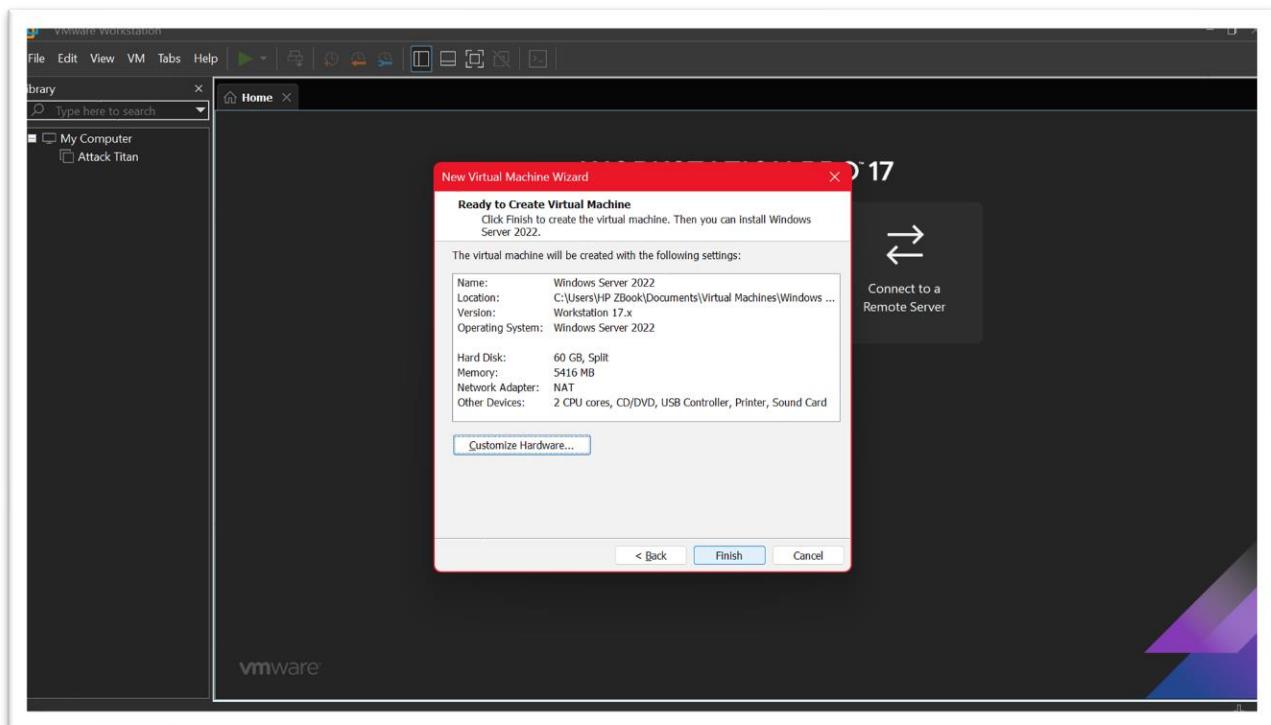
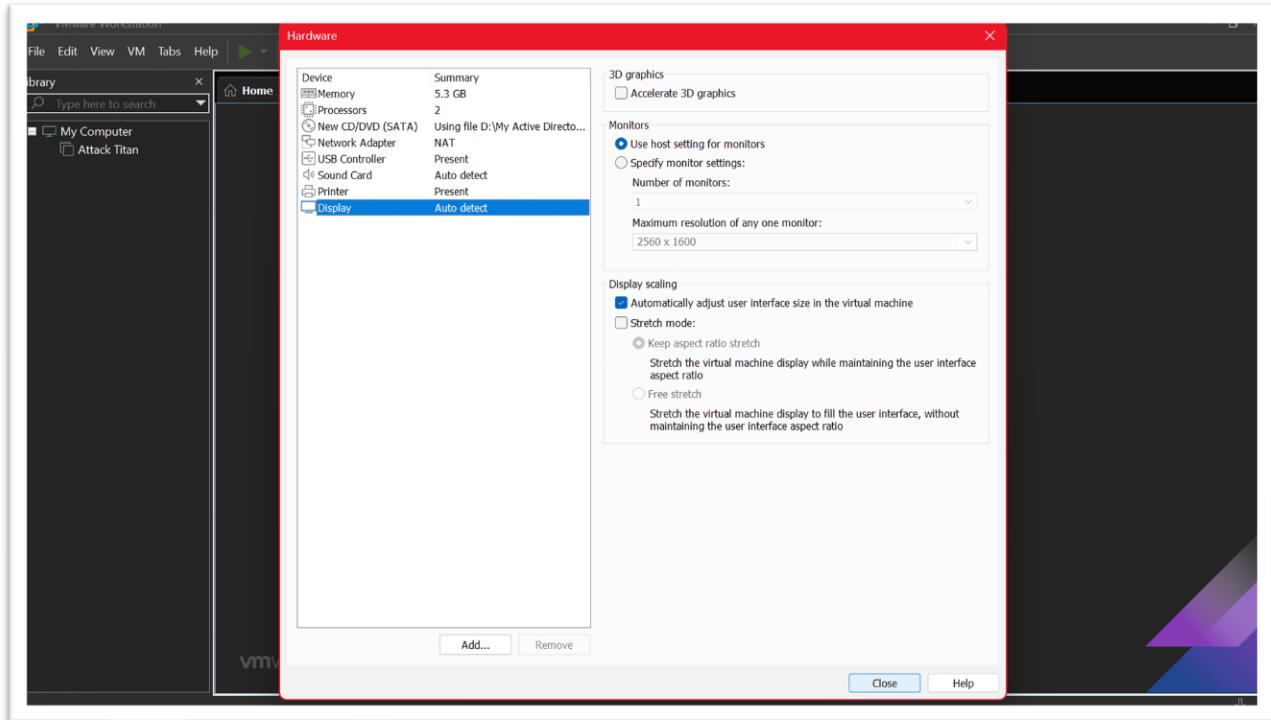


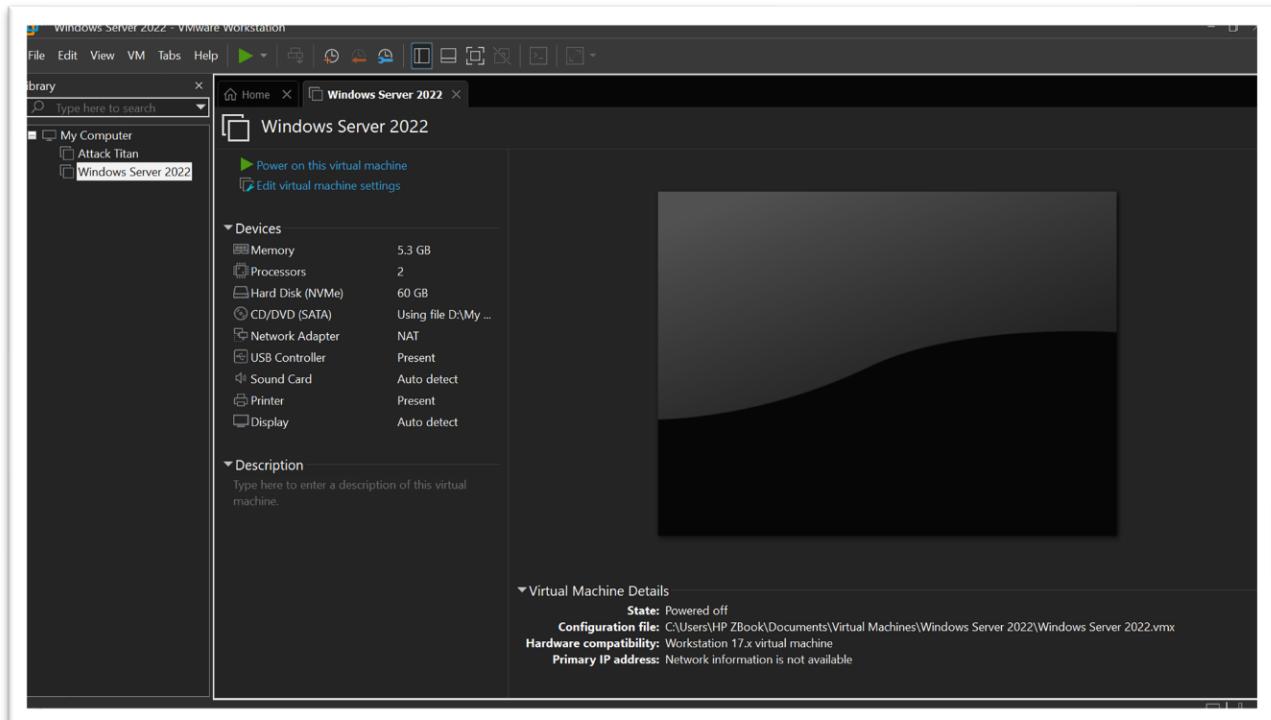


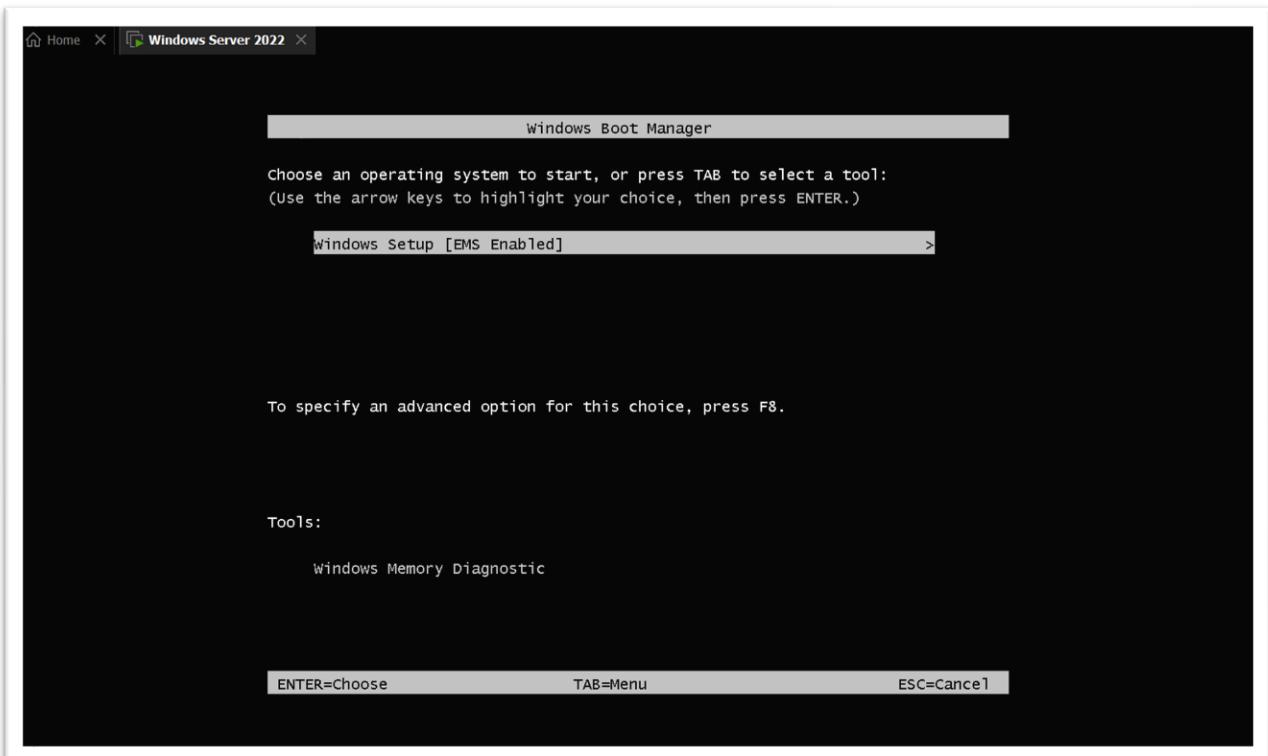
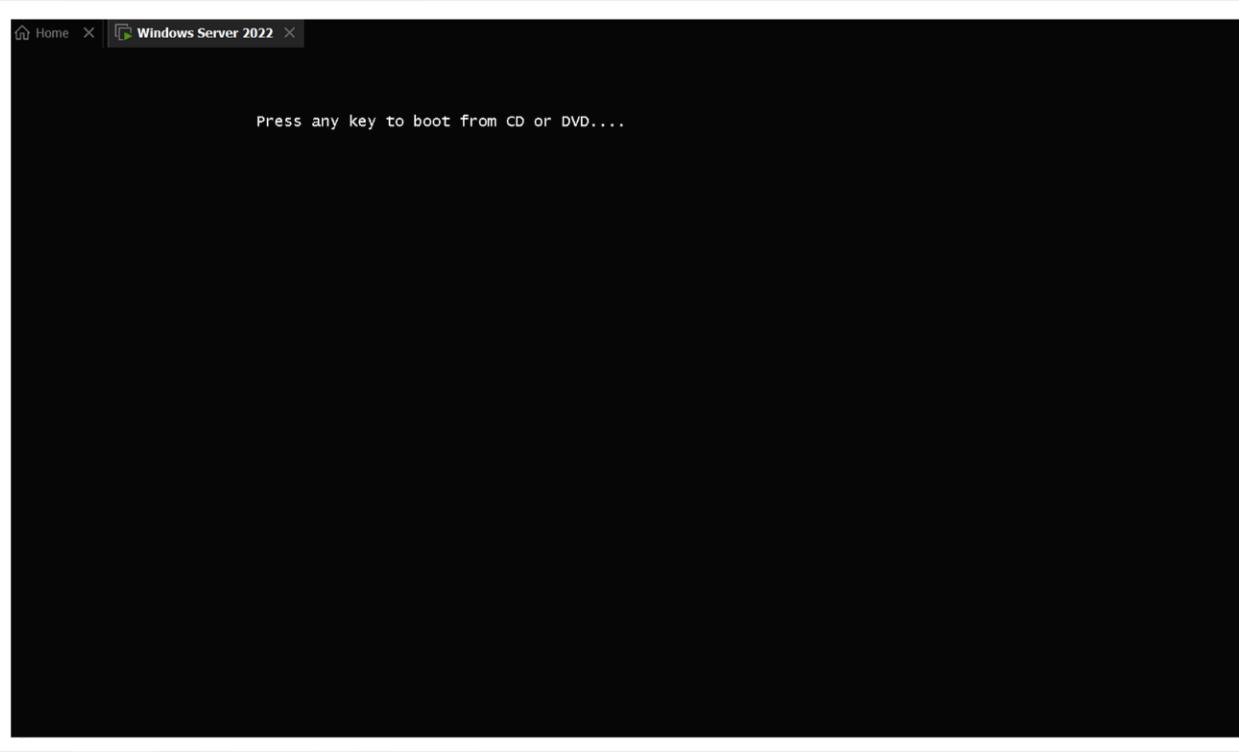


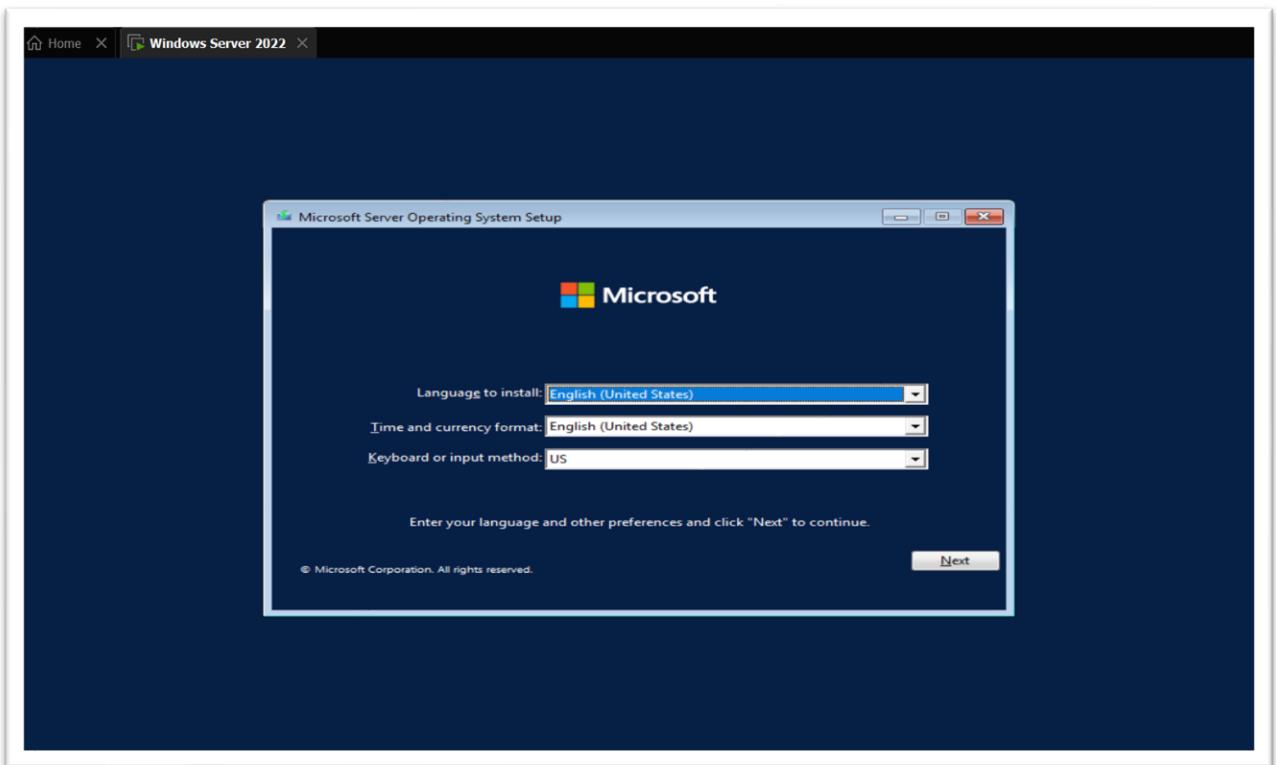
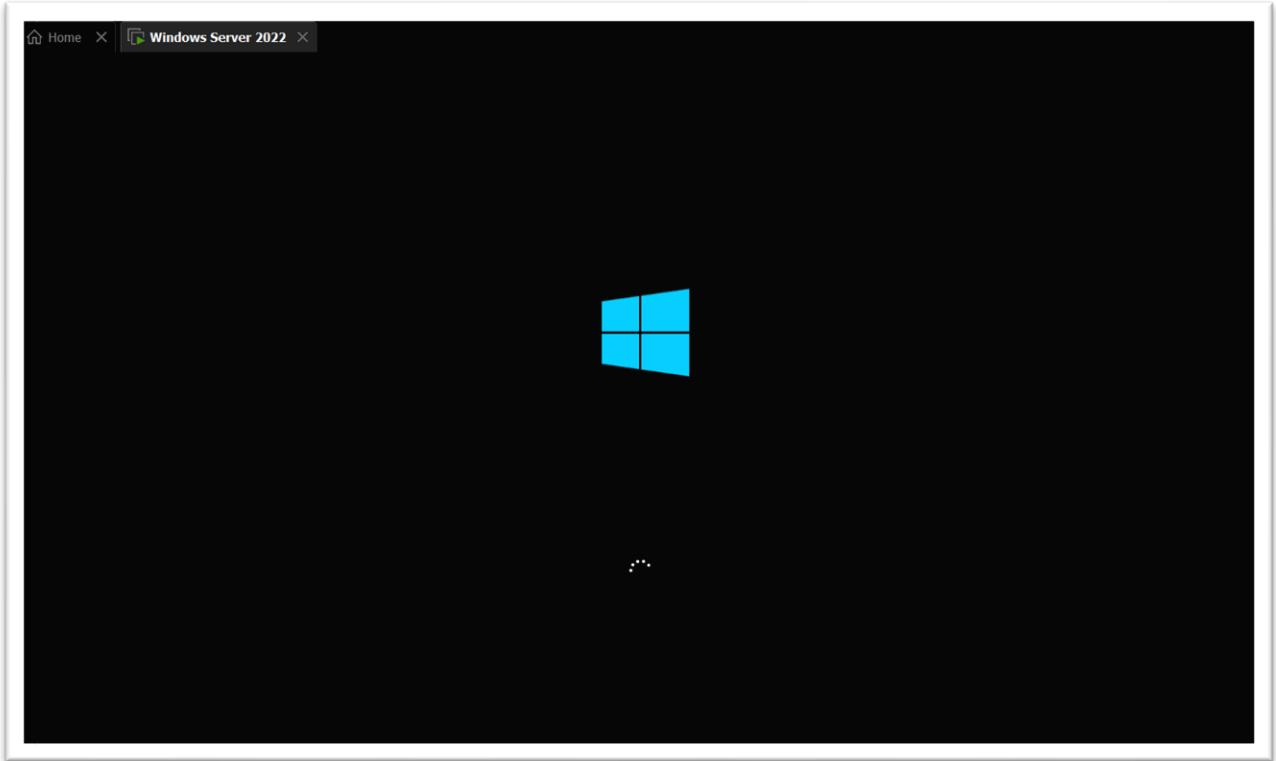


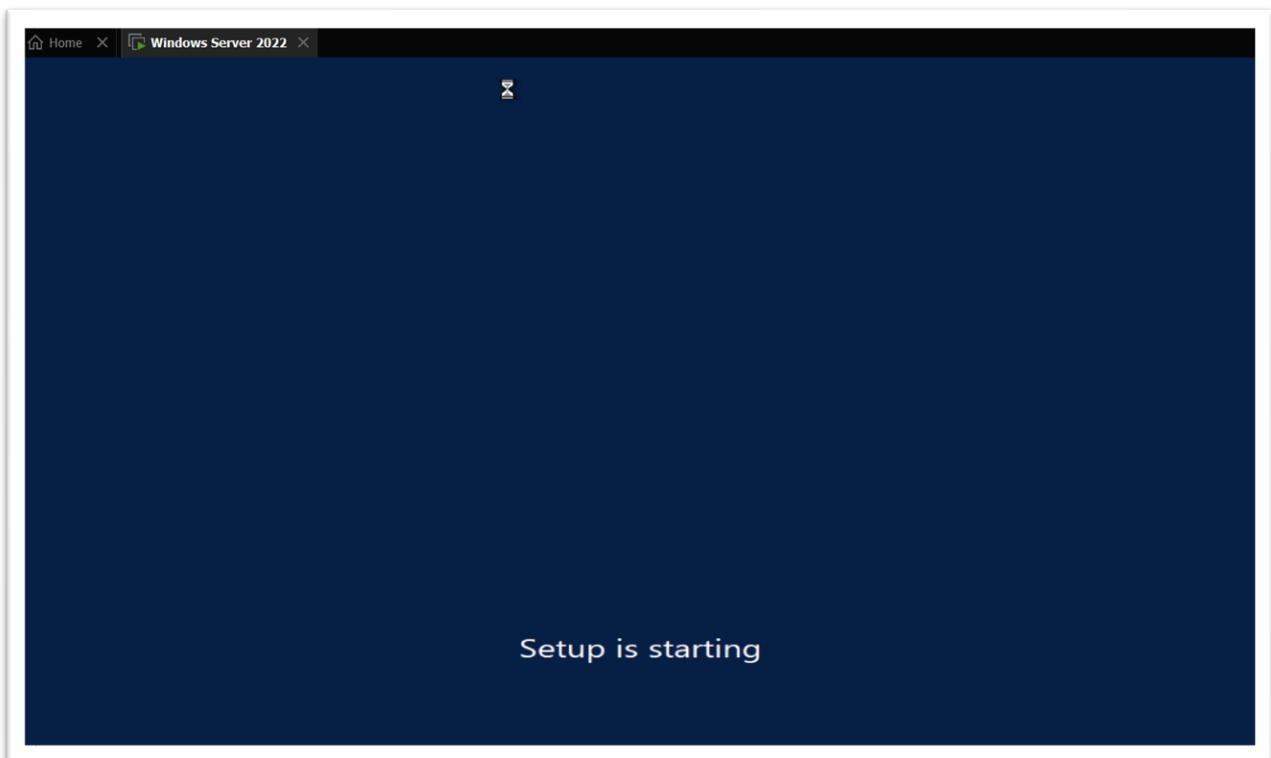
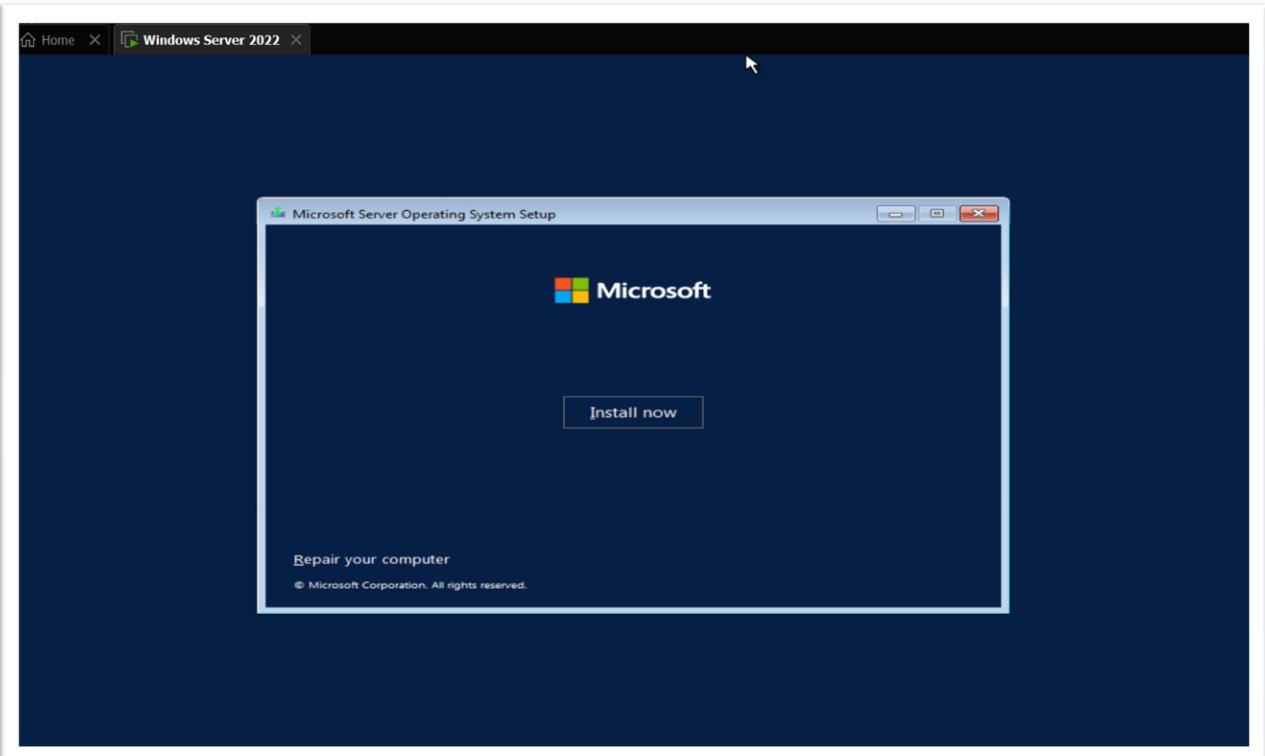


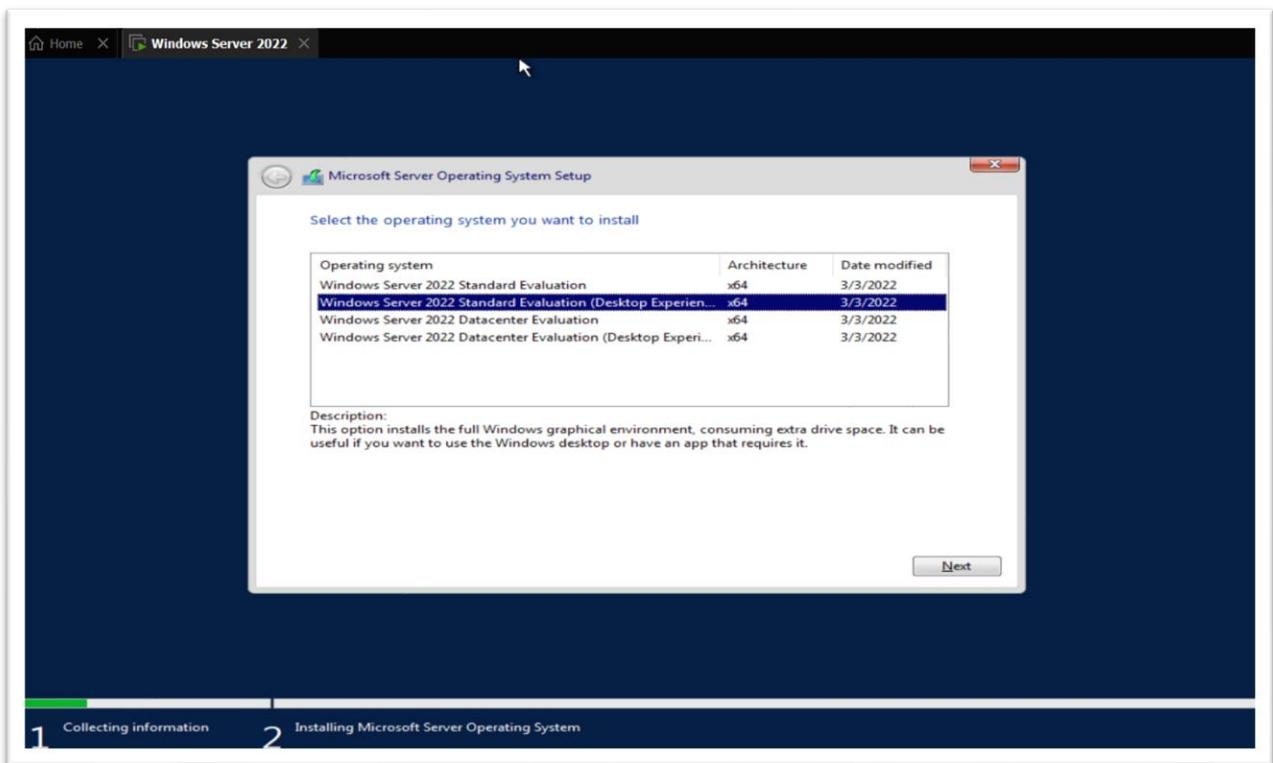
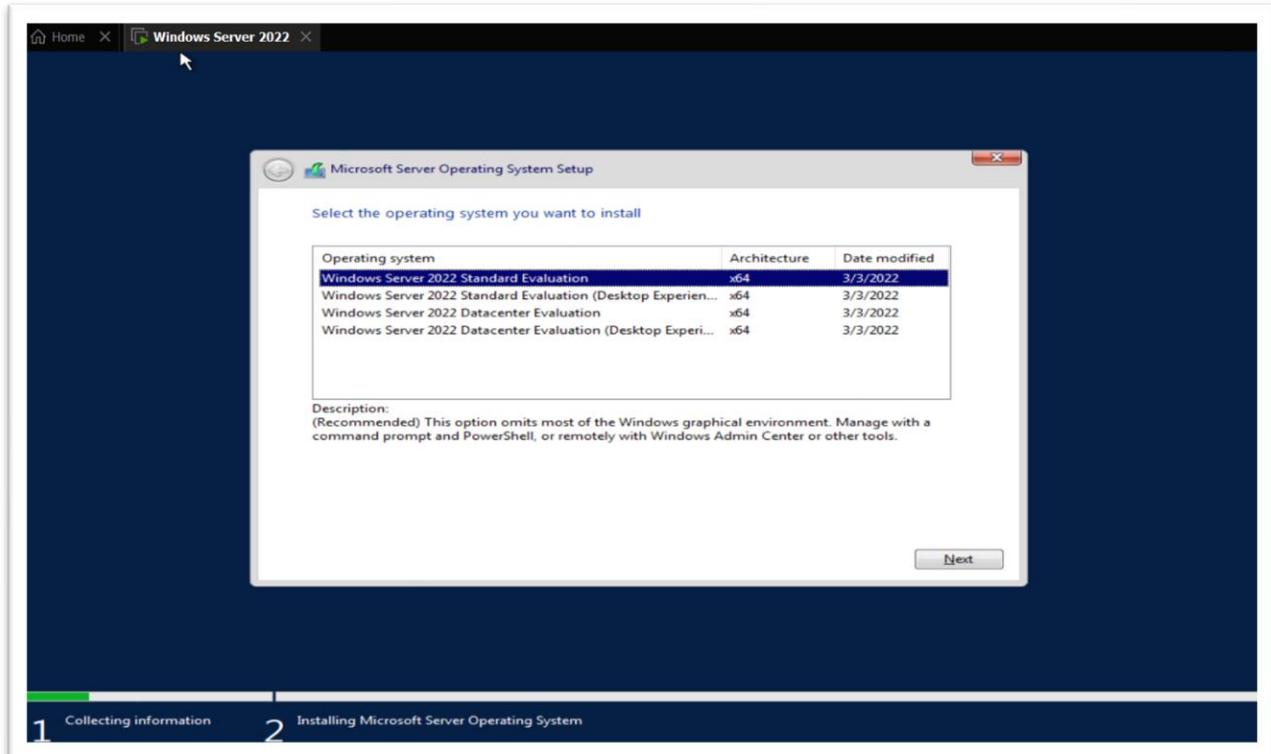


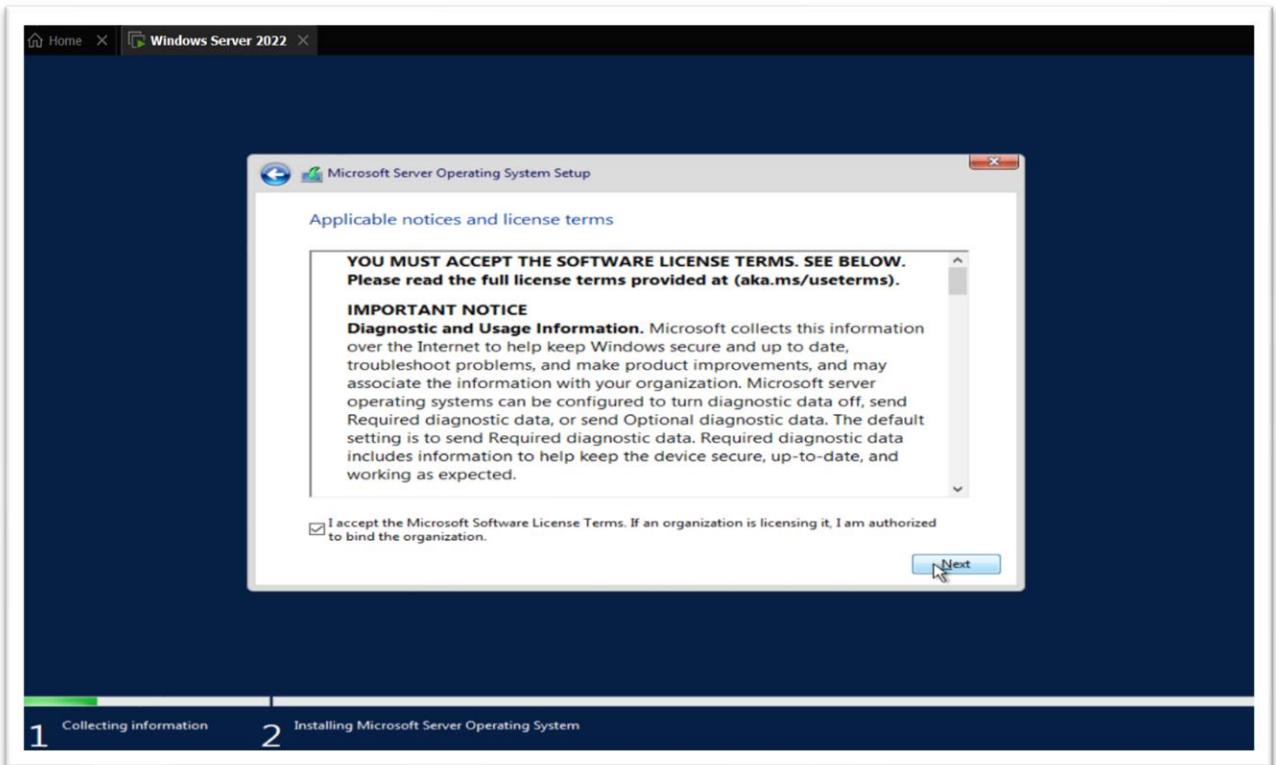
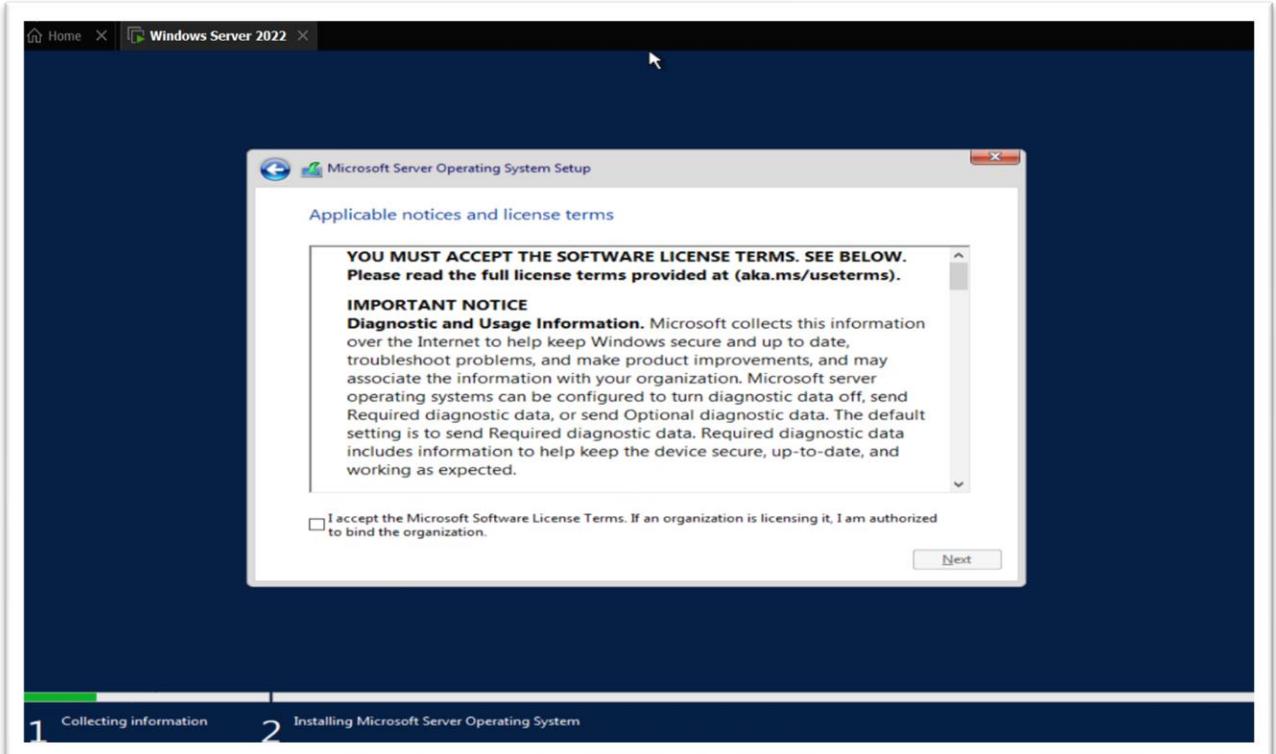


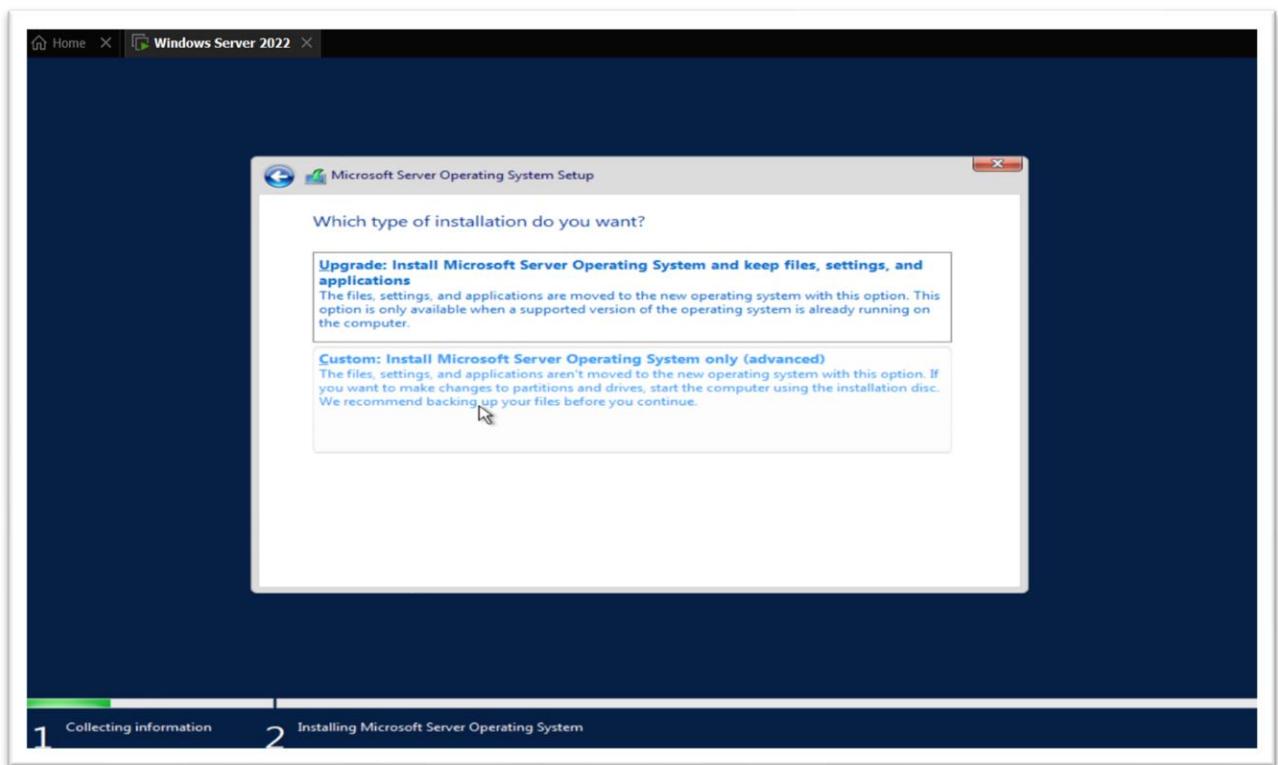
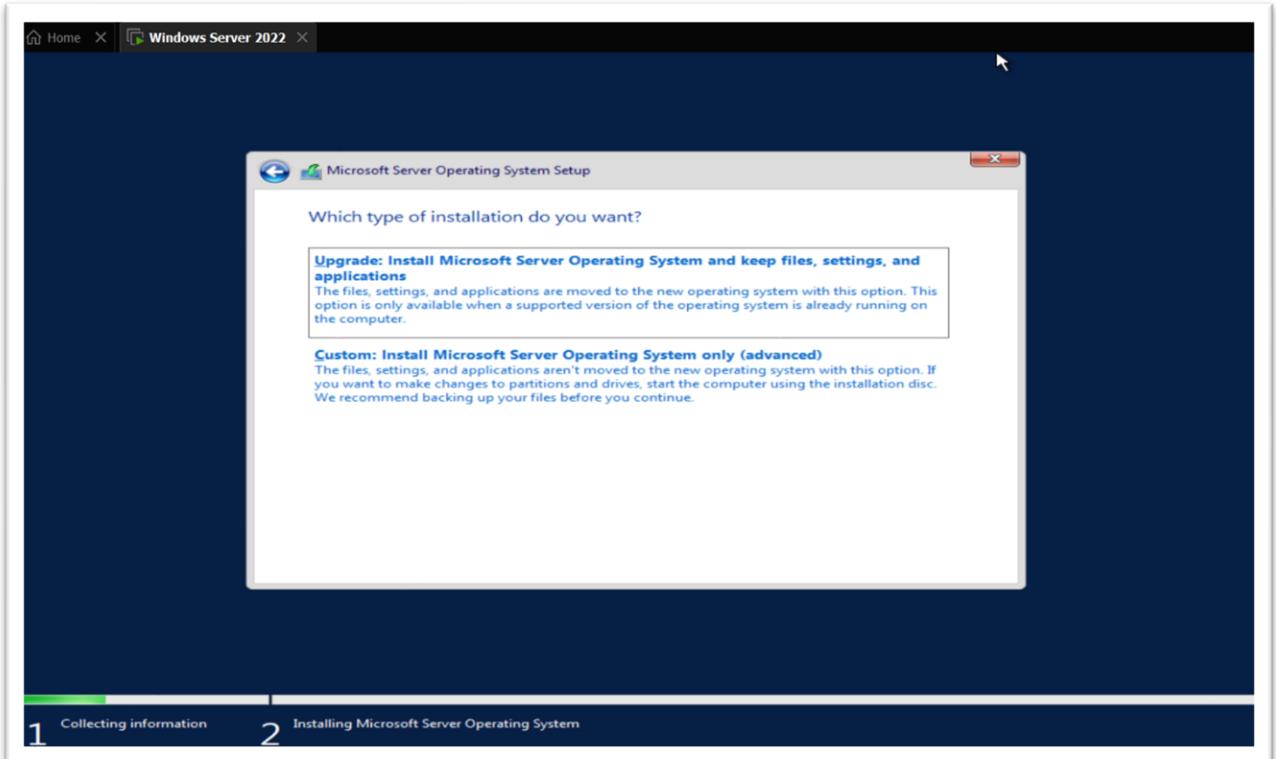


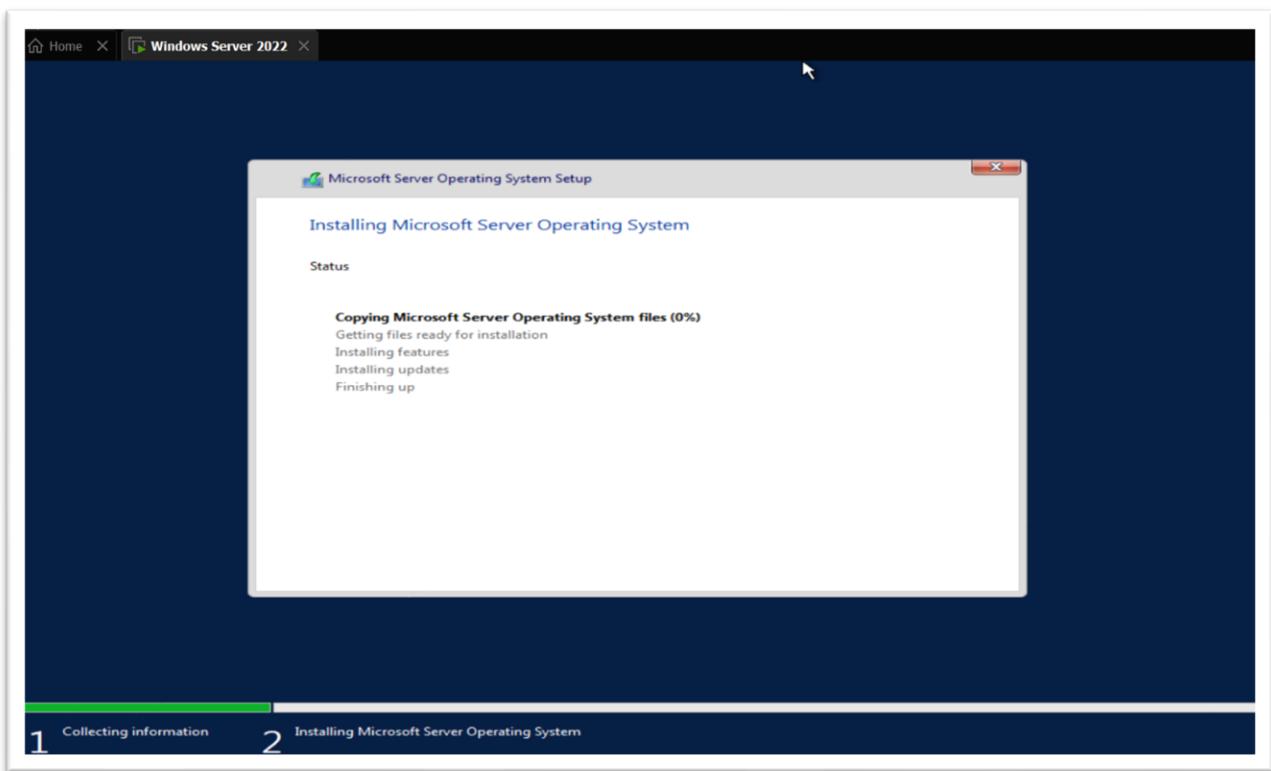
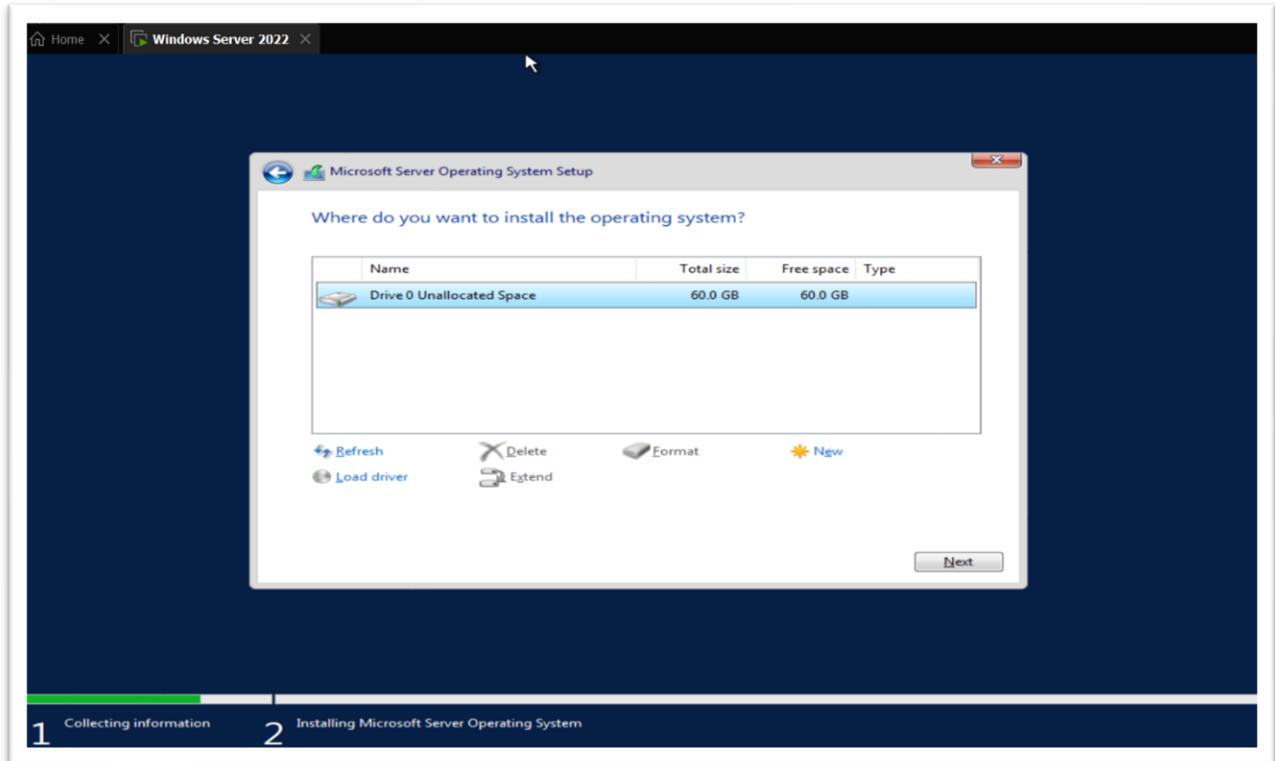


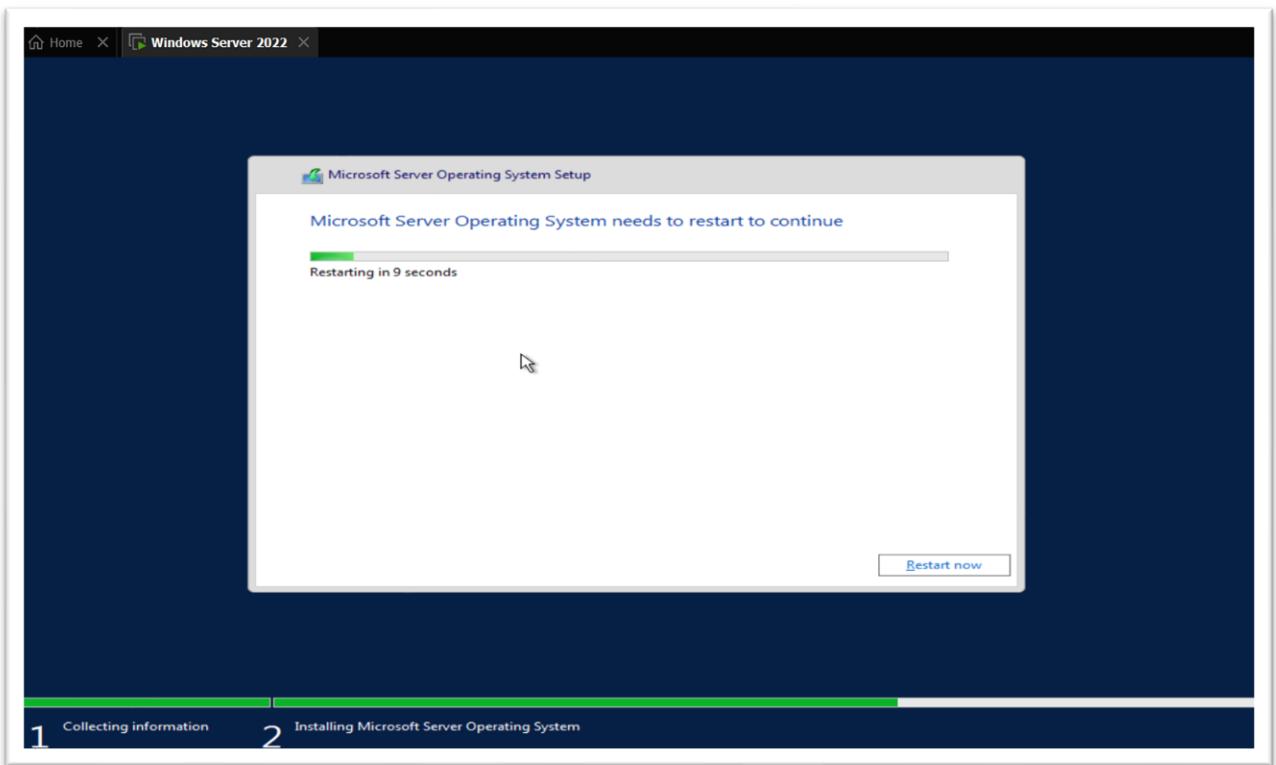
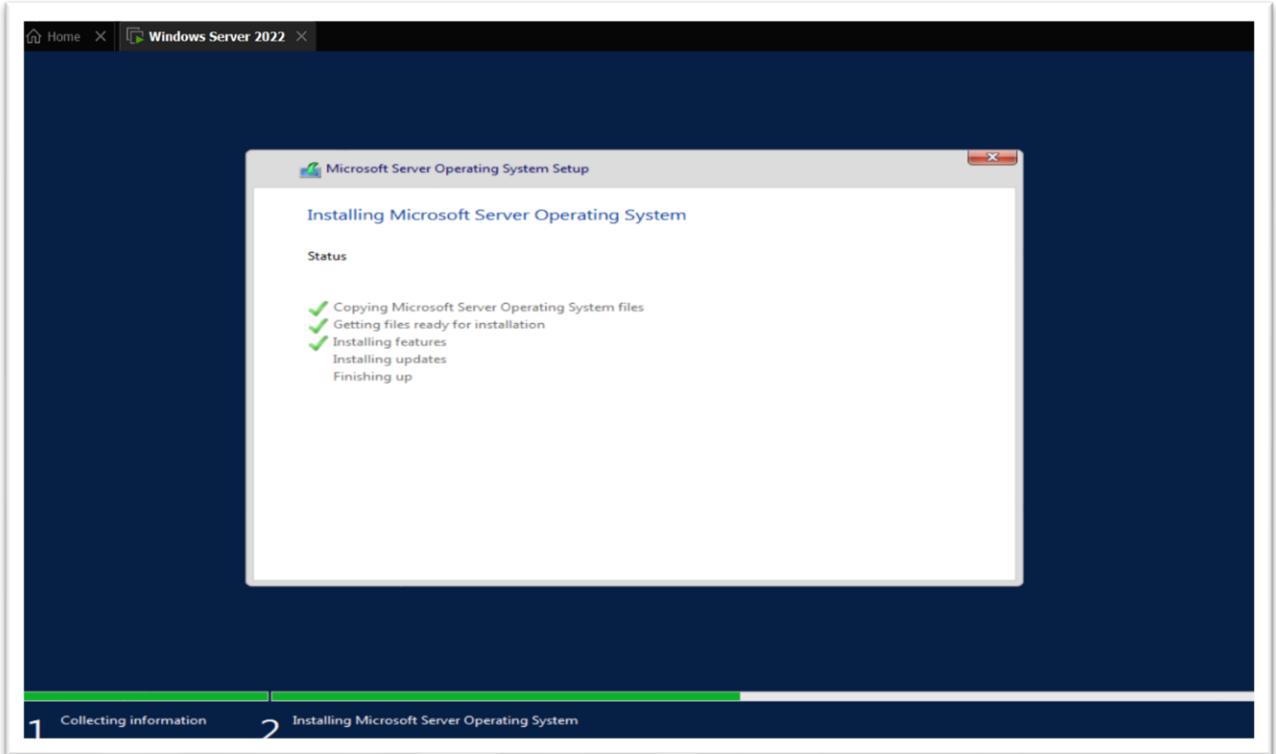


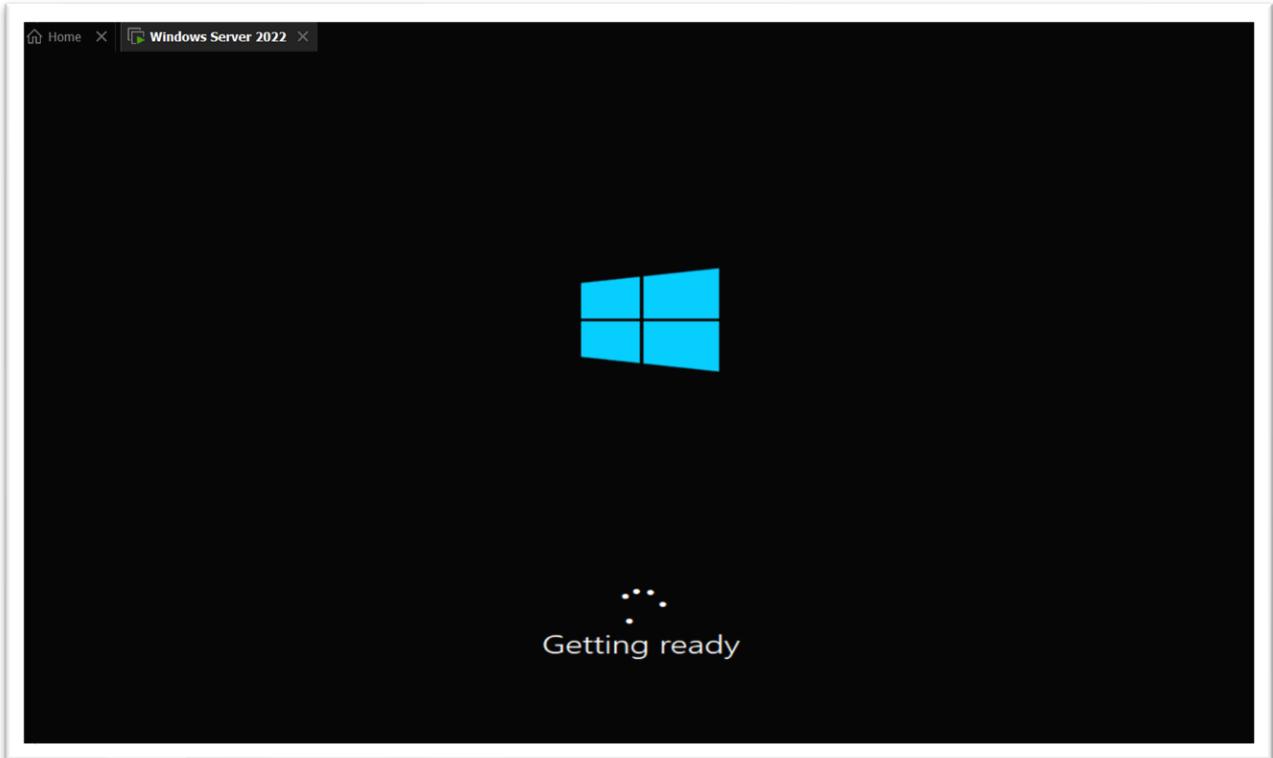
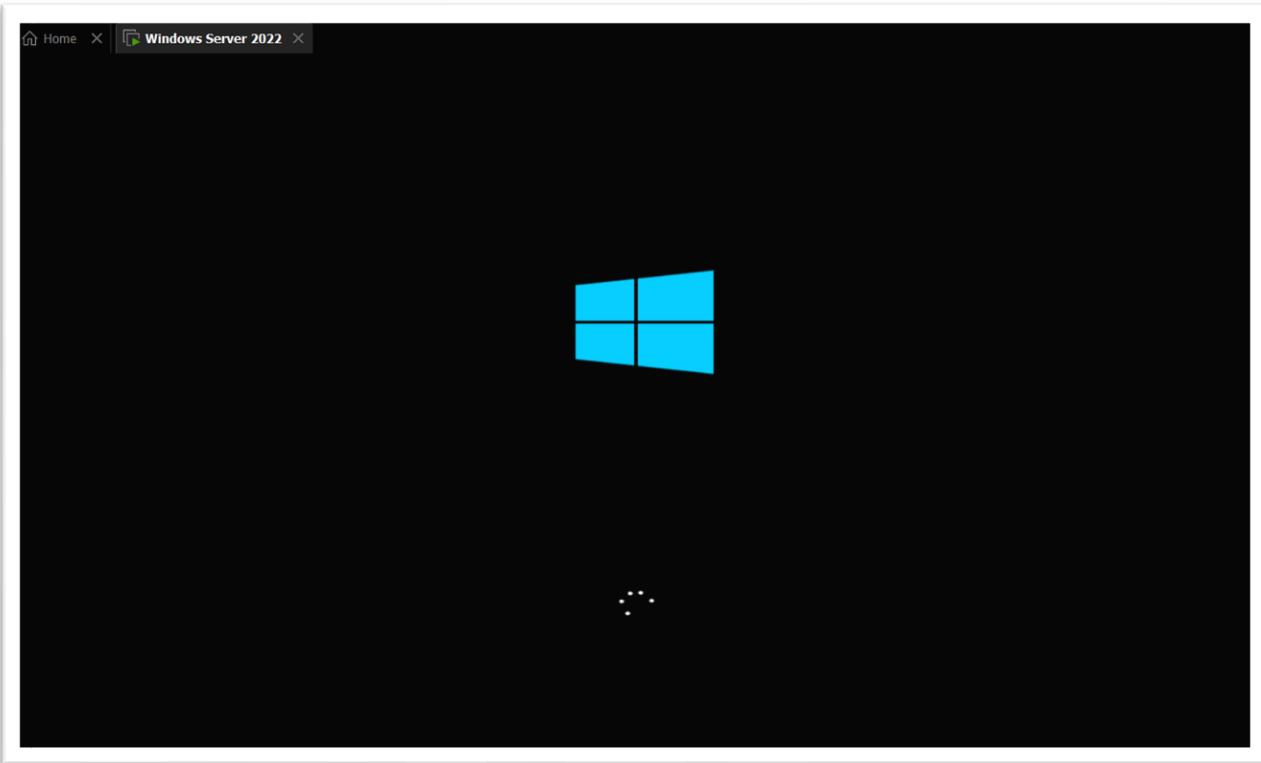


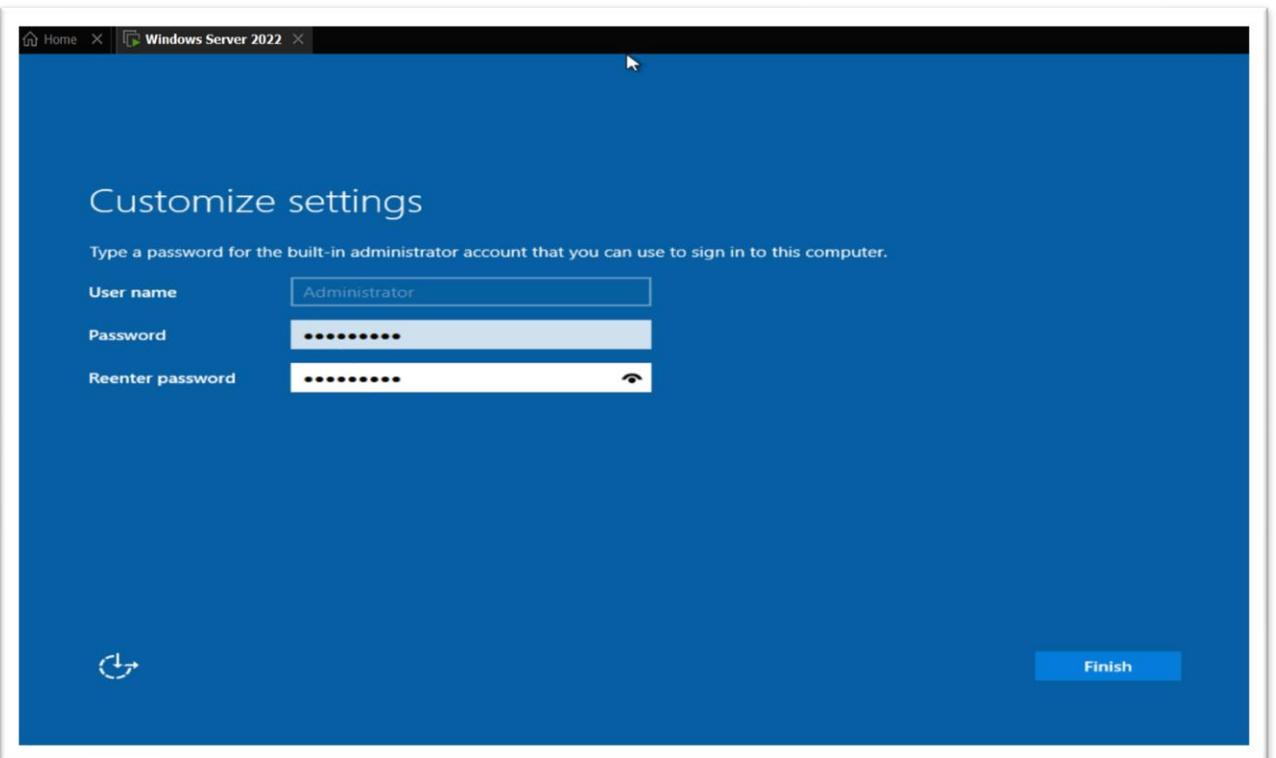
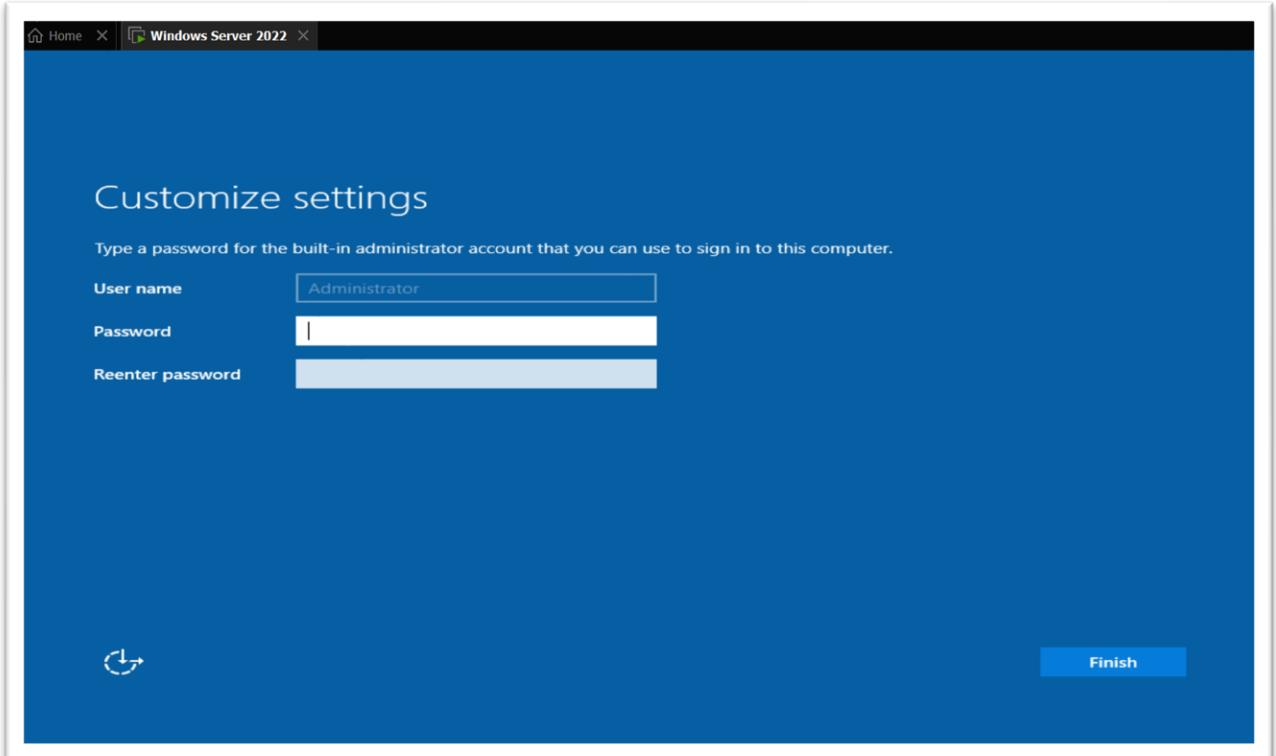


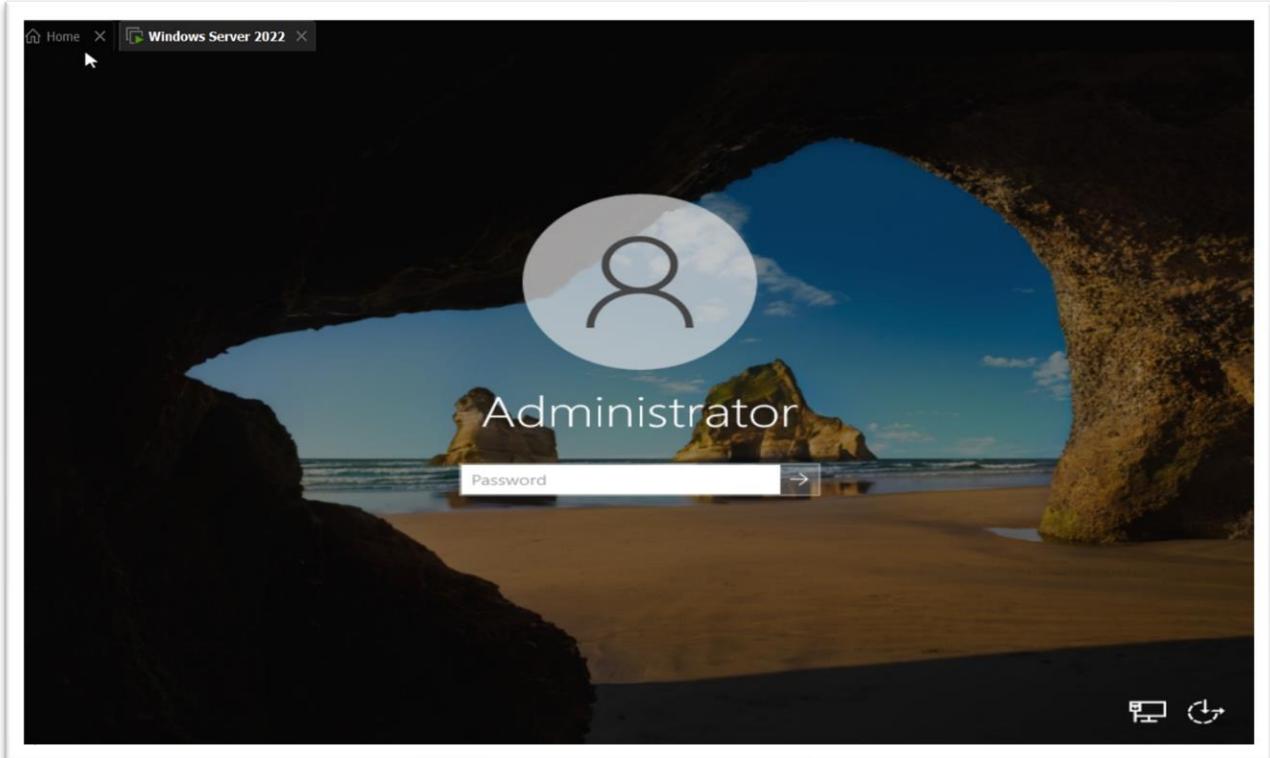


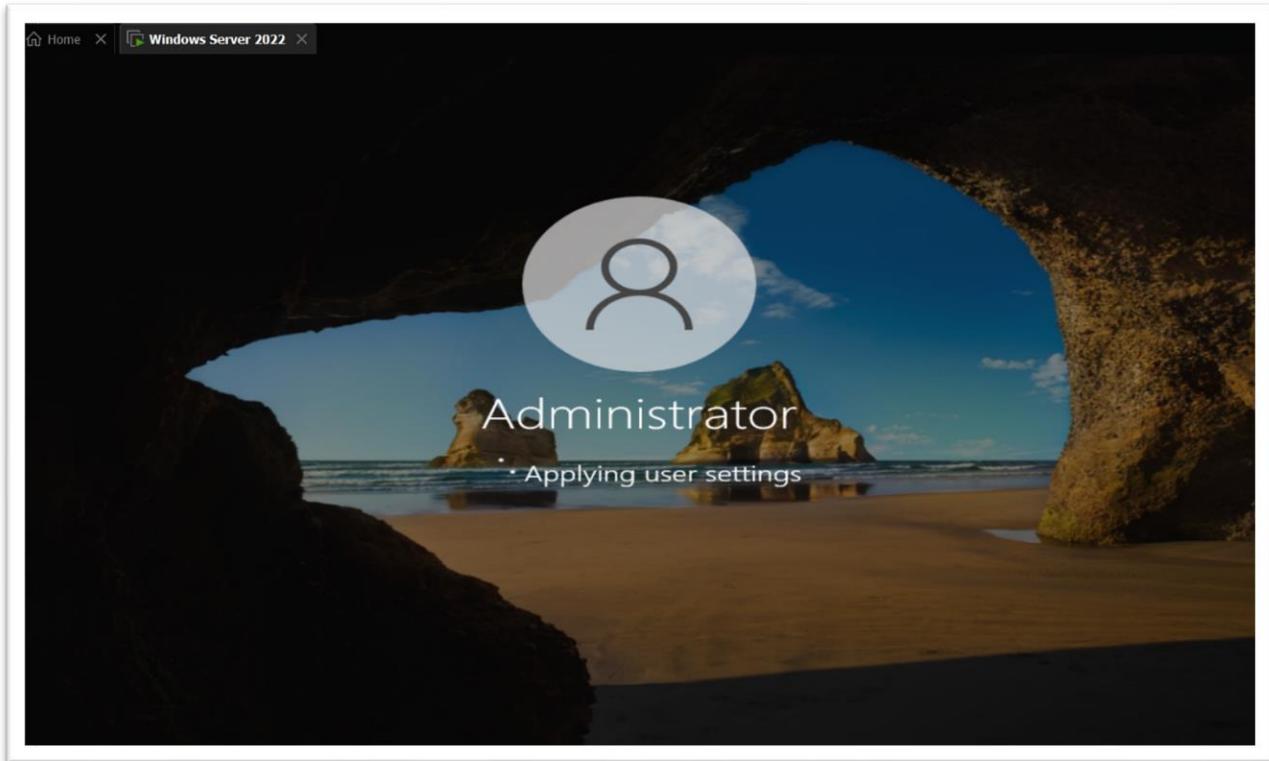
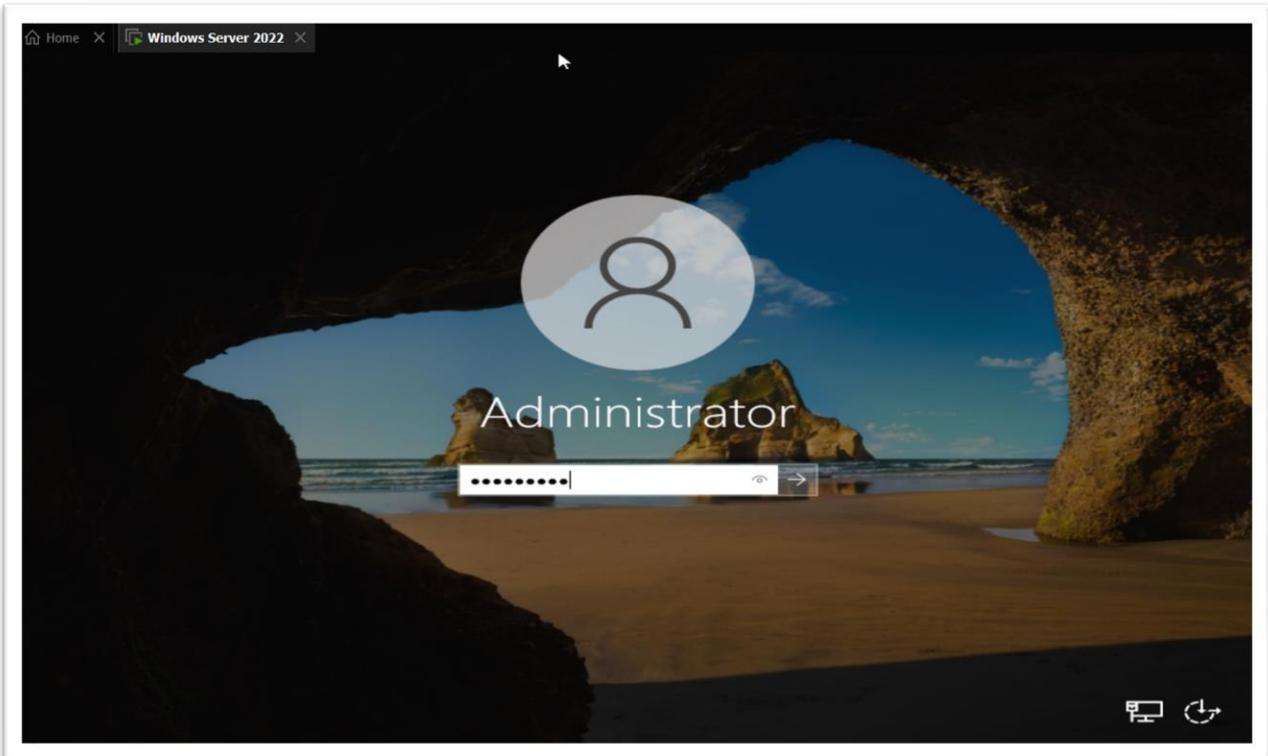


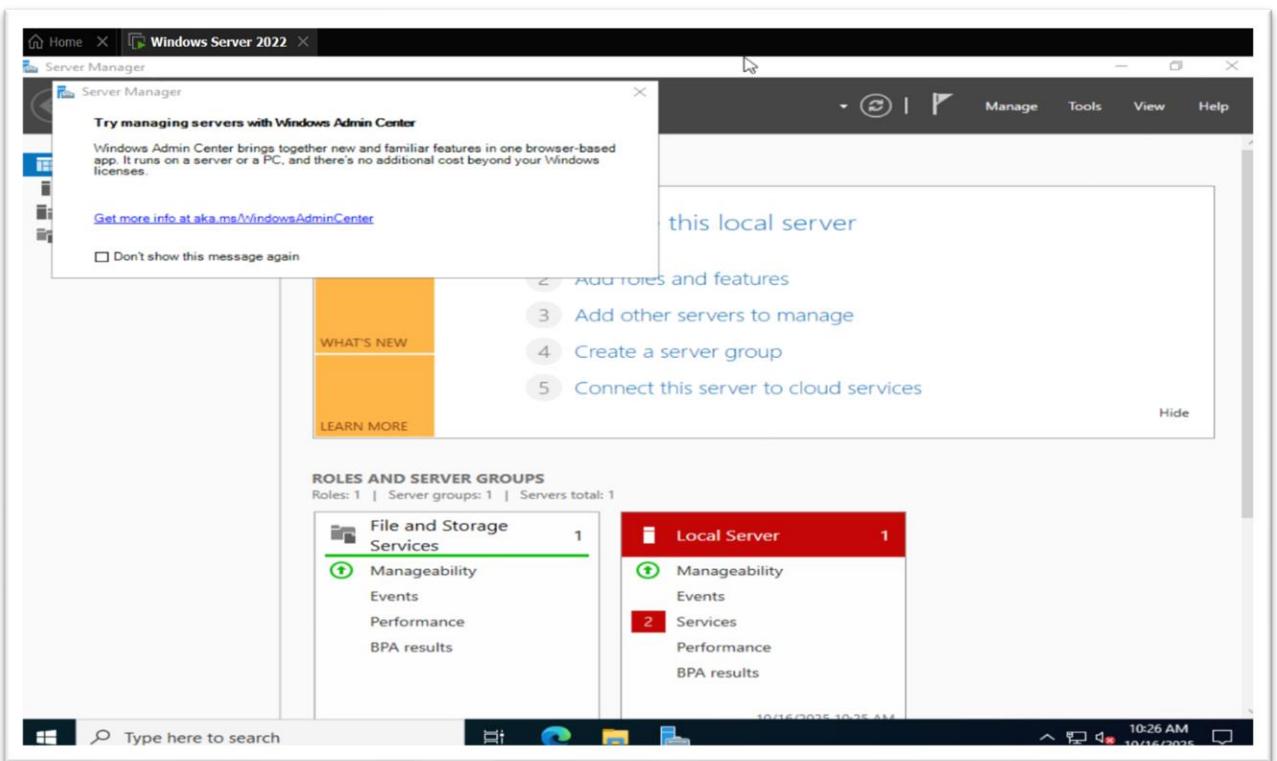
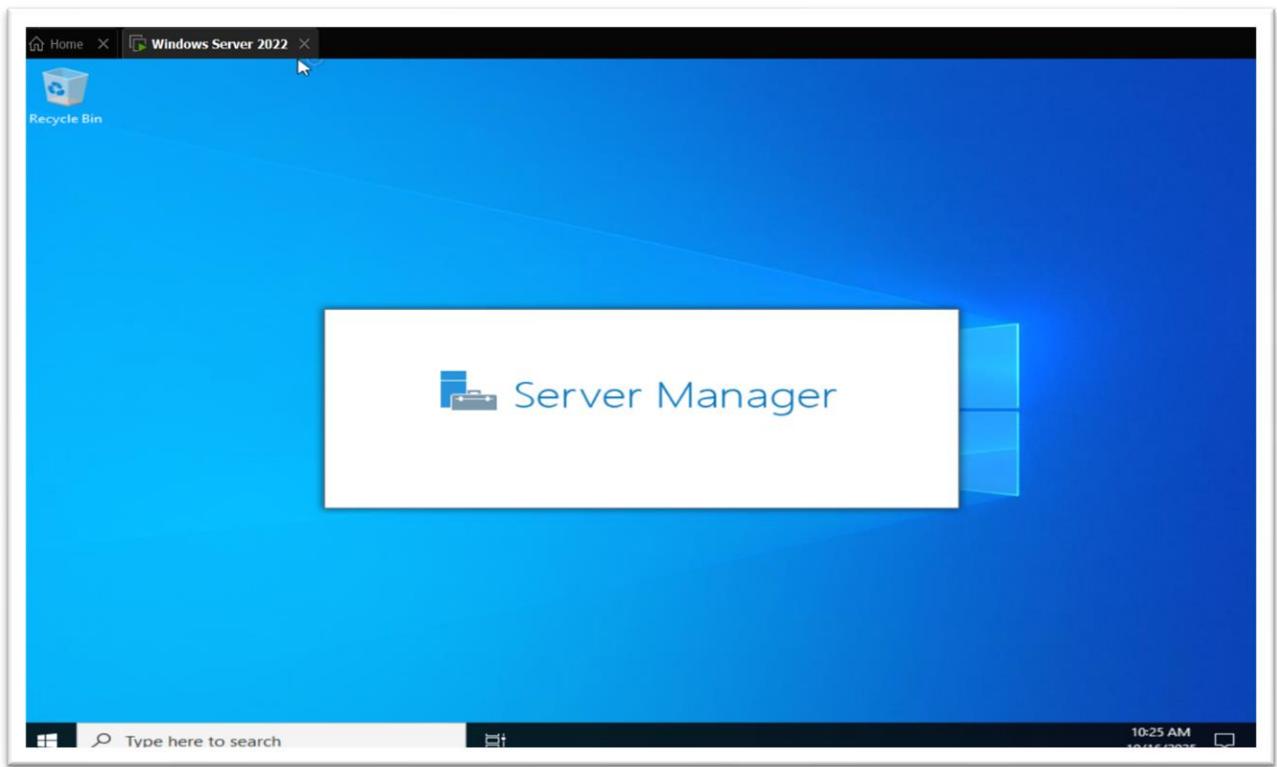




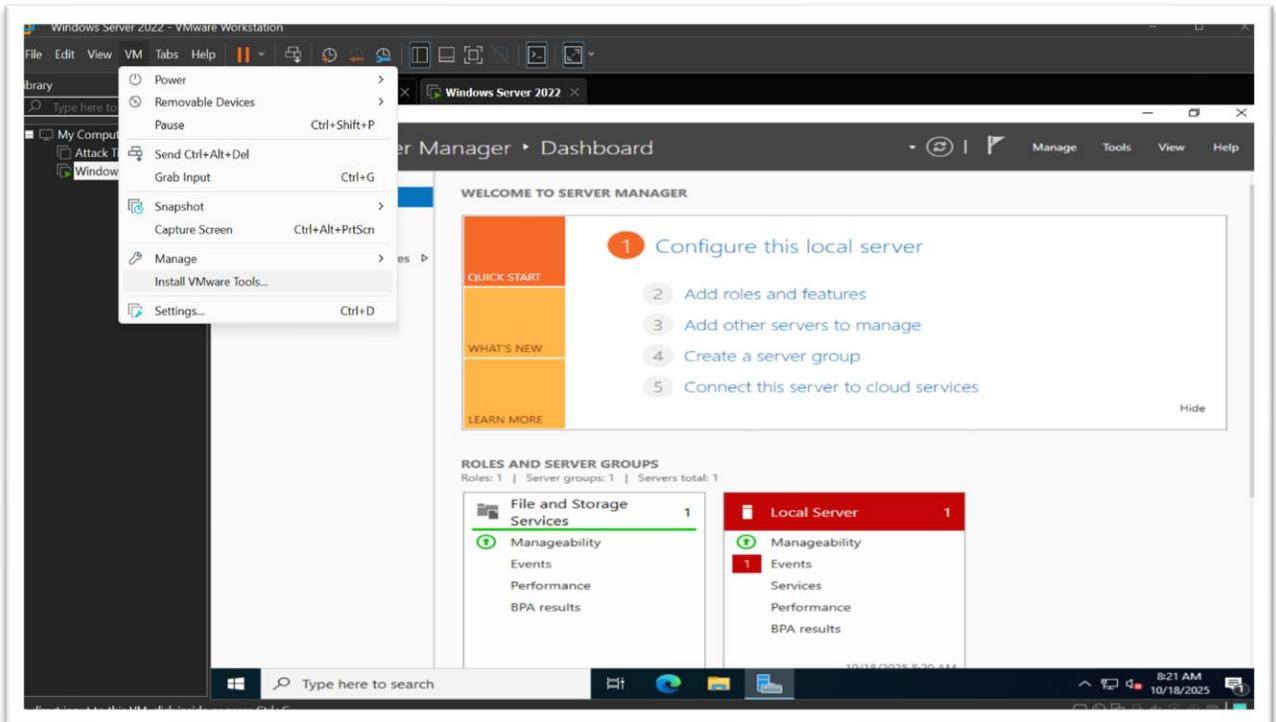
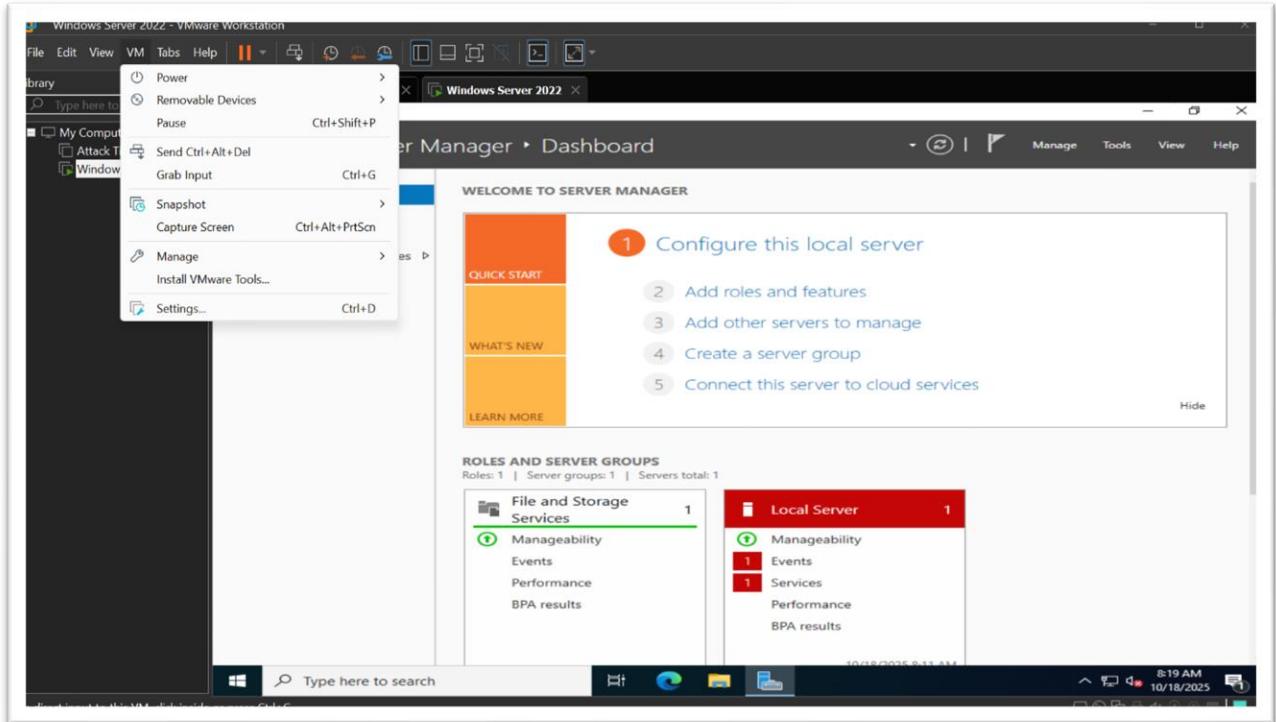


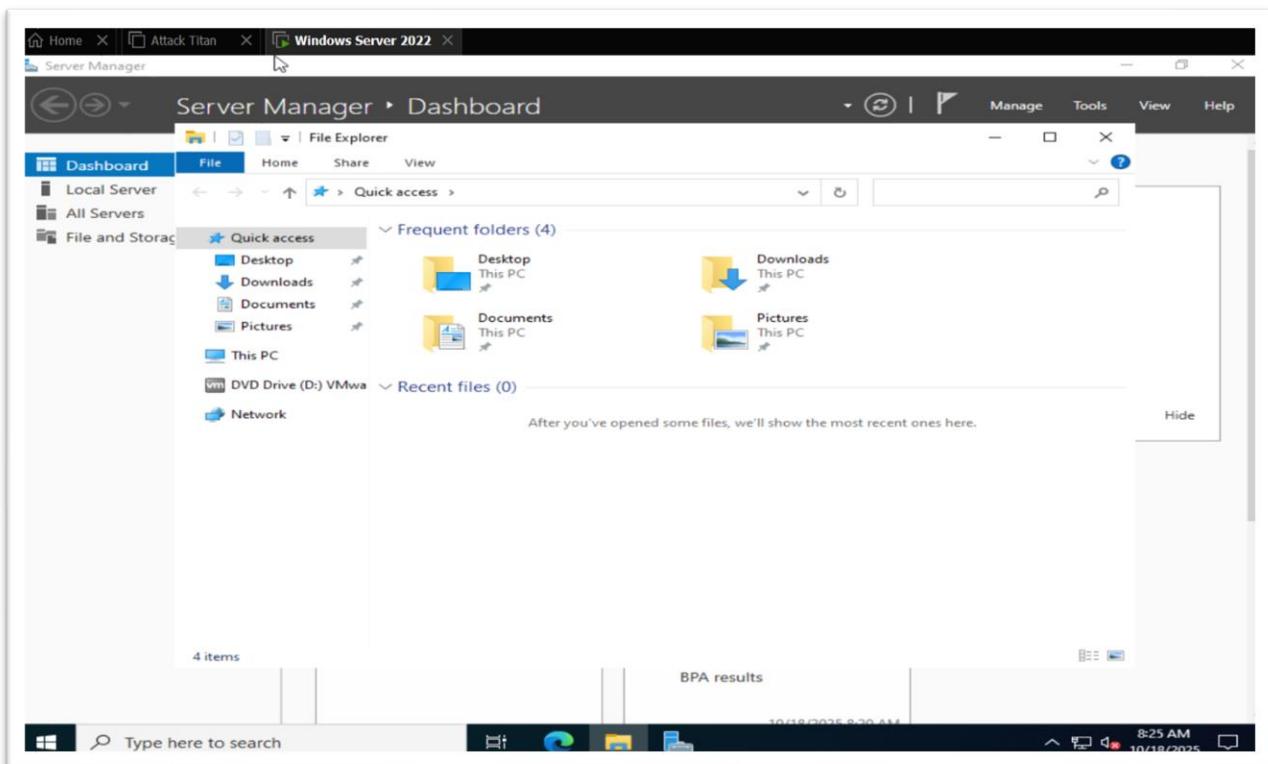
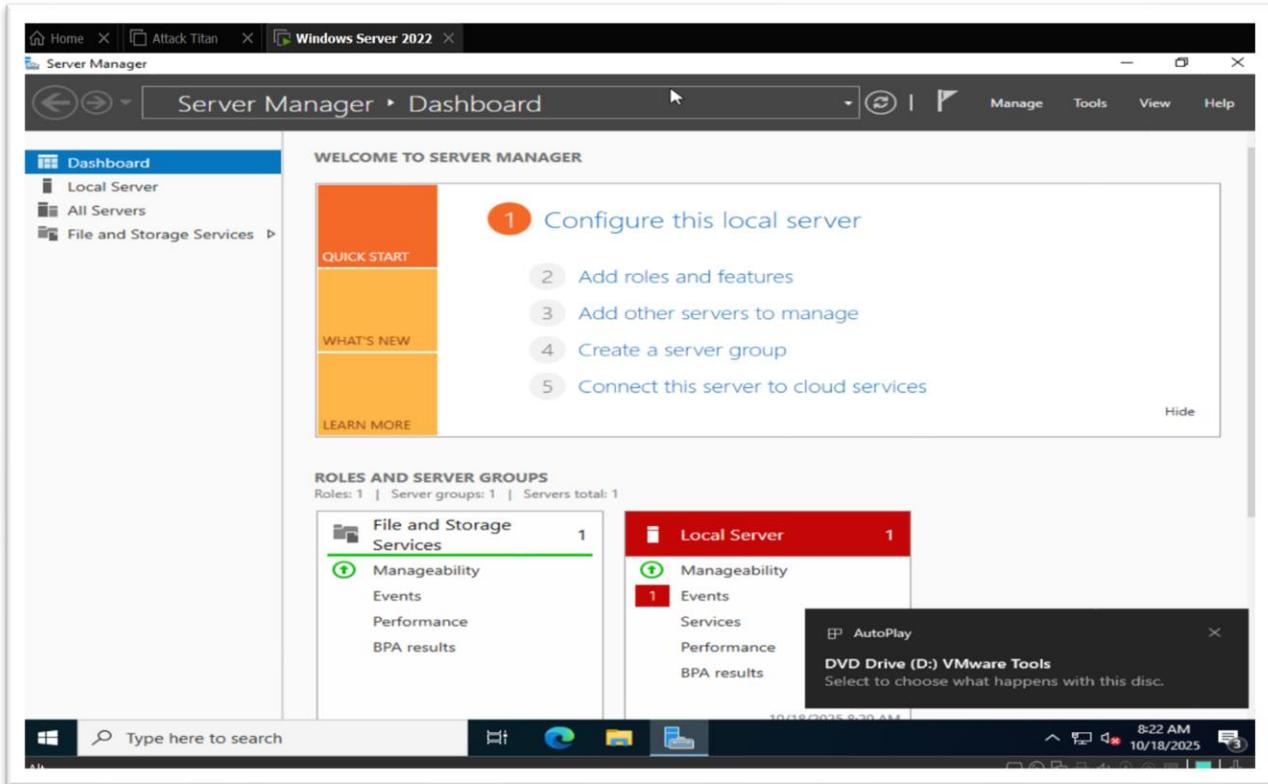


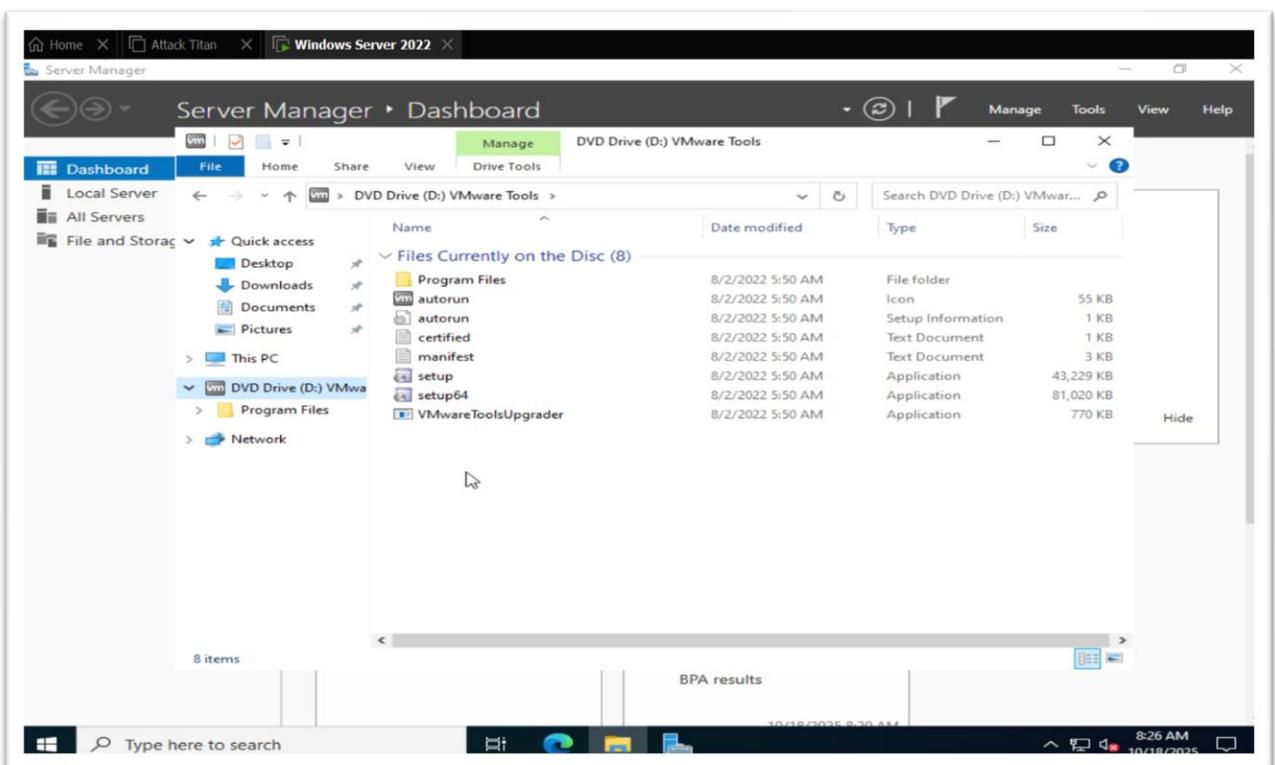
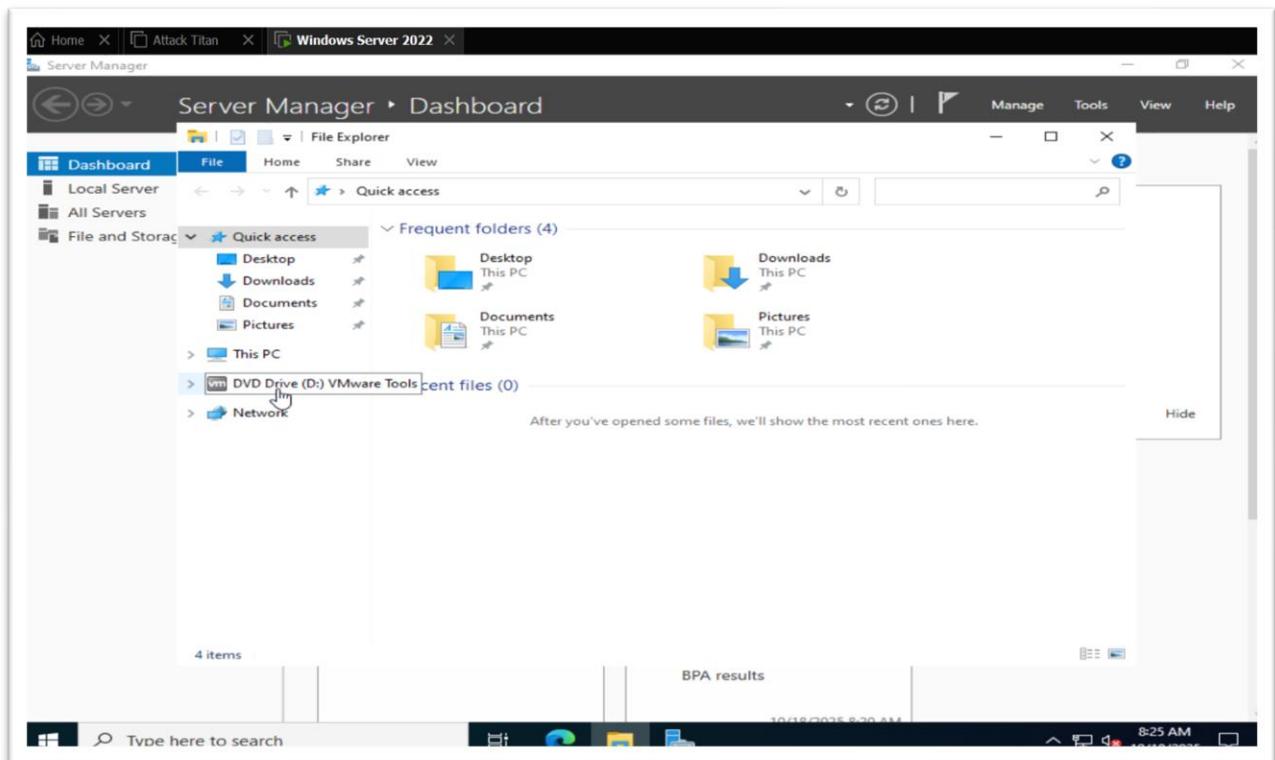


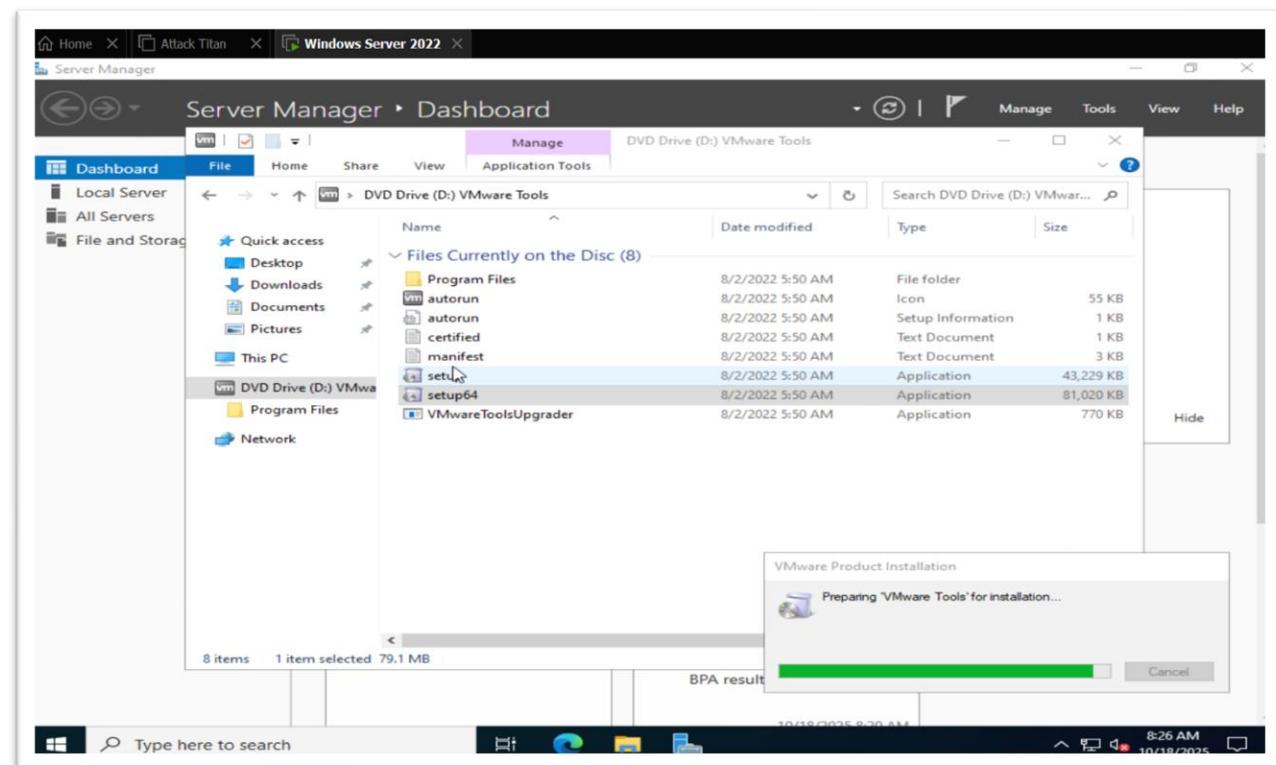
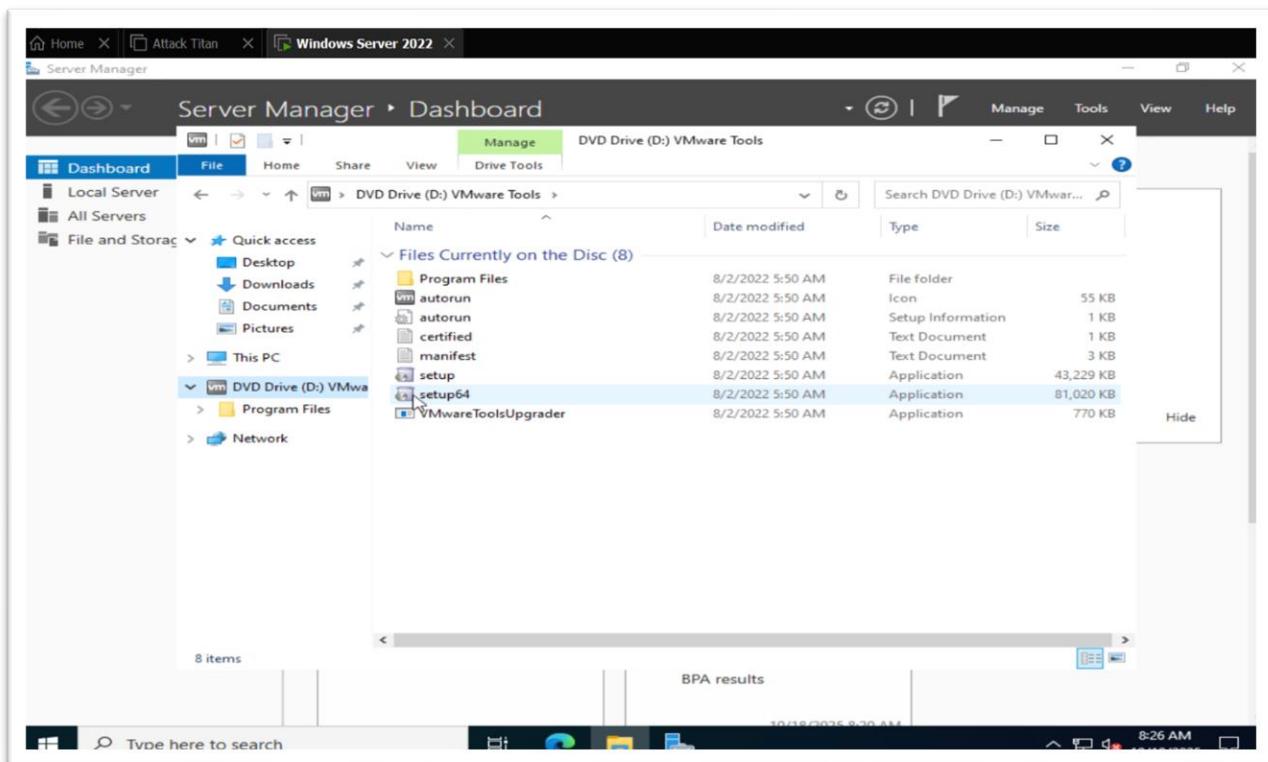


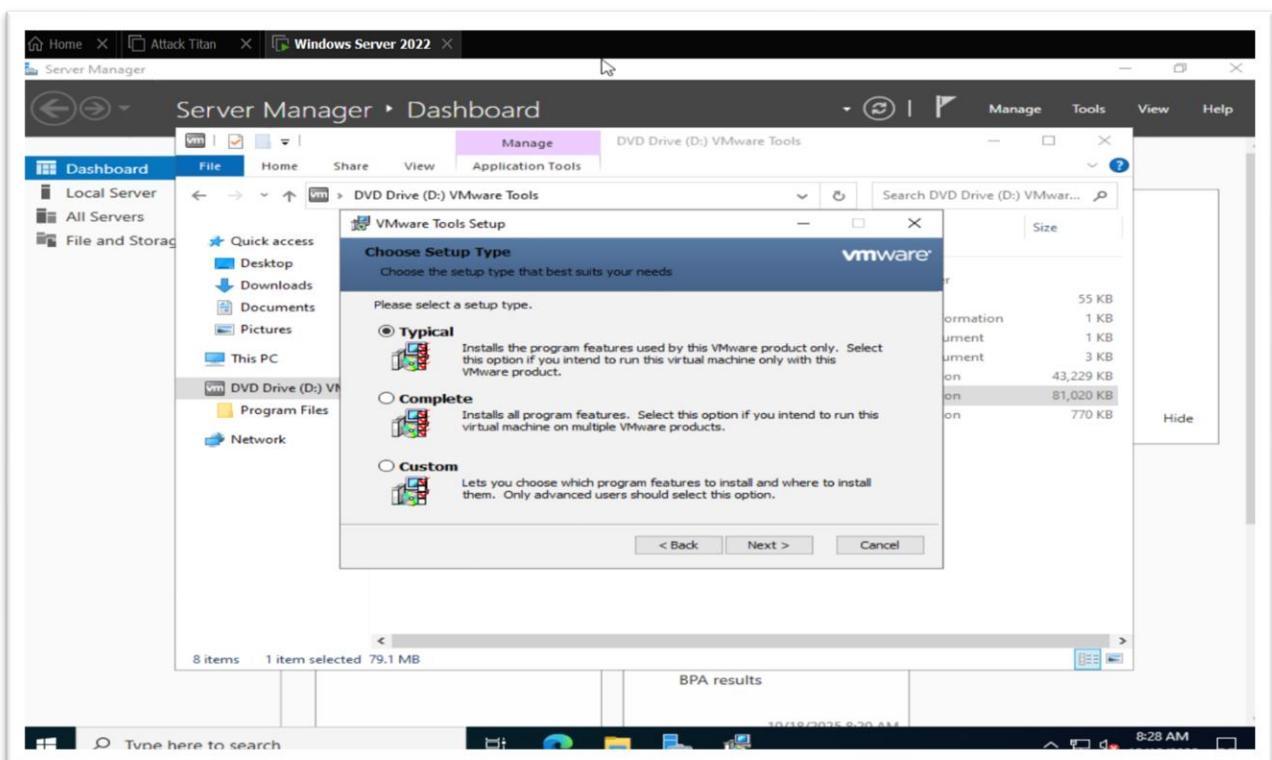
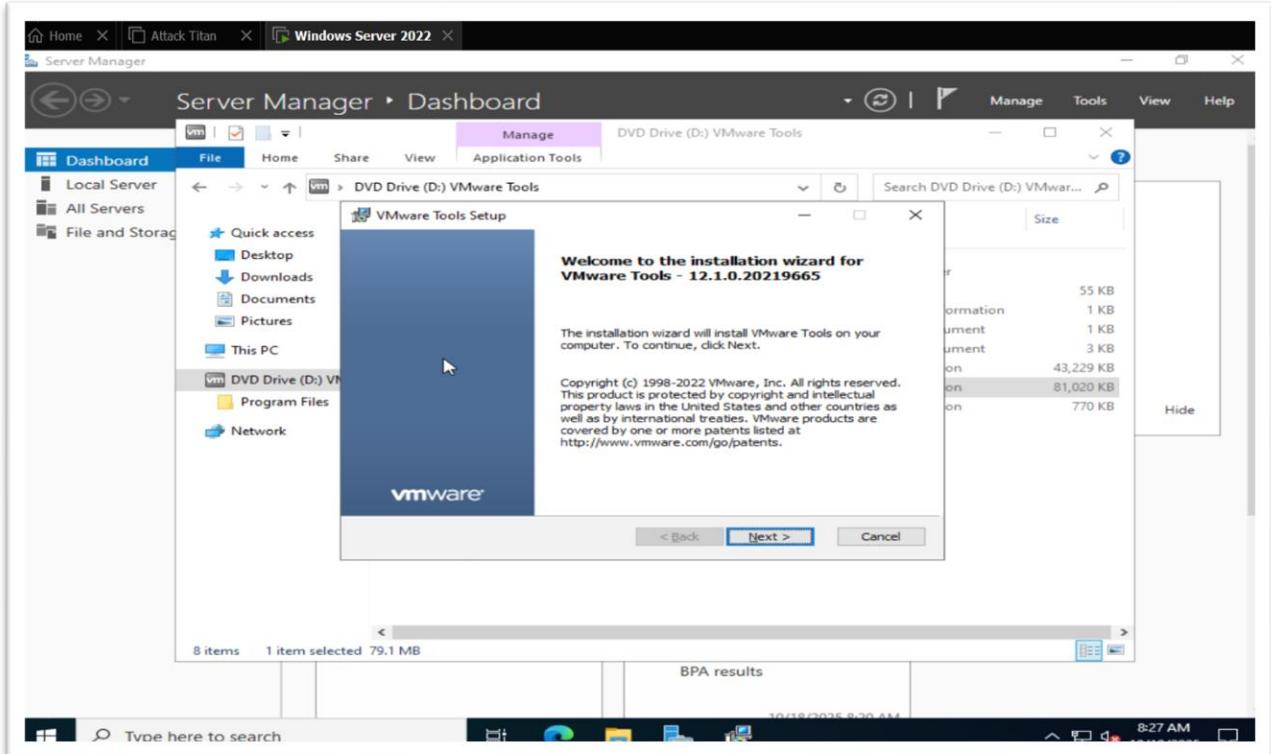
- Install VMware Tools

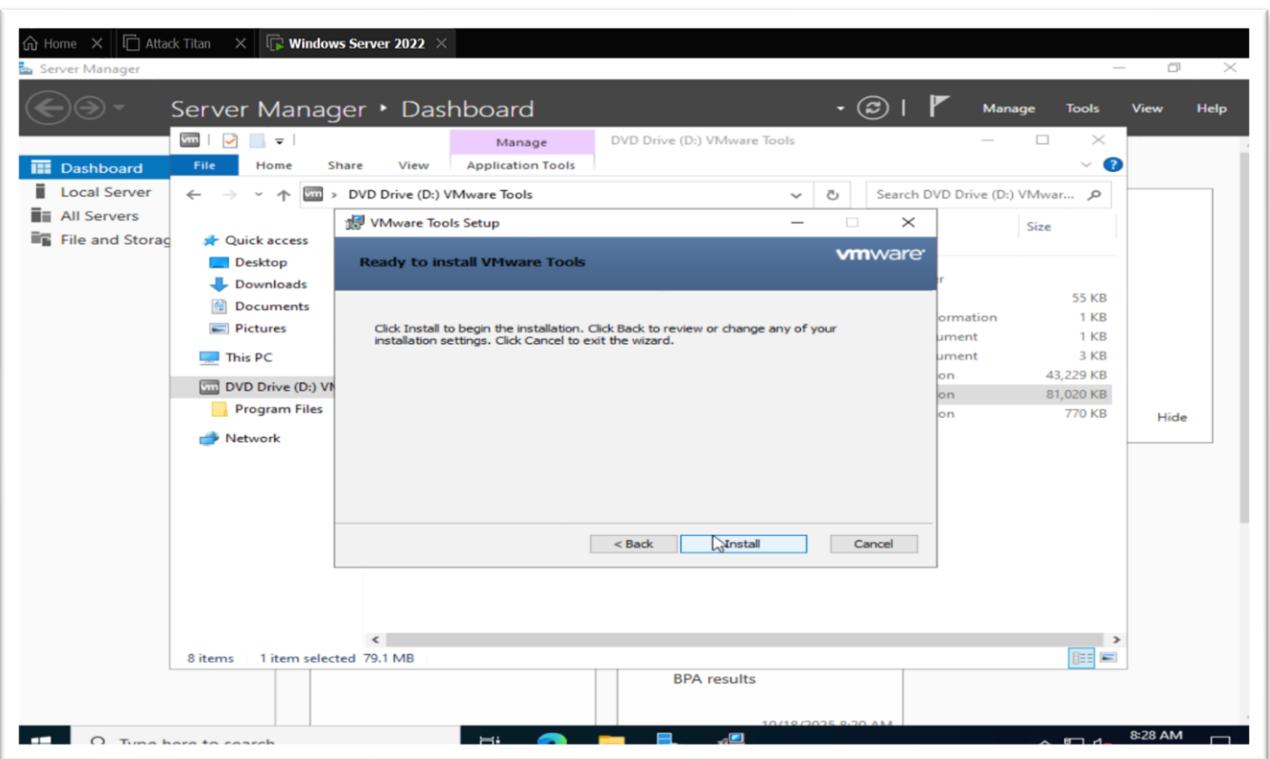
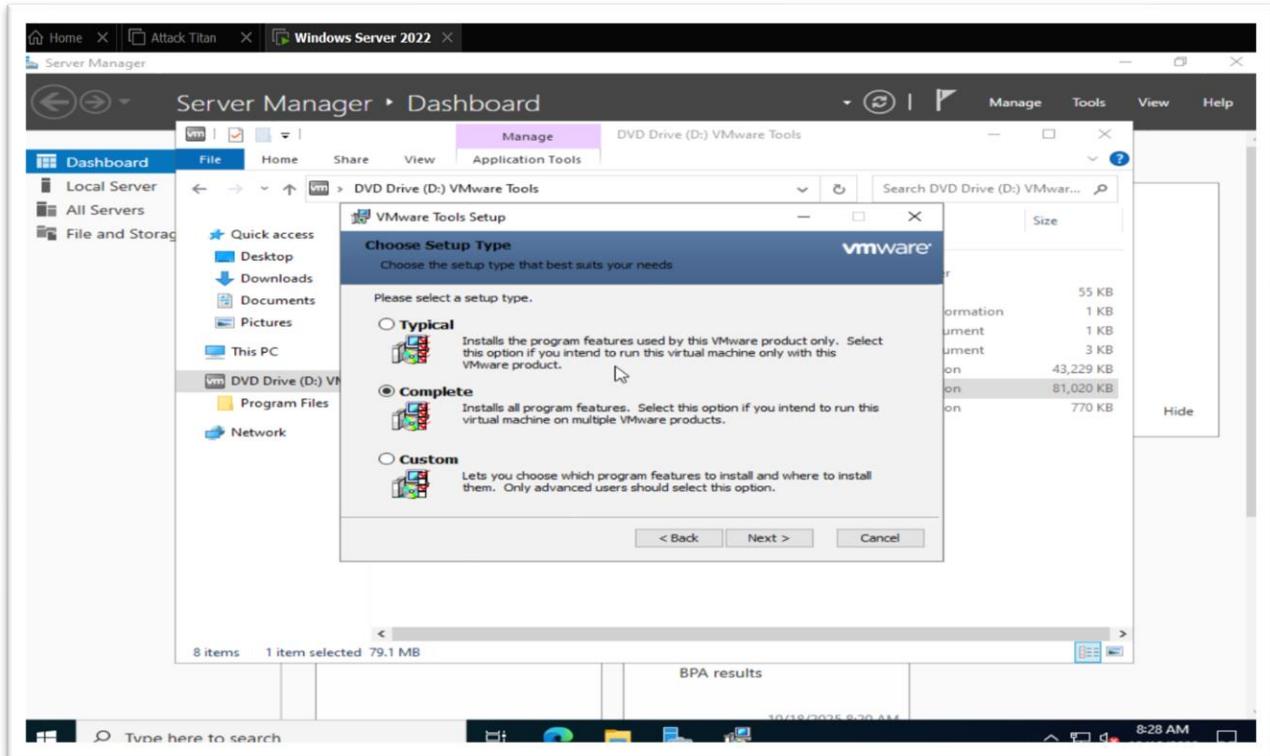


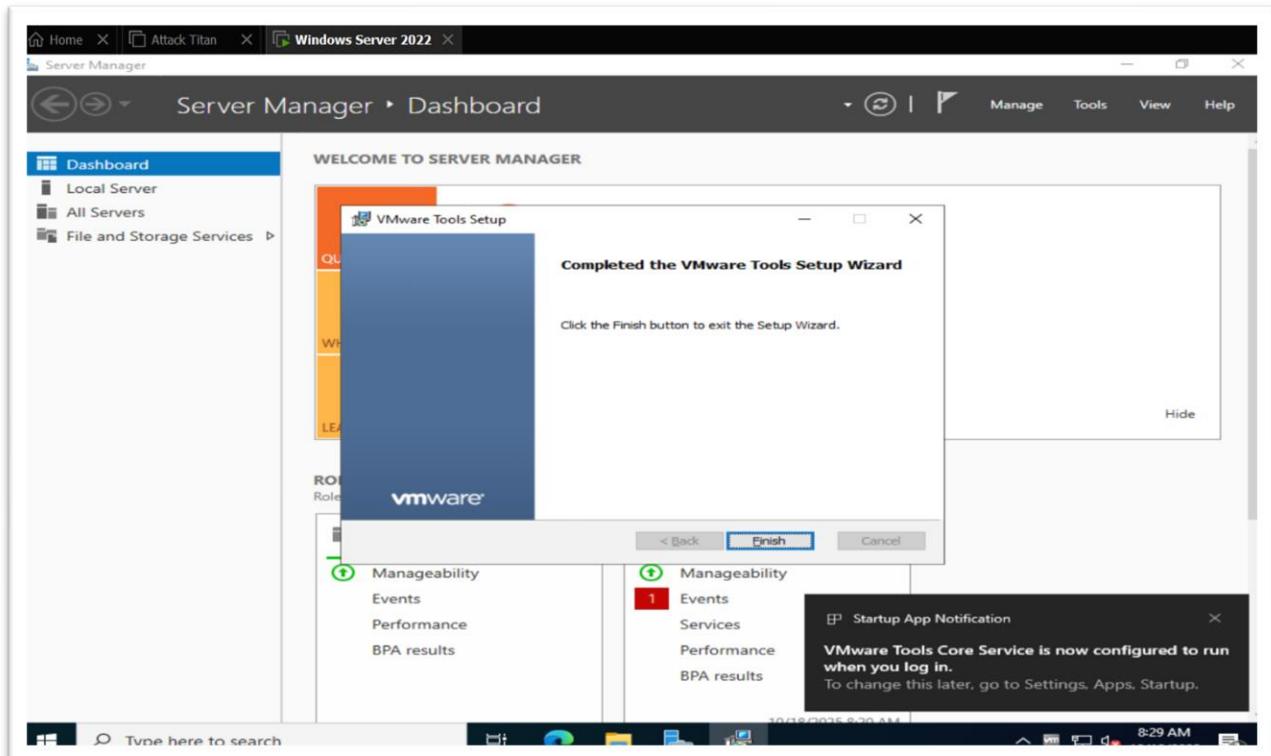
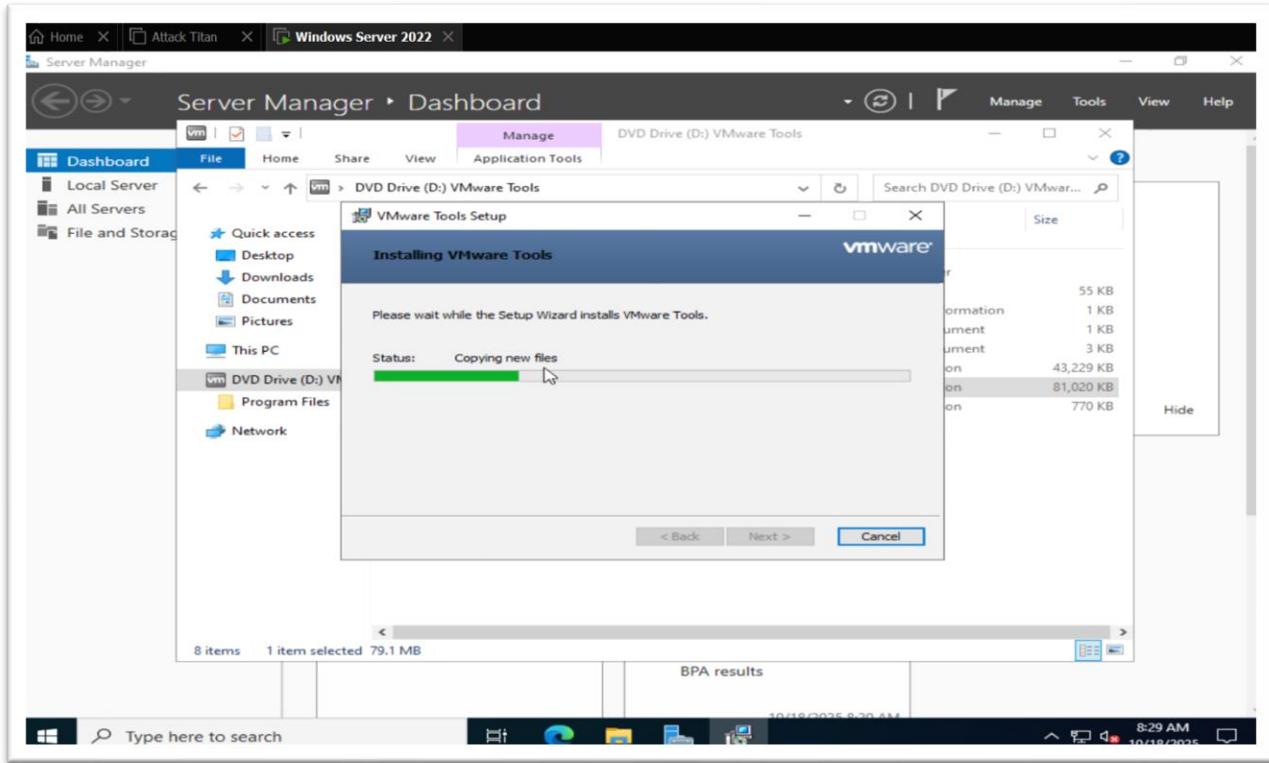


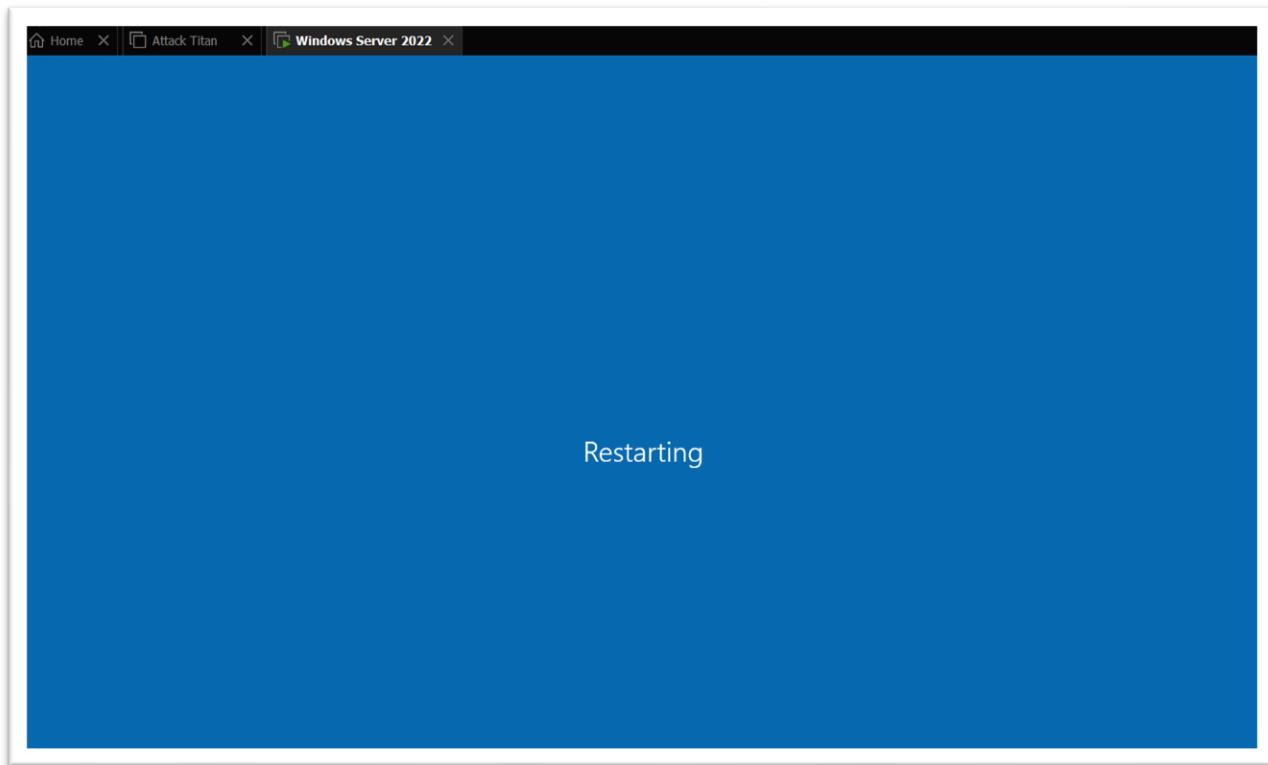
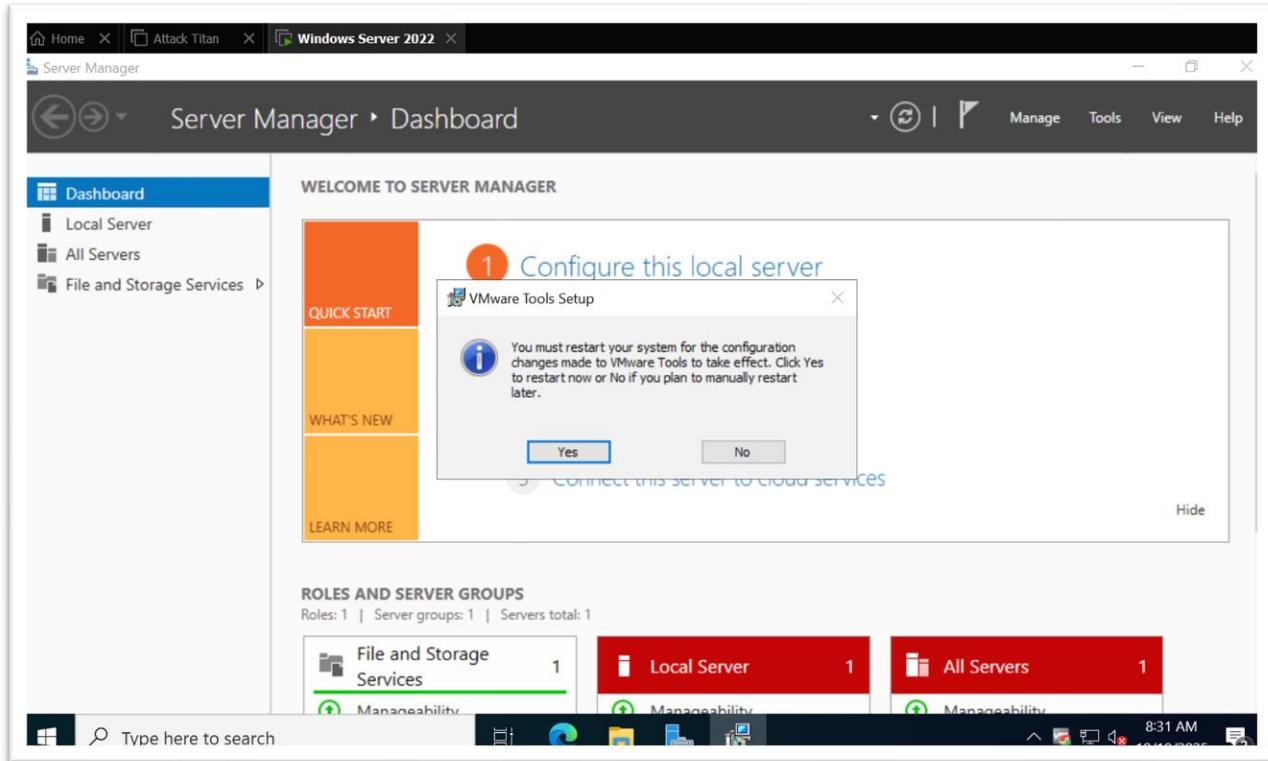






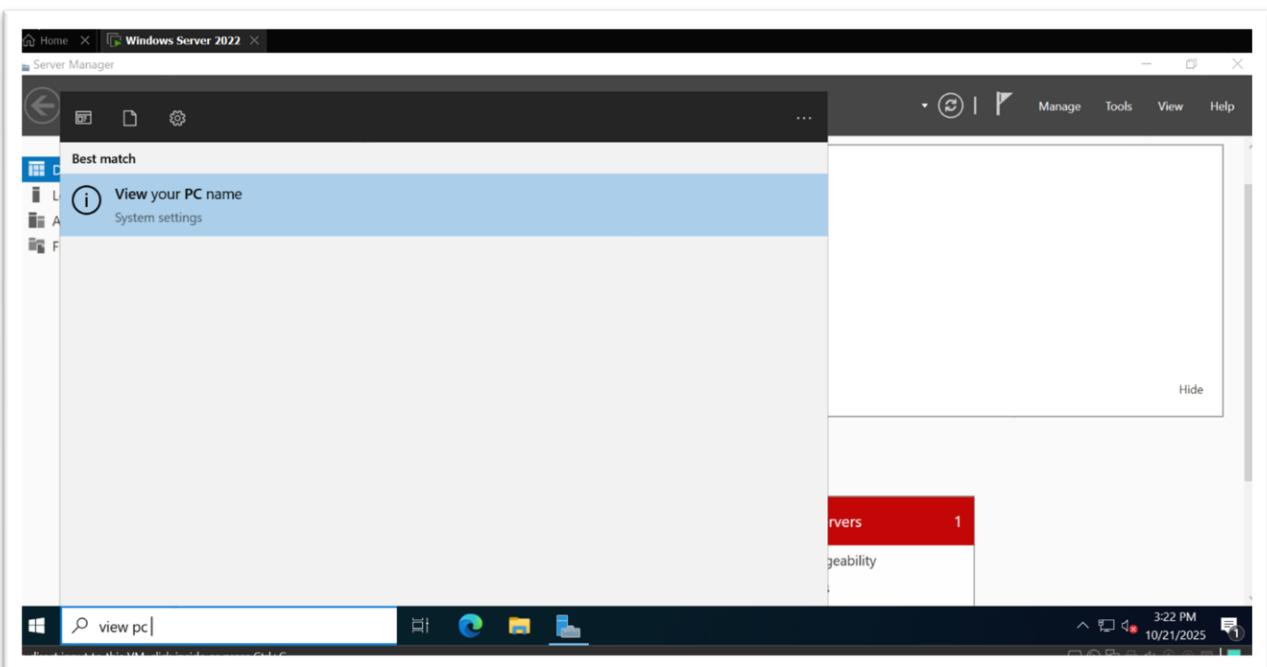
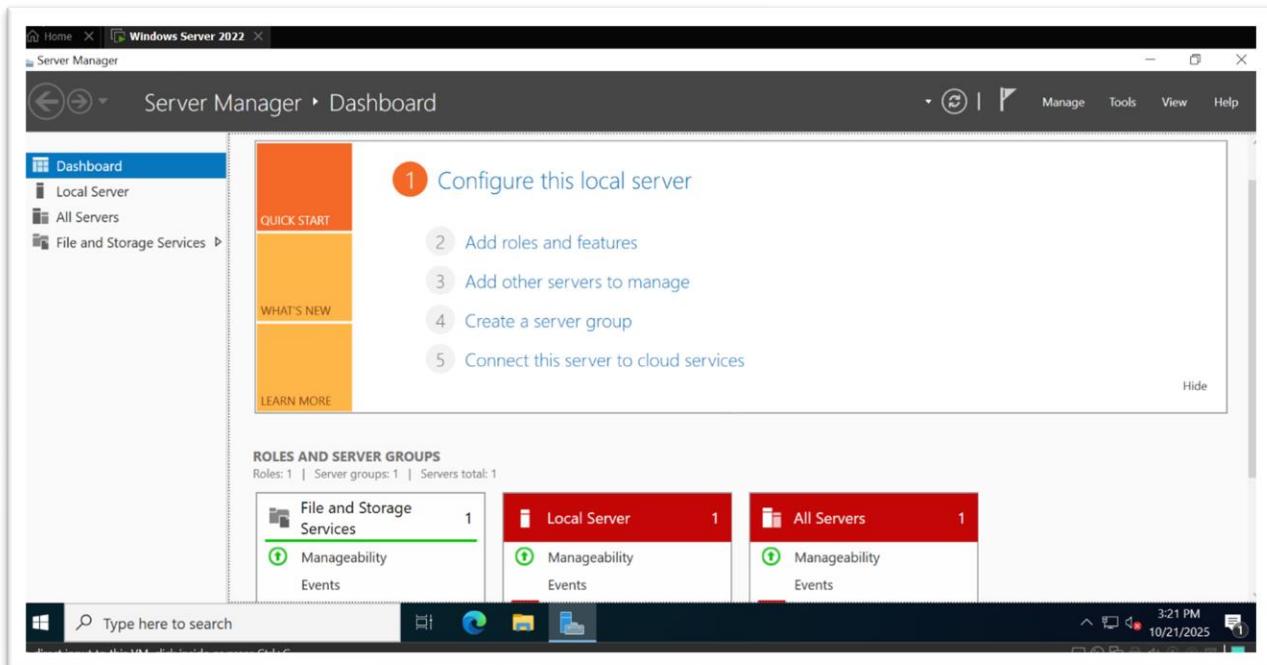


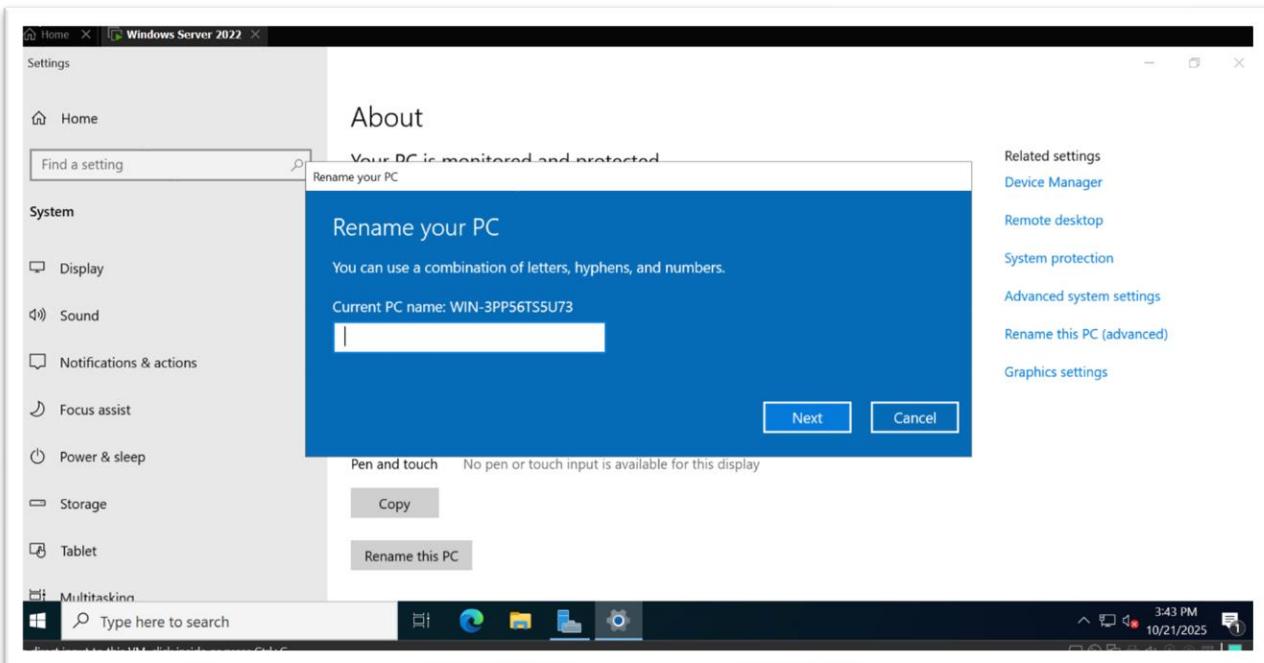
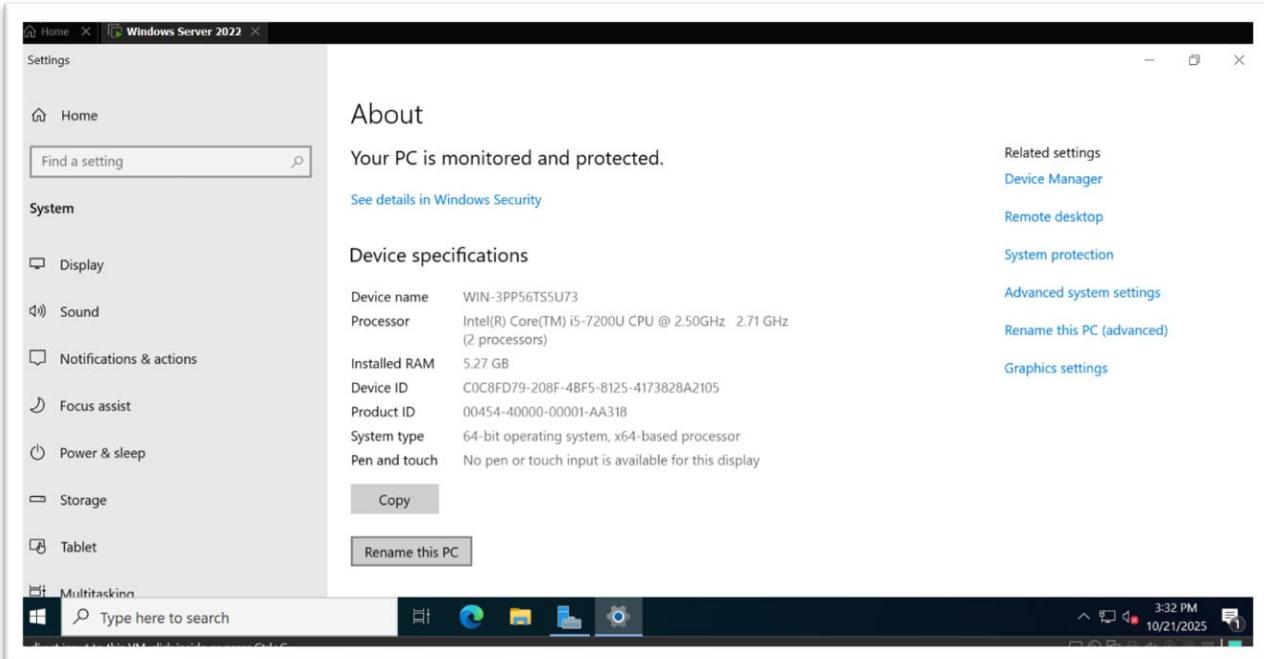


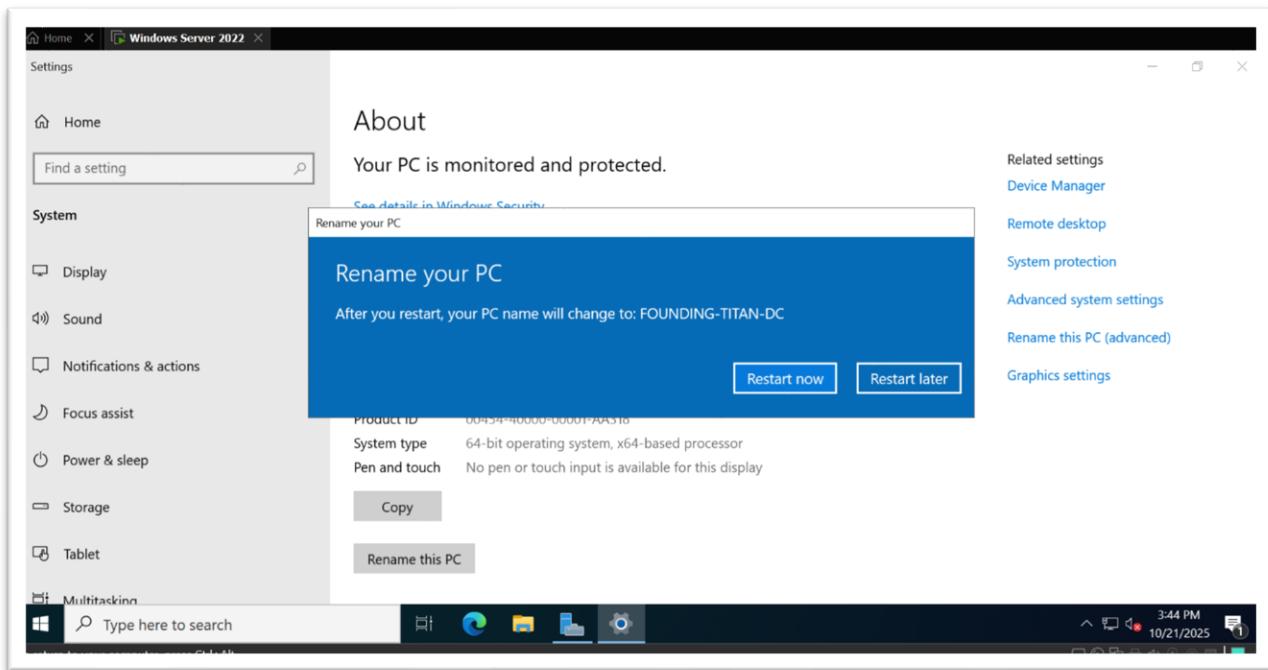
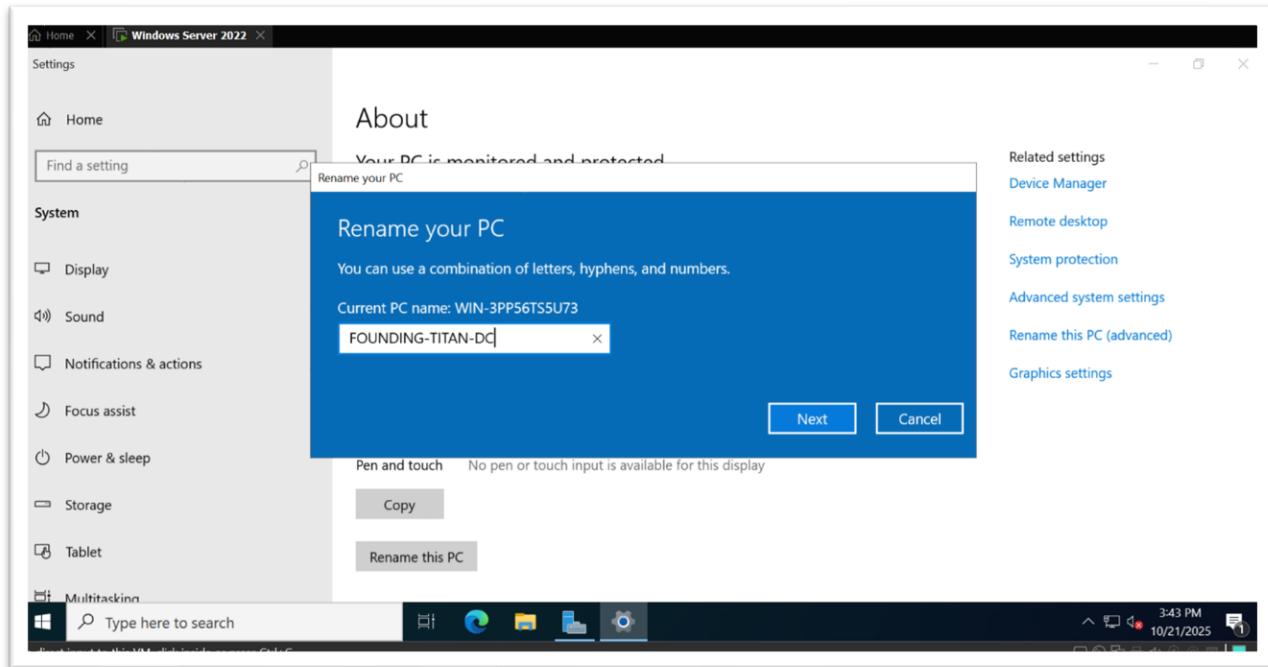


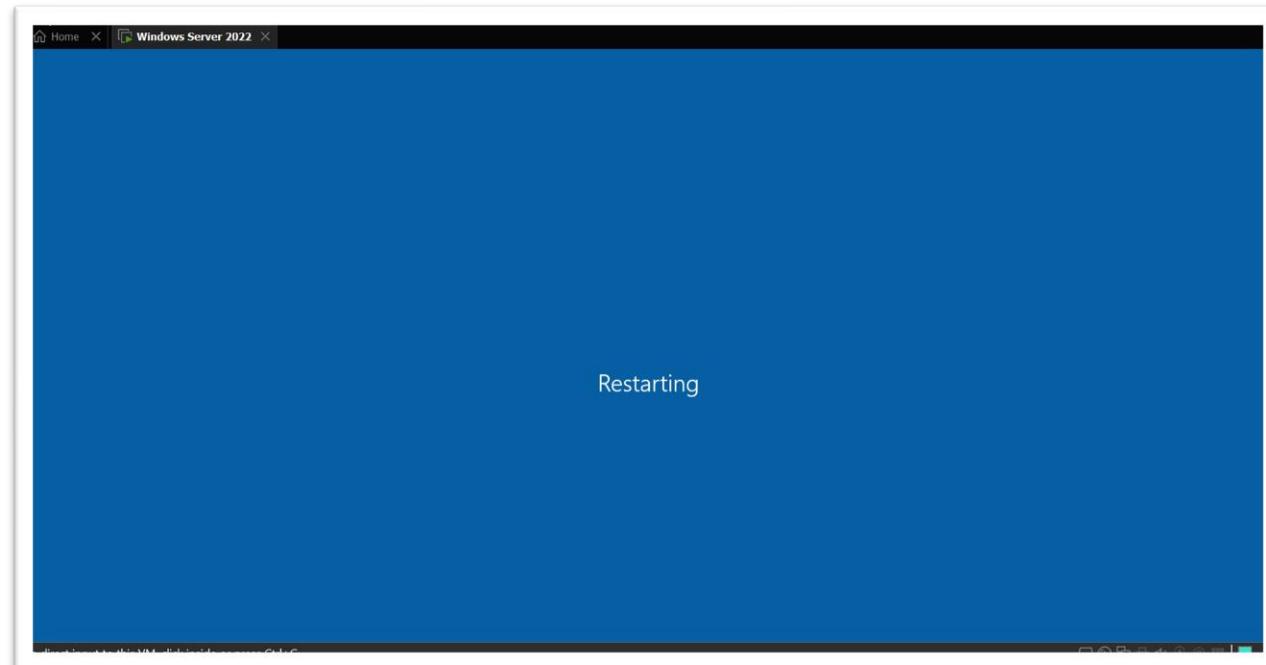
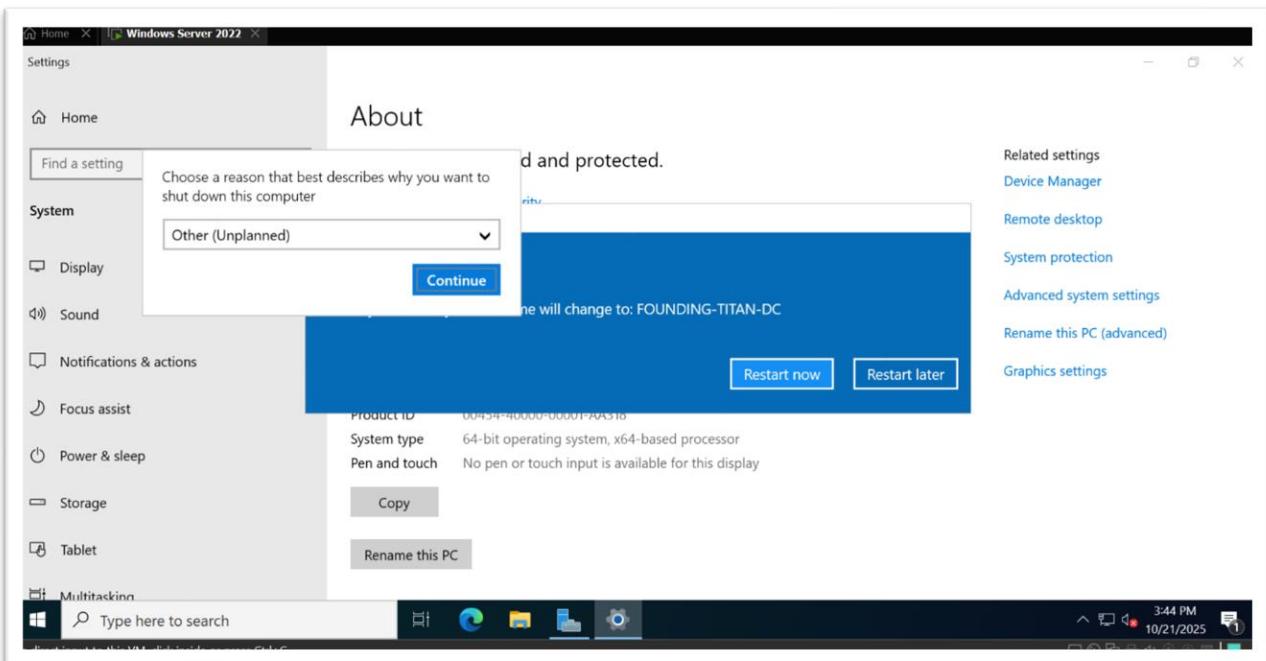
Step 2: Configure Windows Server as Domain Controller

- Rename “PC name” as domain controller name

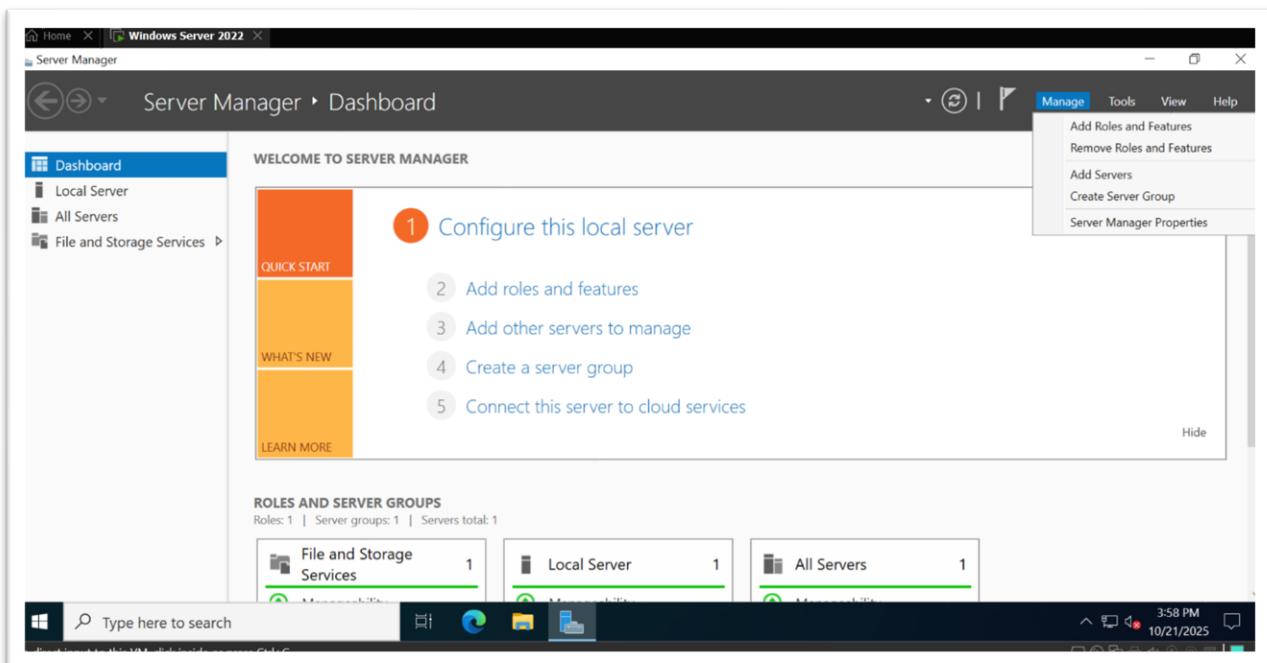
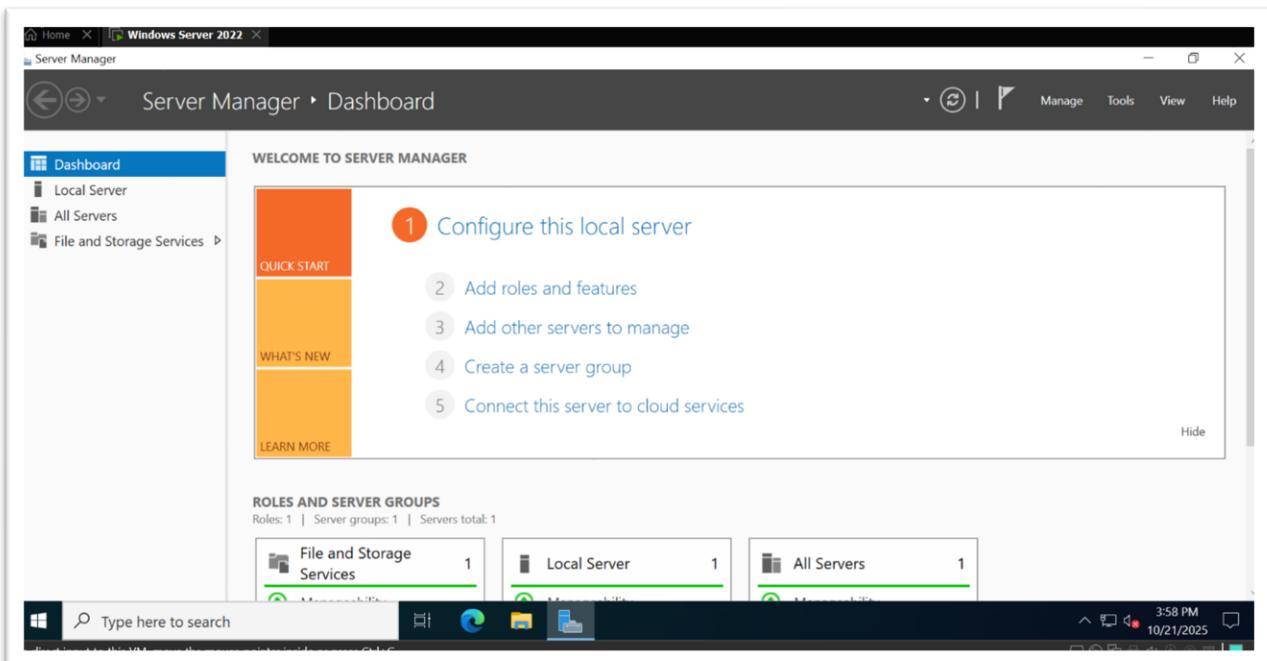


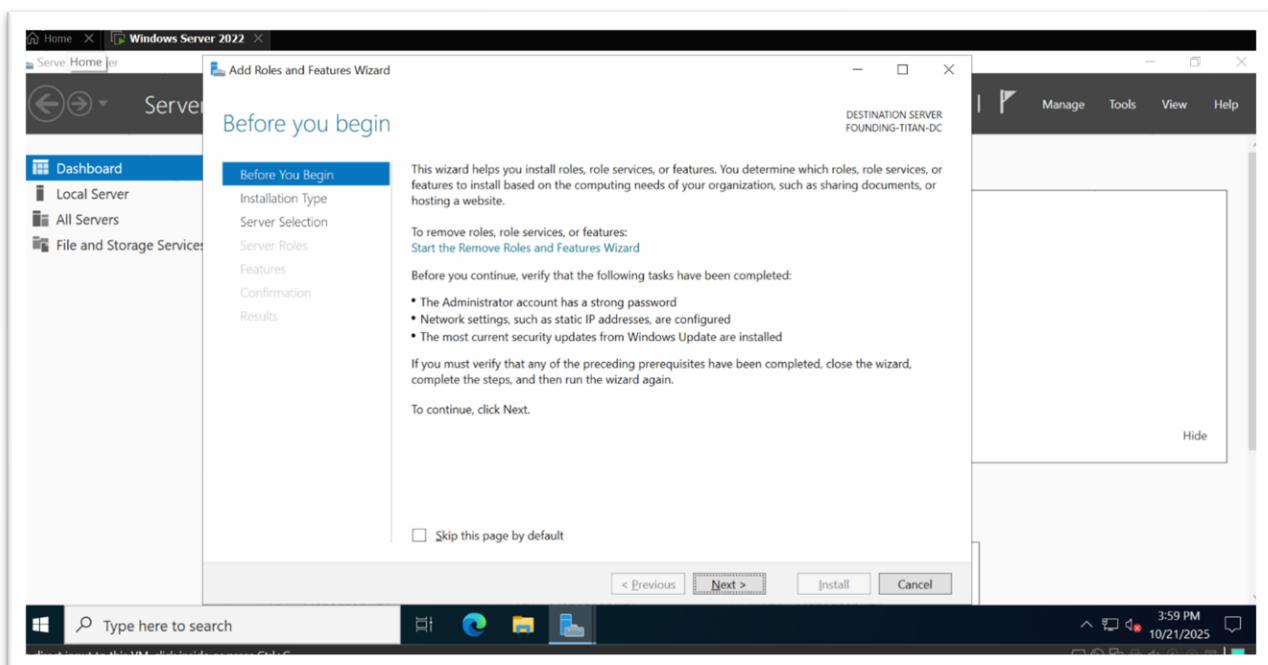
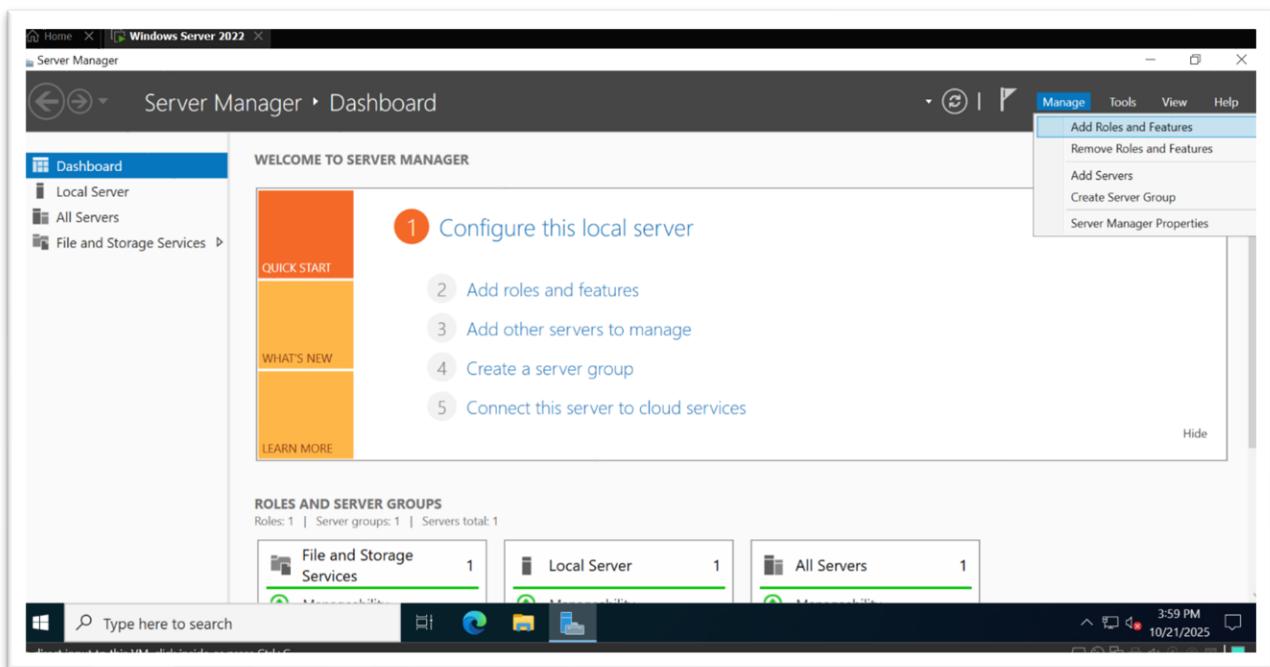


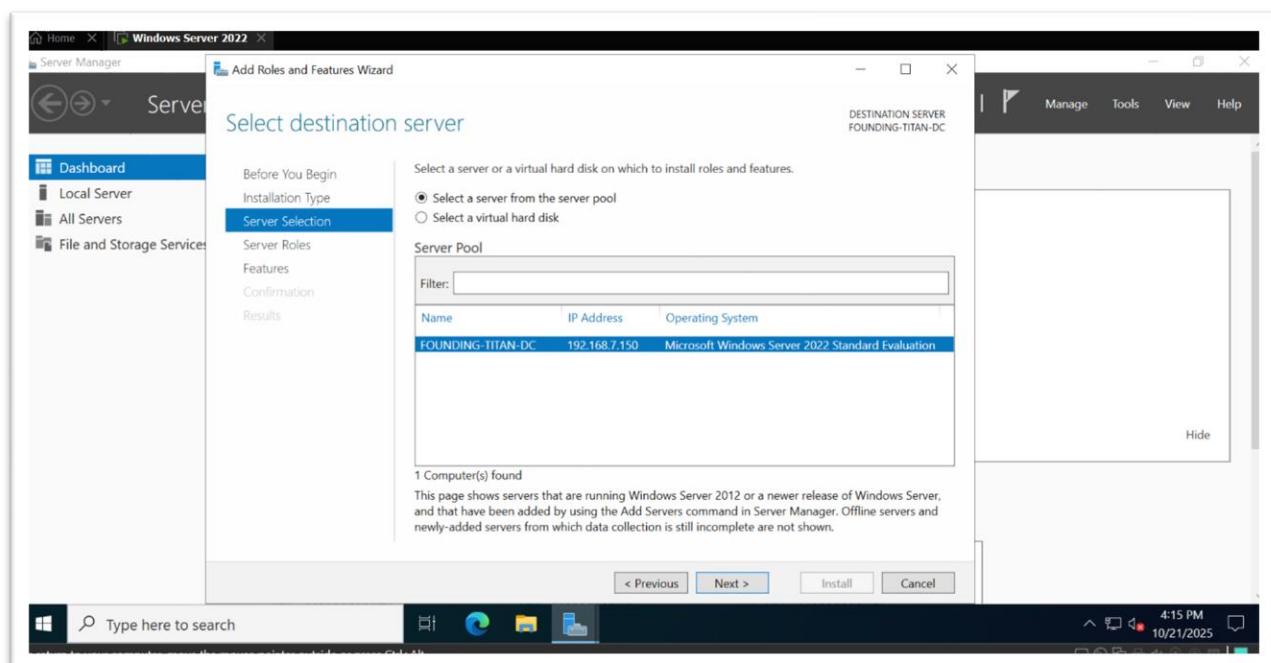
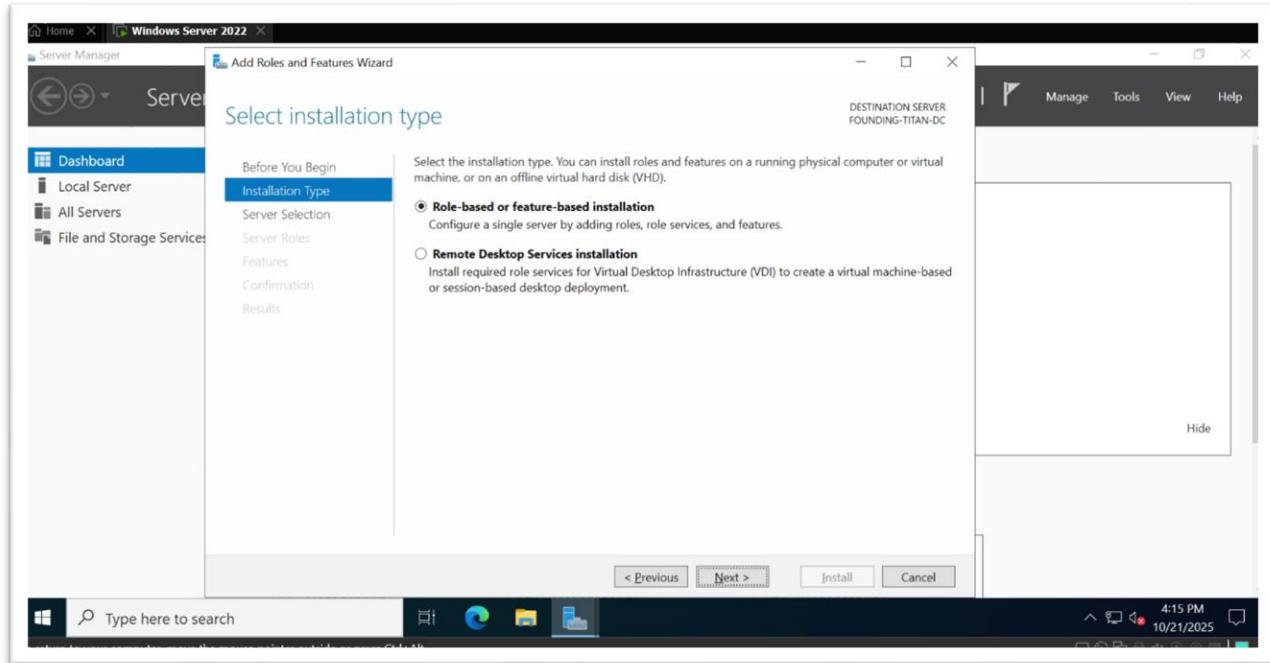




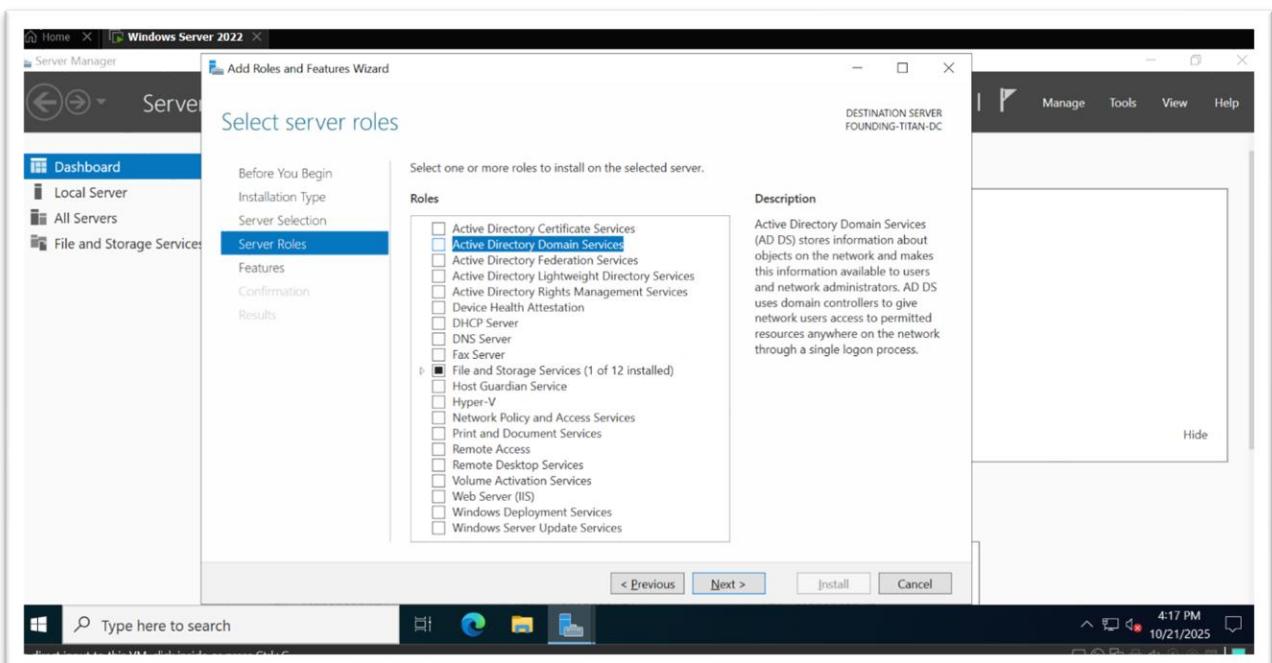
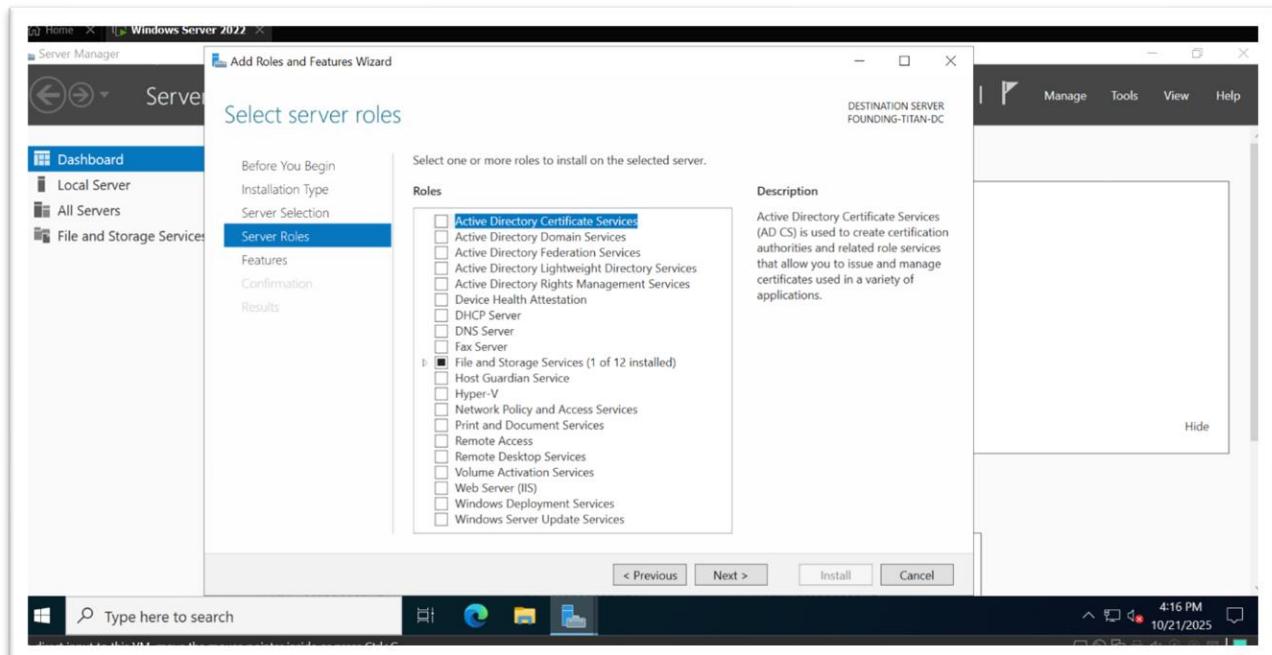
- Add server roles and features

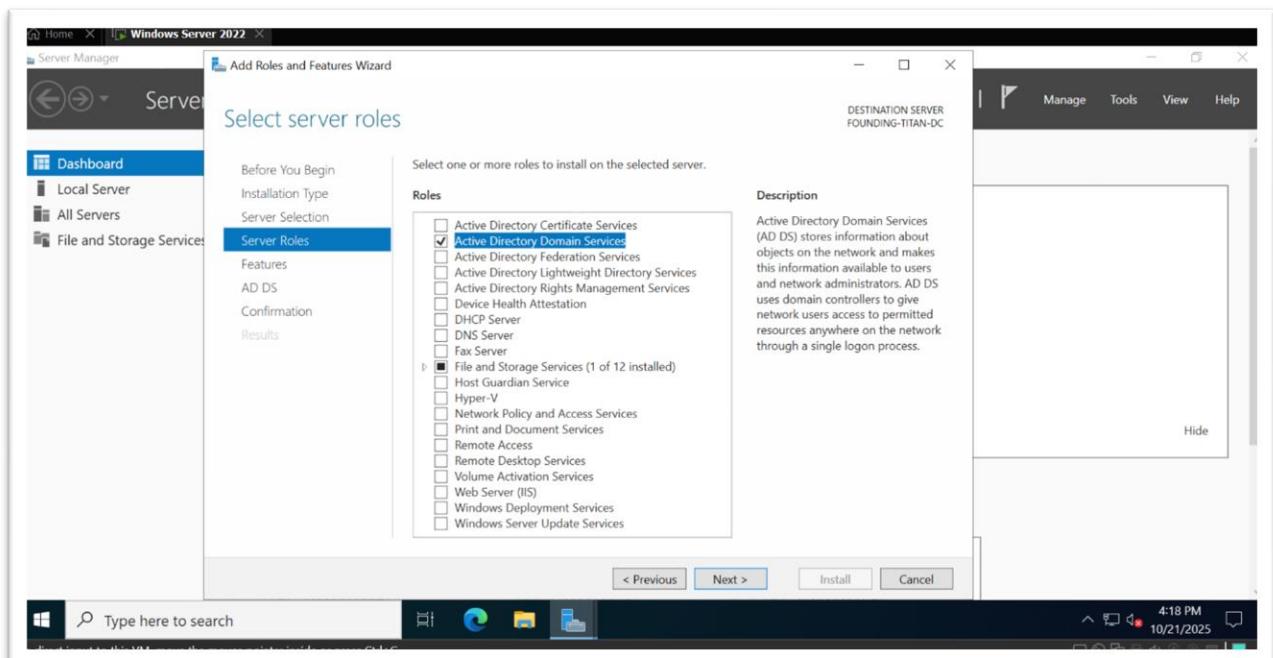
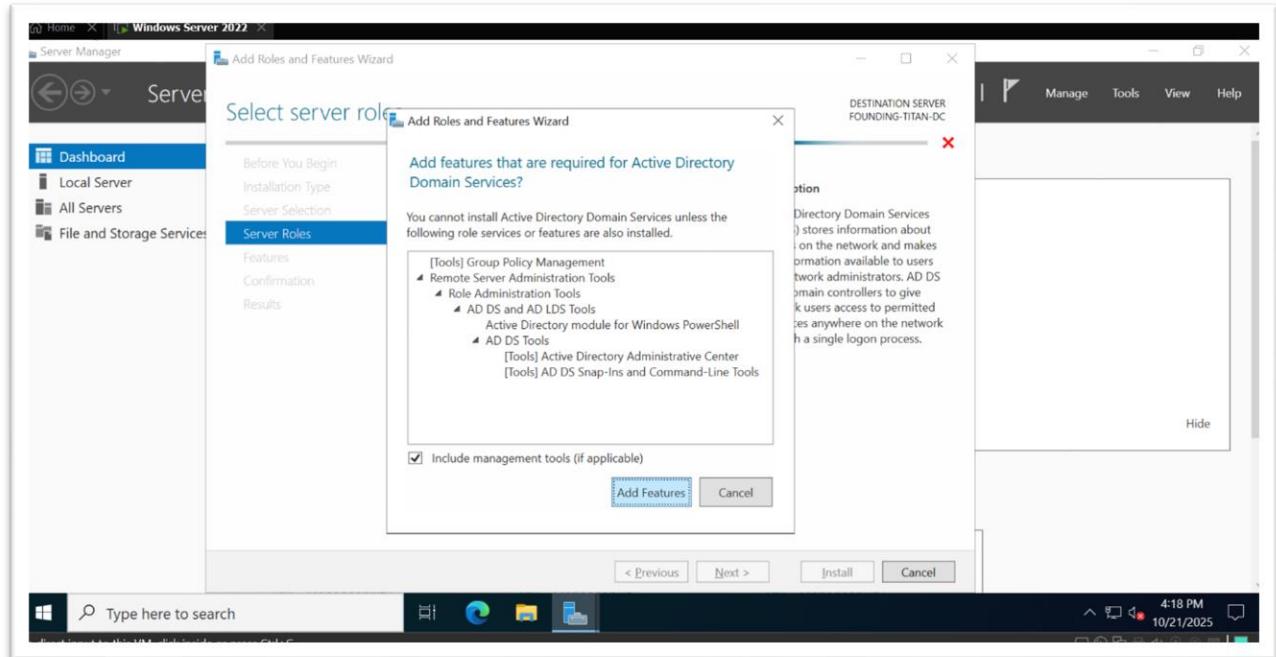


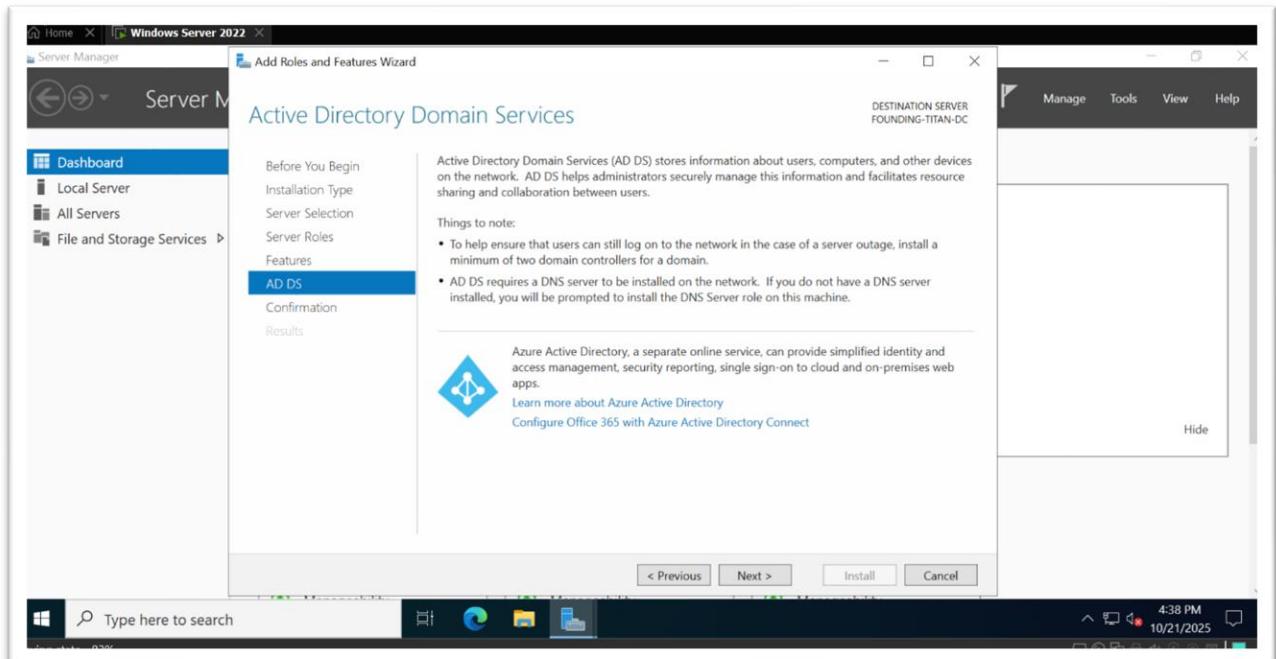
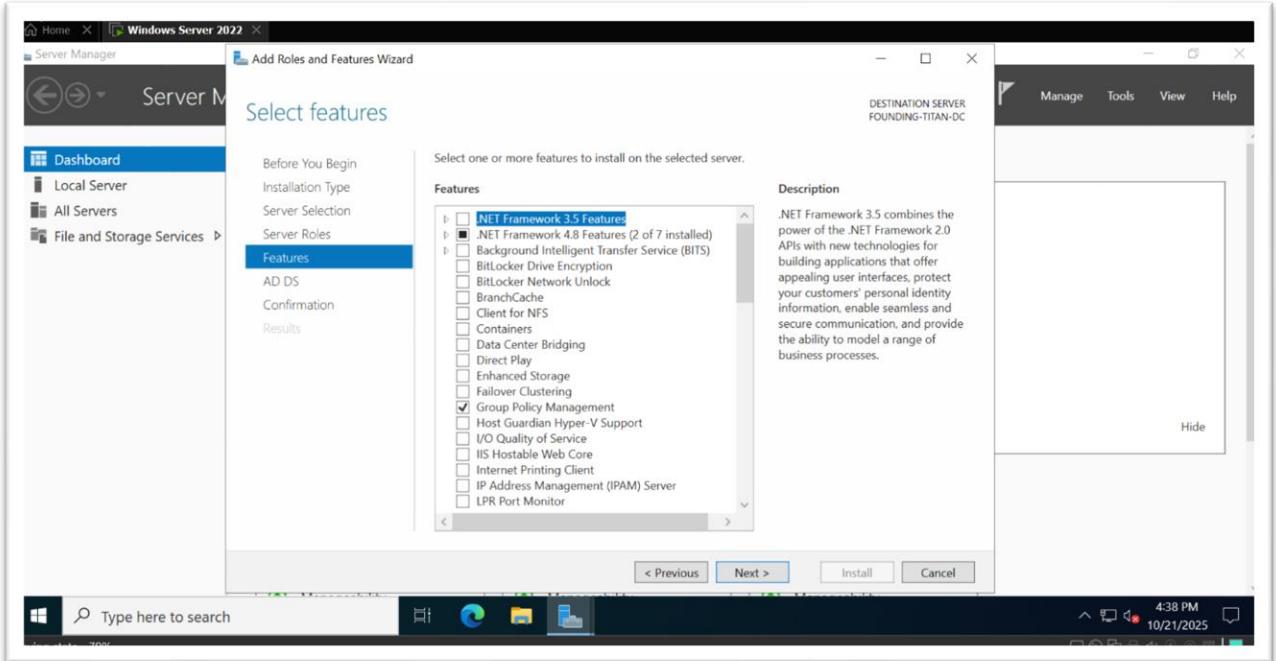


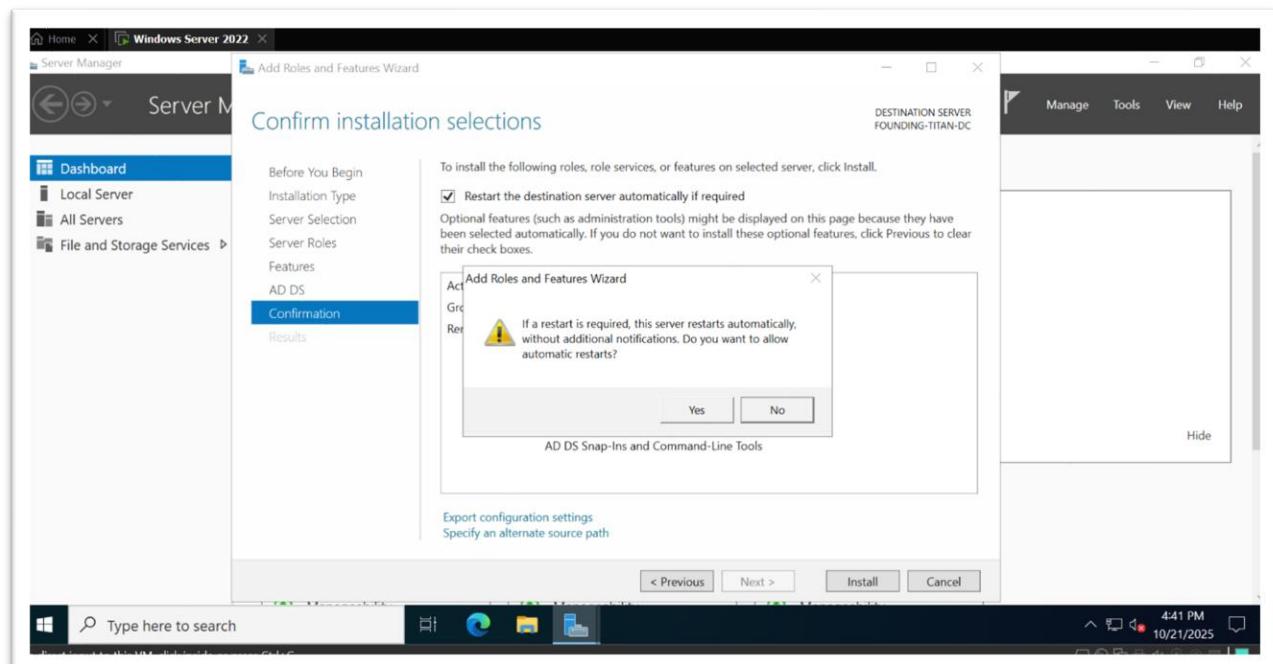
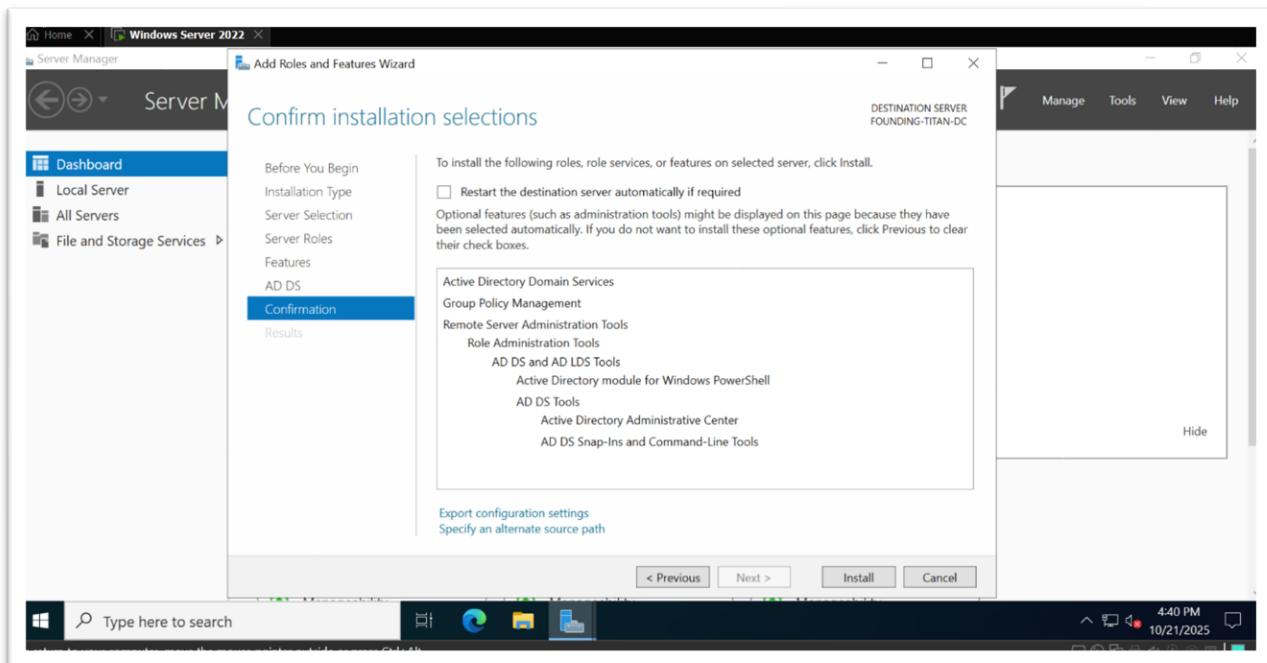


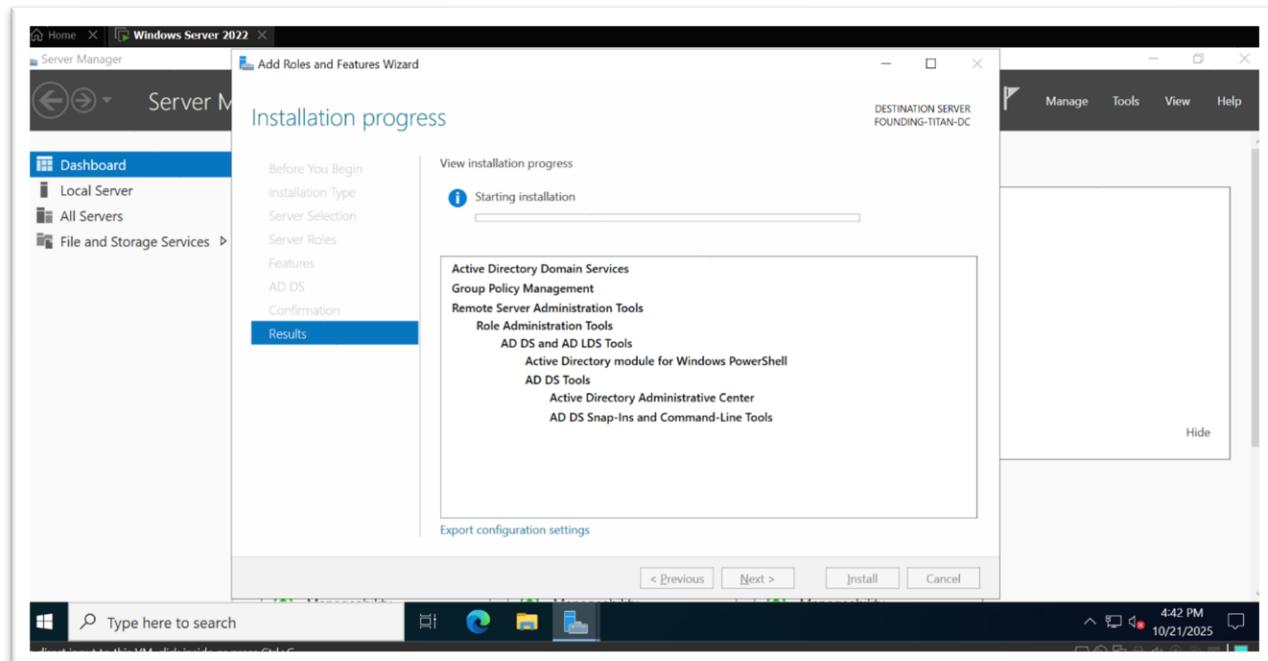
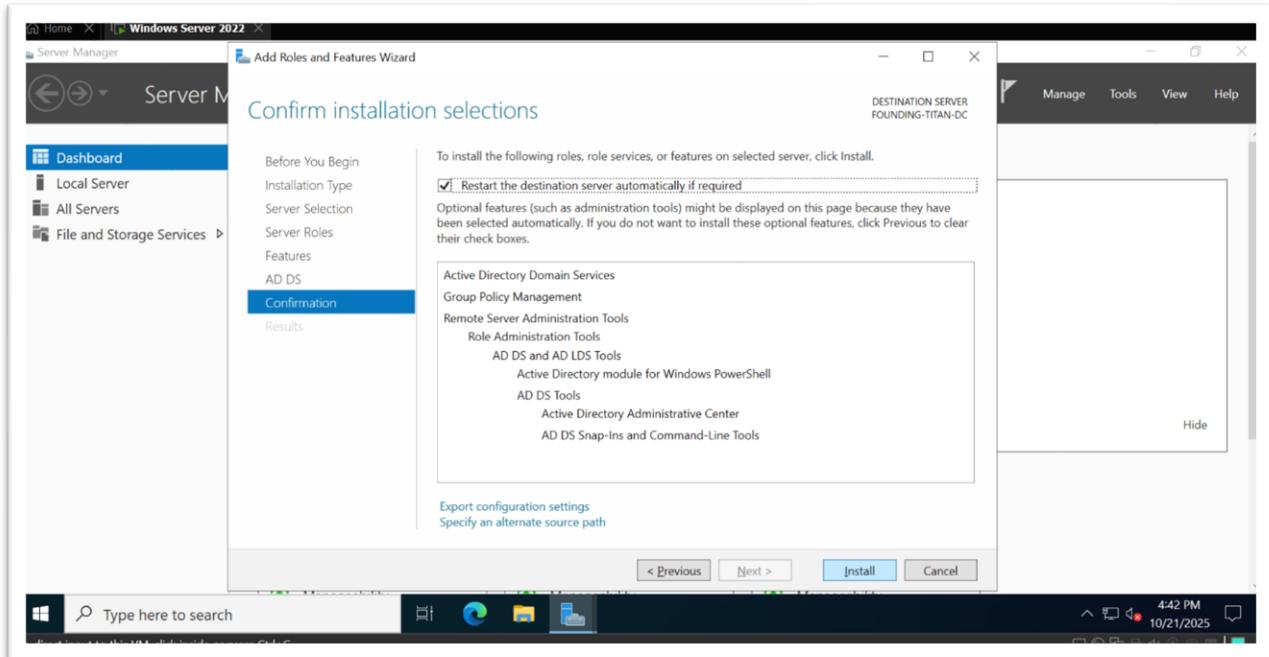
1. Add “Active Directory Domain Services” role

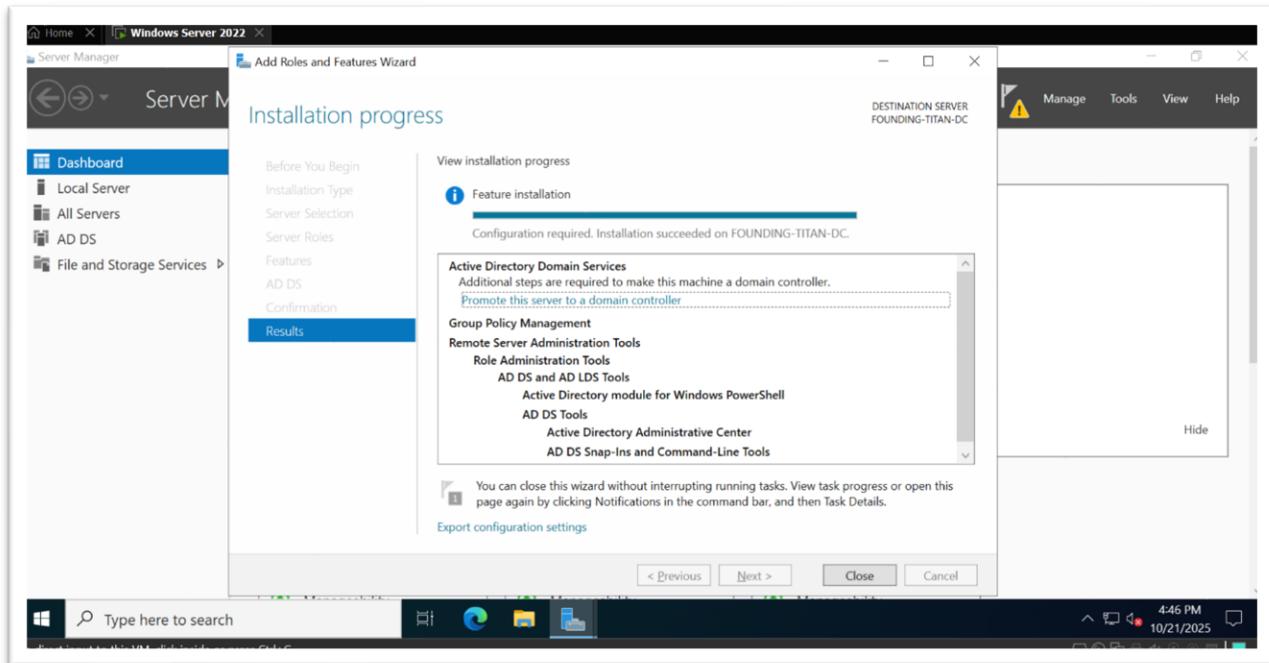
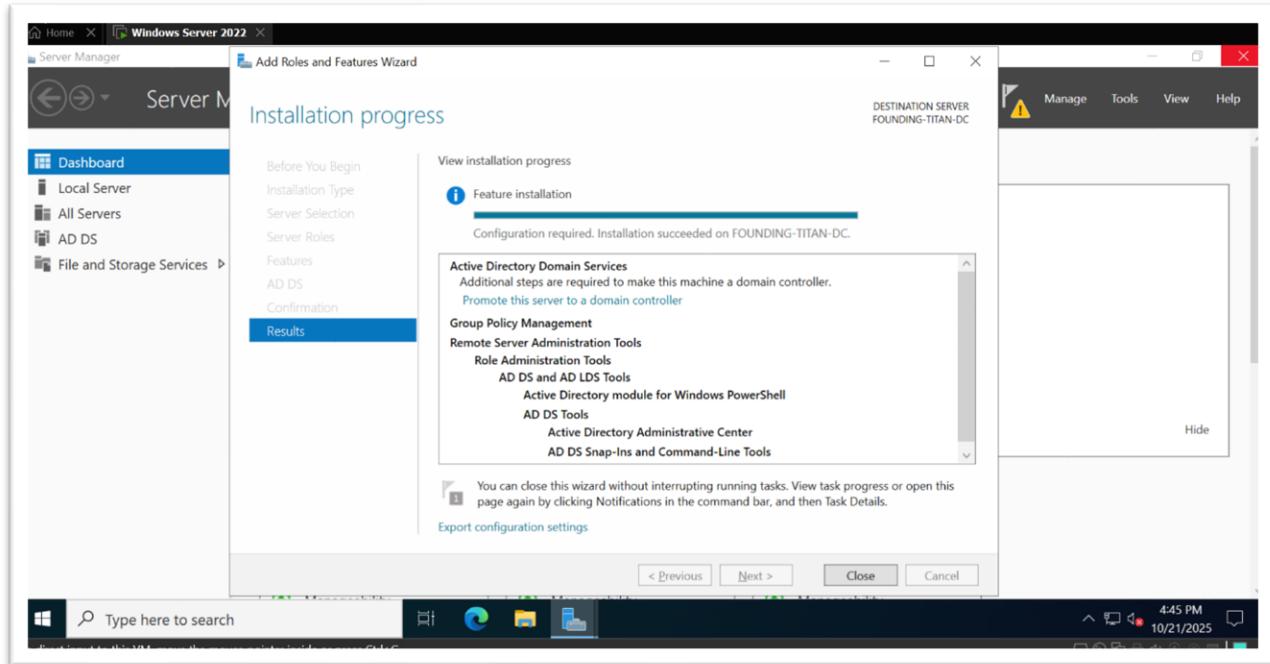




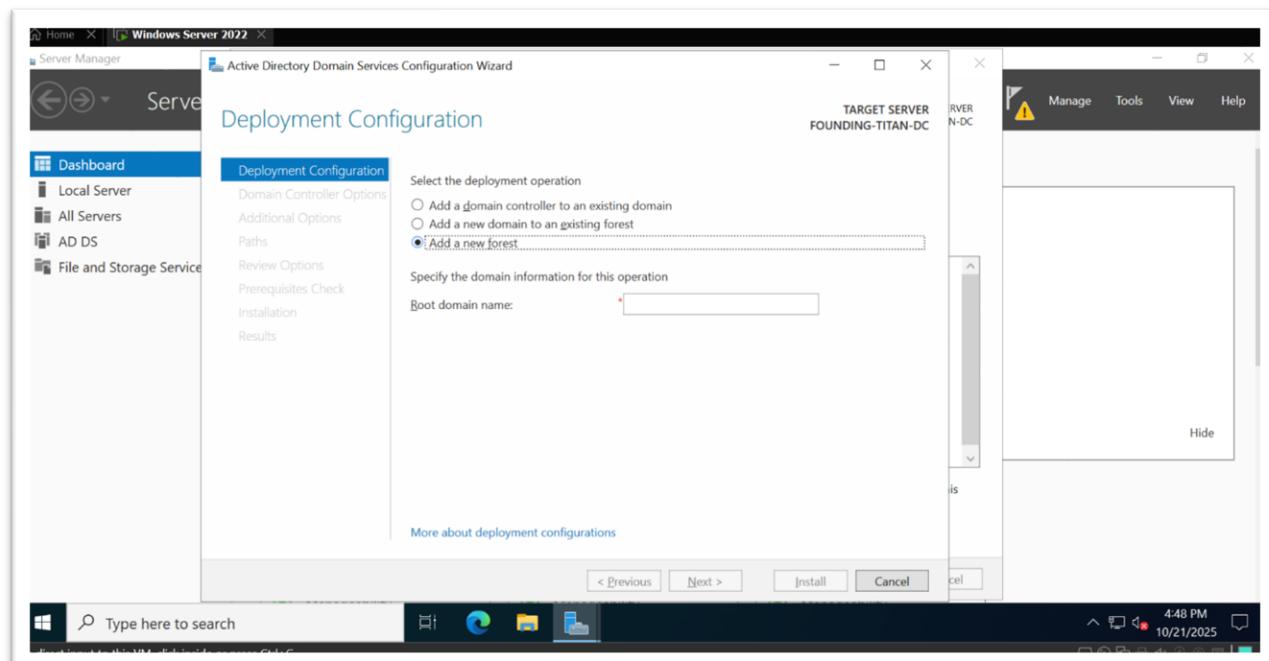
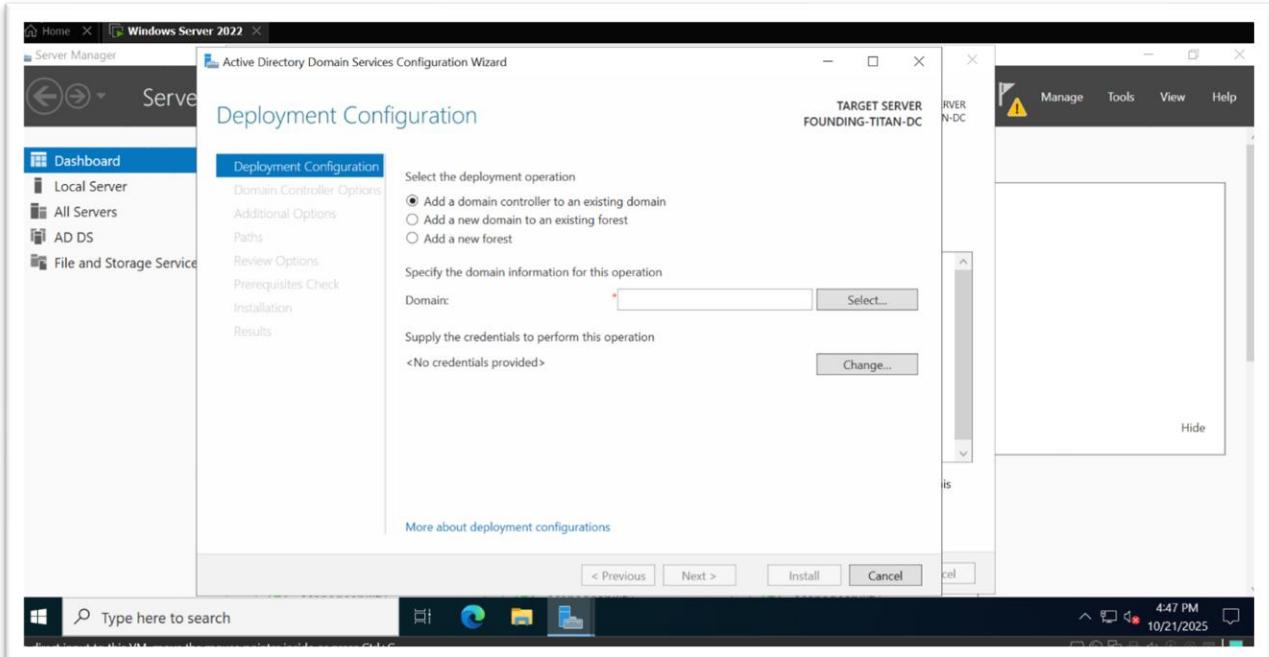


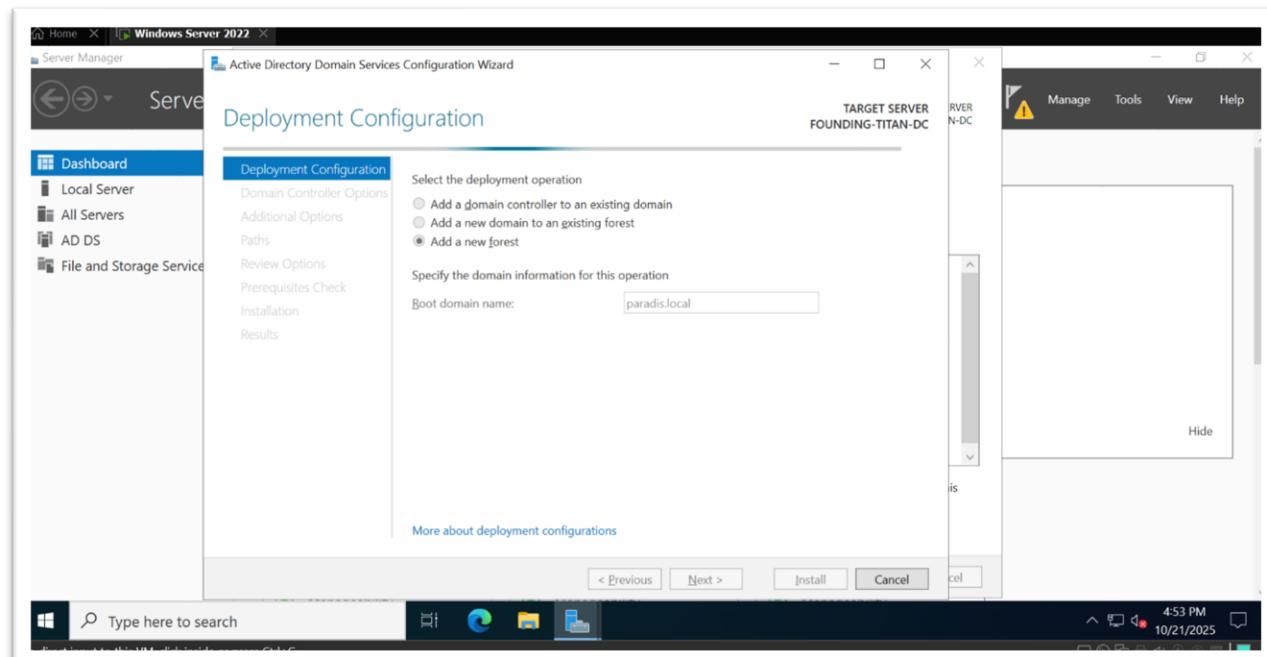
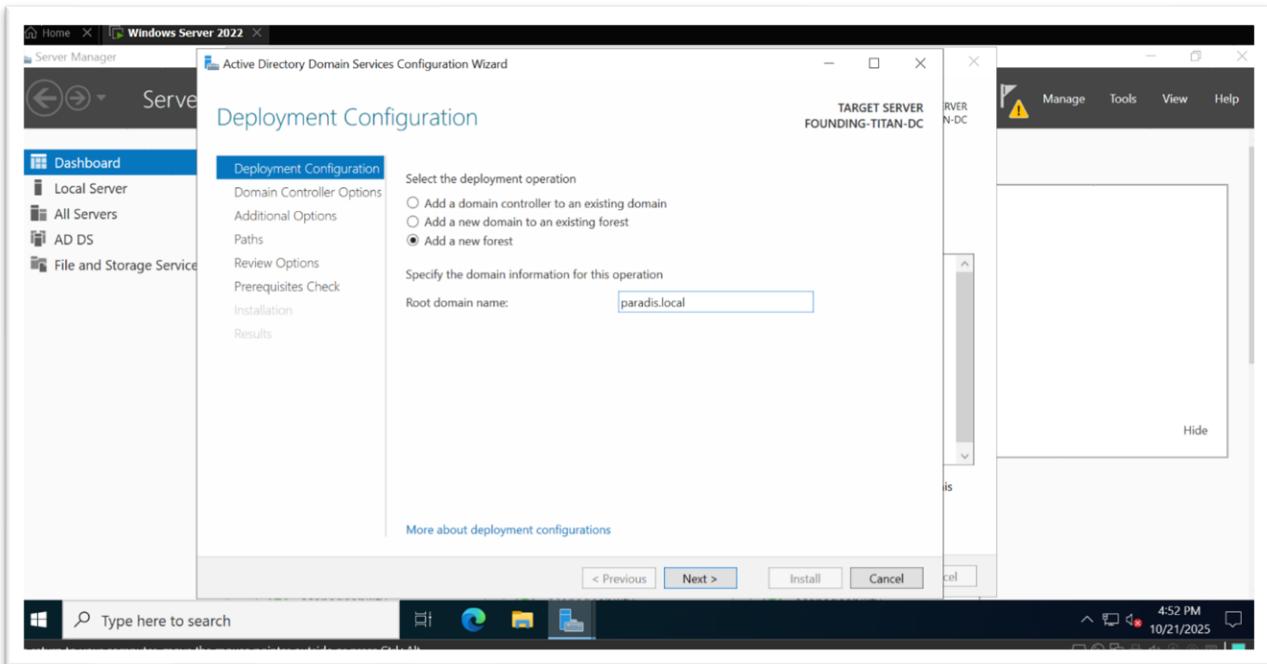


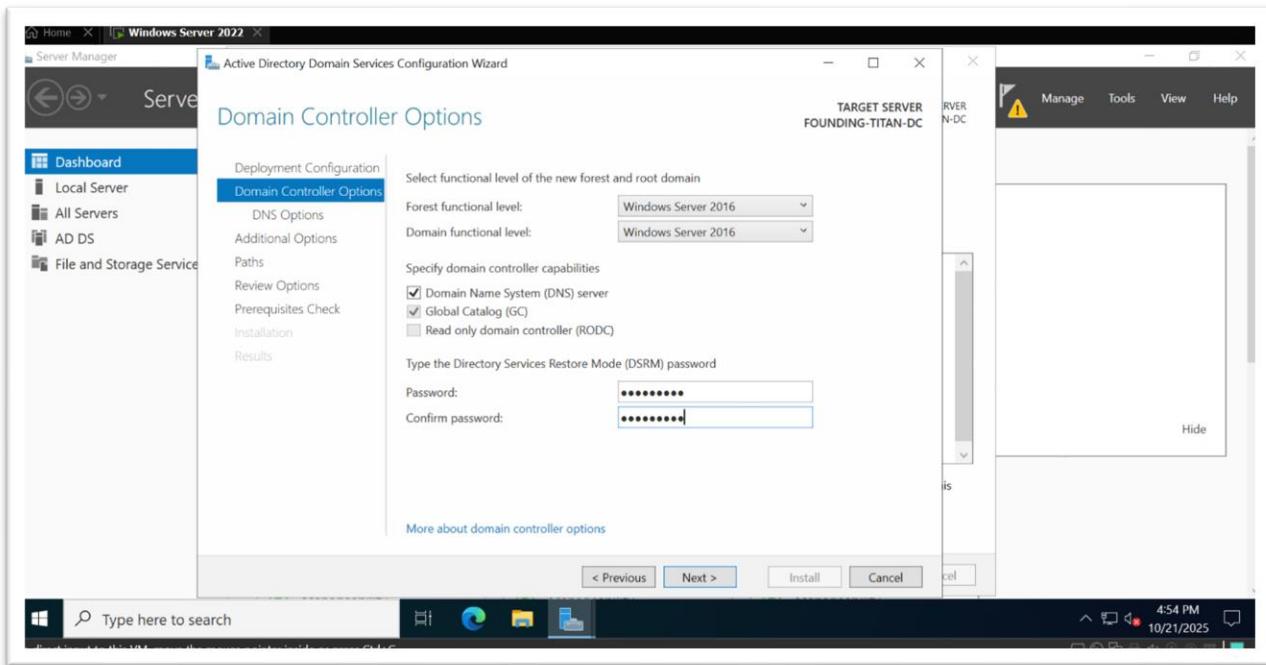
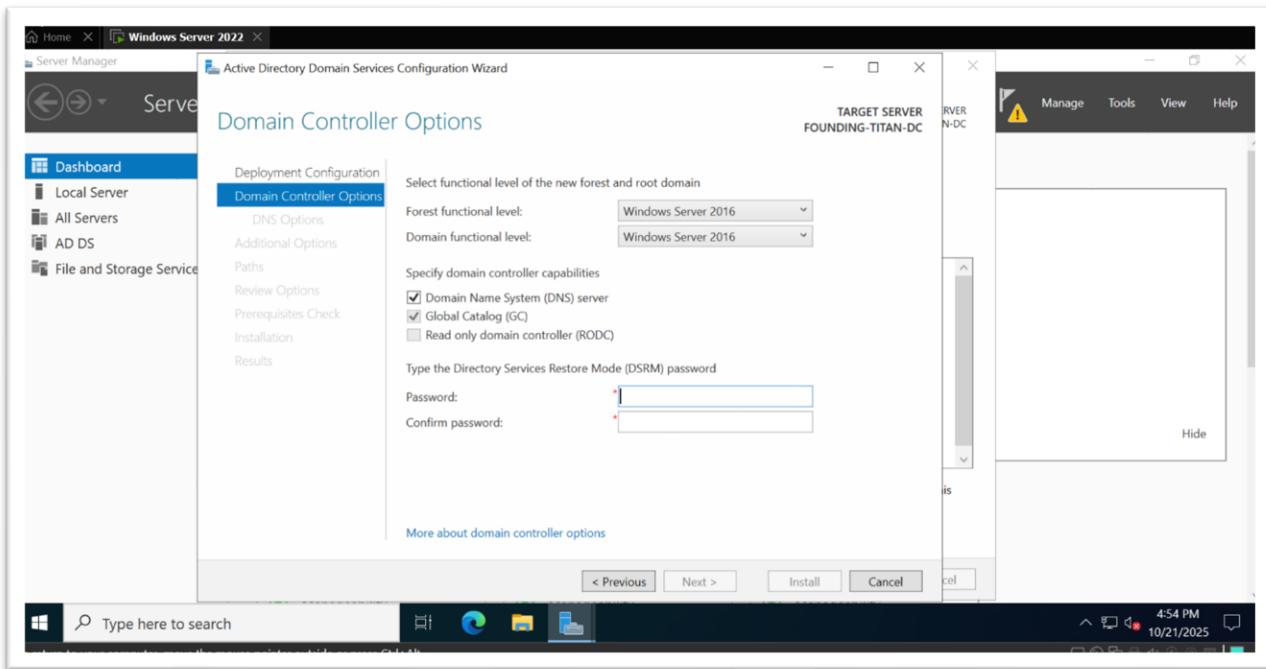


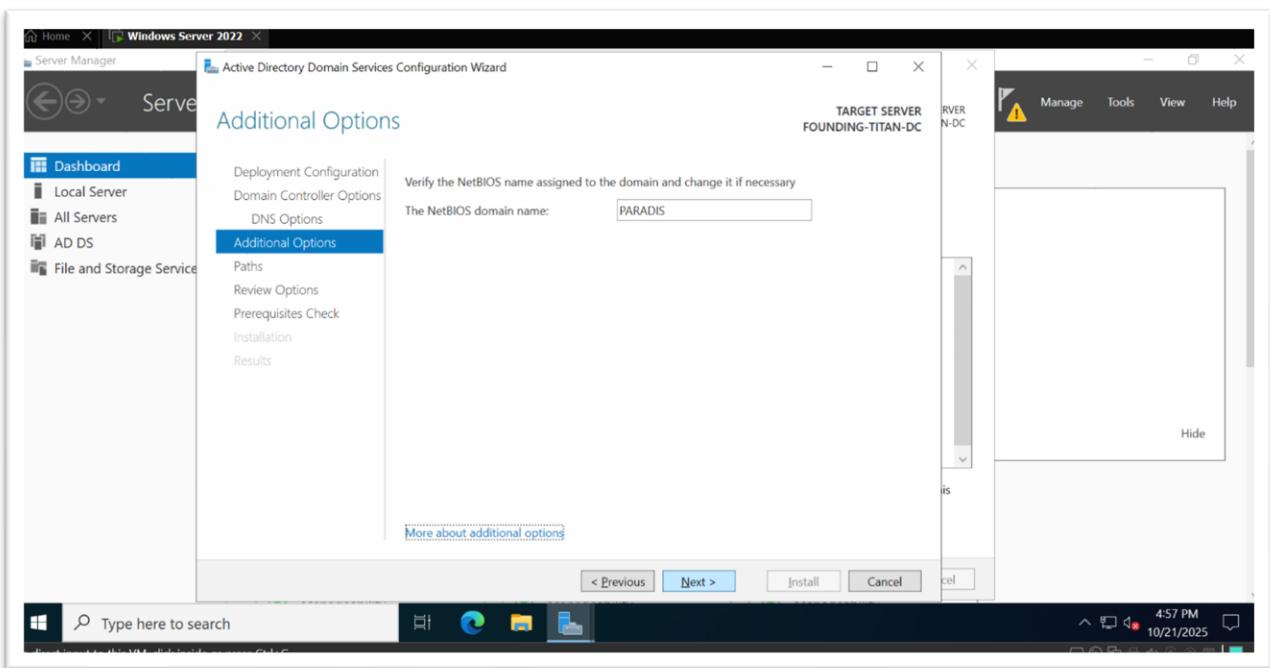
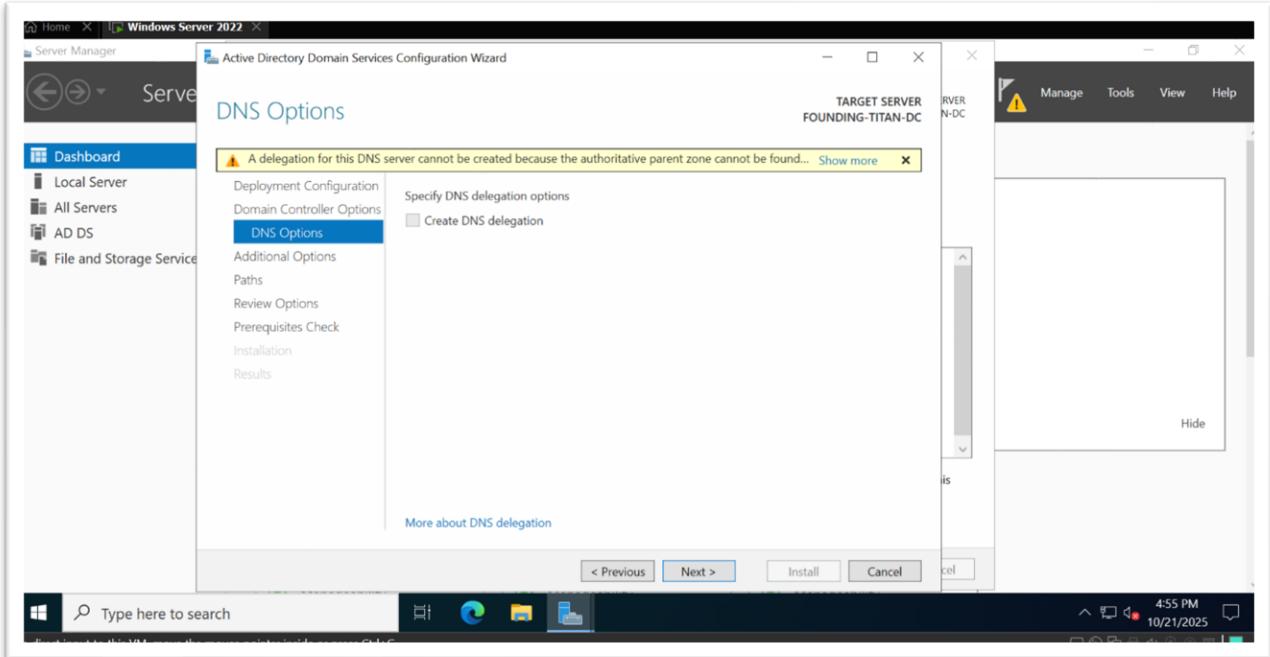


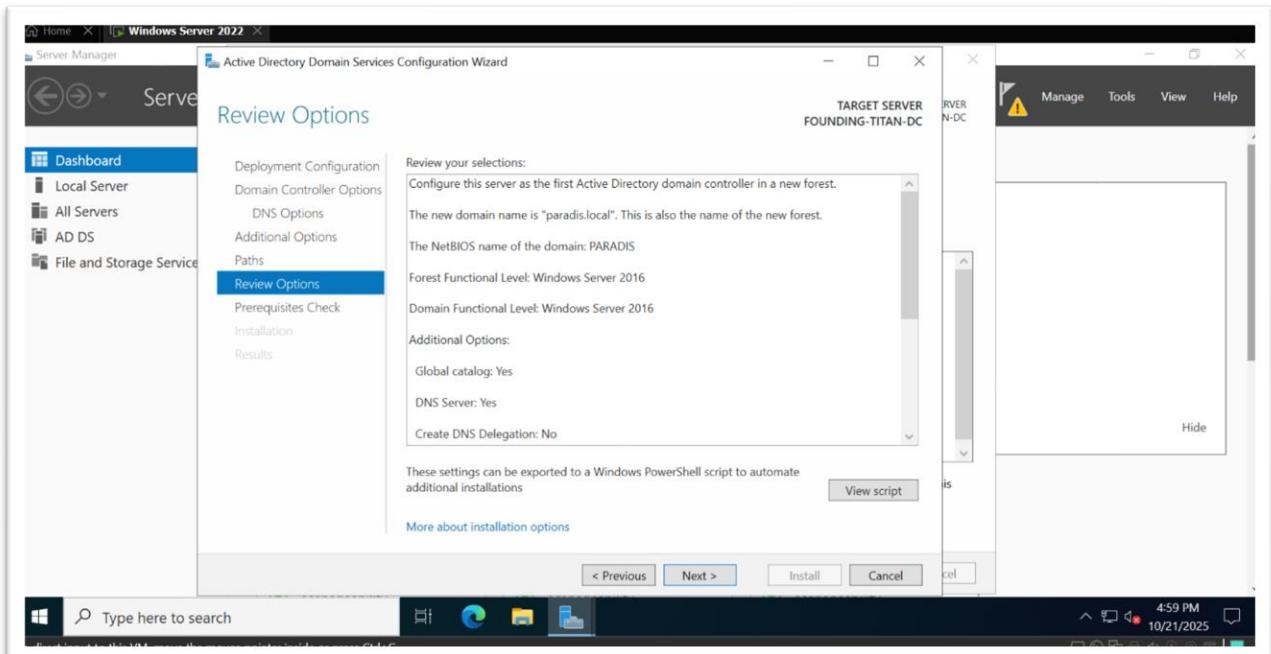
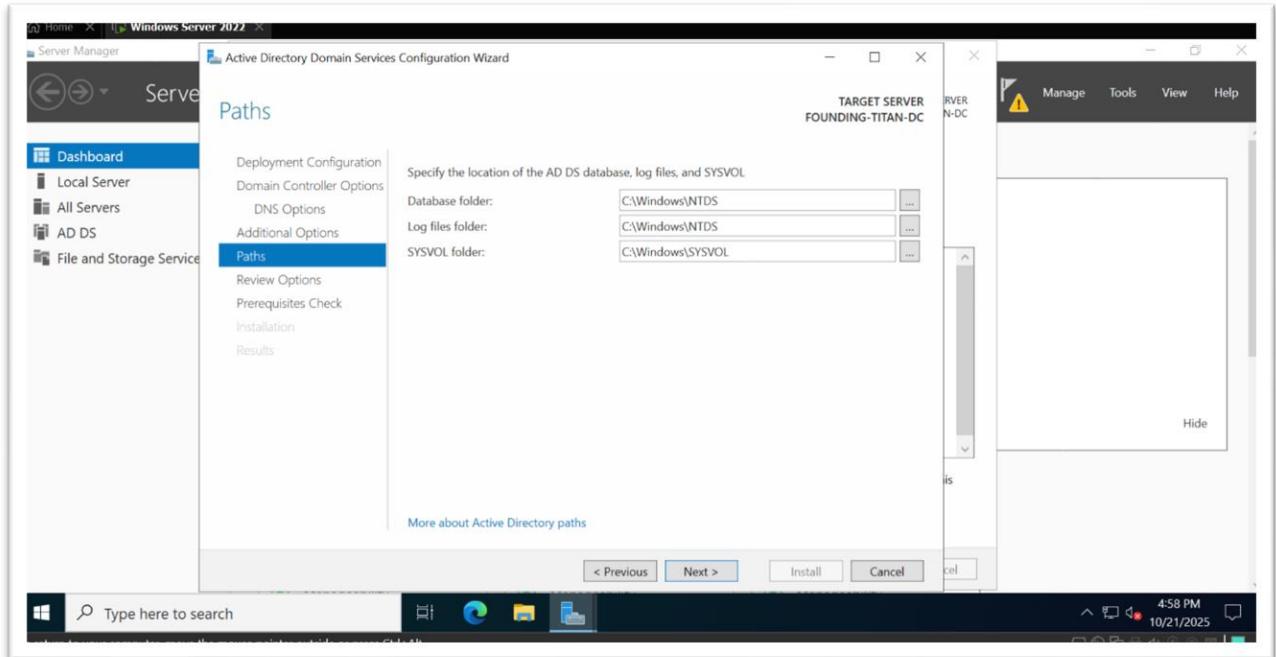
1.1. Specify Domain name for Domain Controller

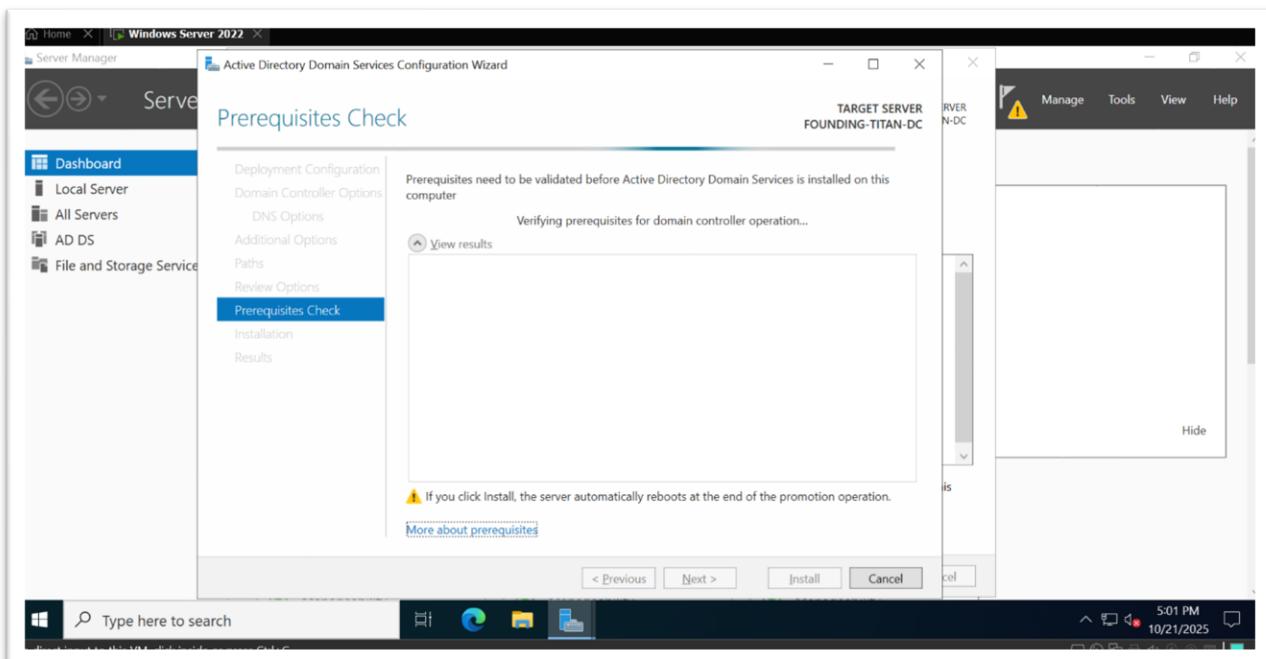
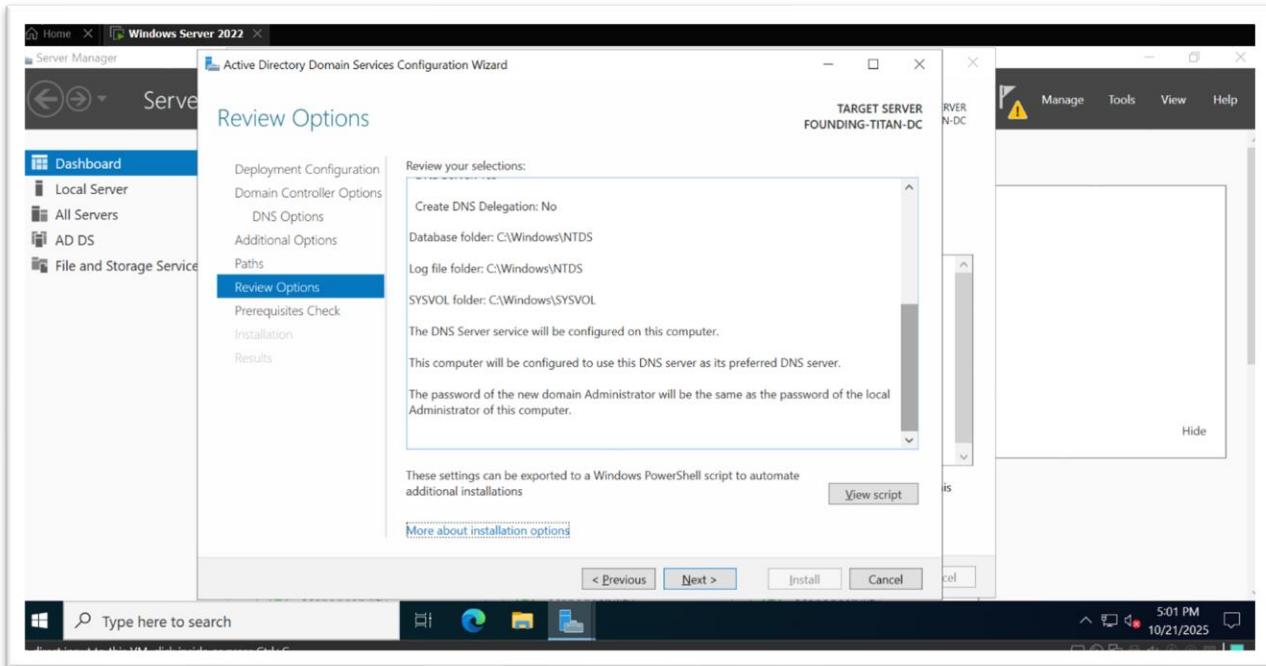


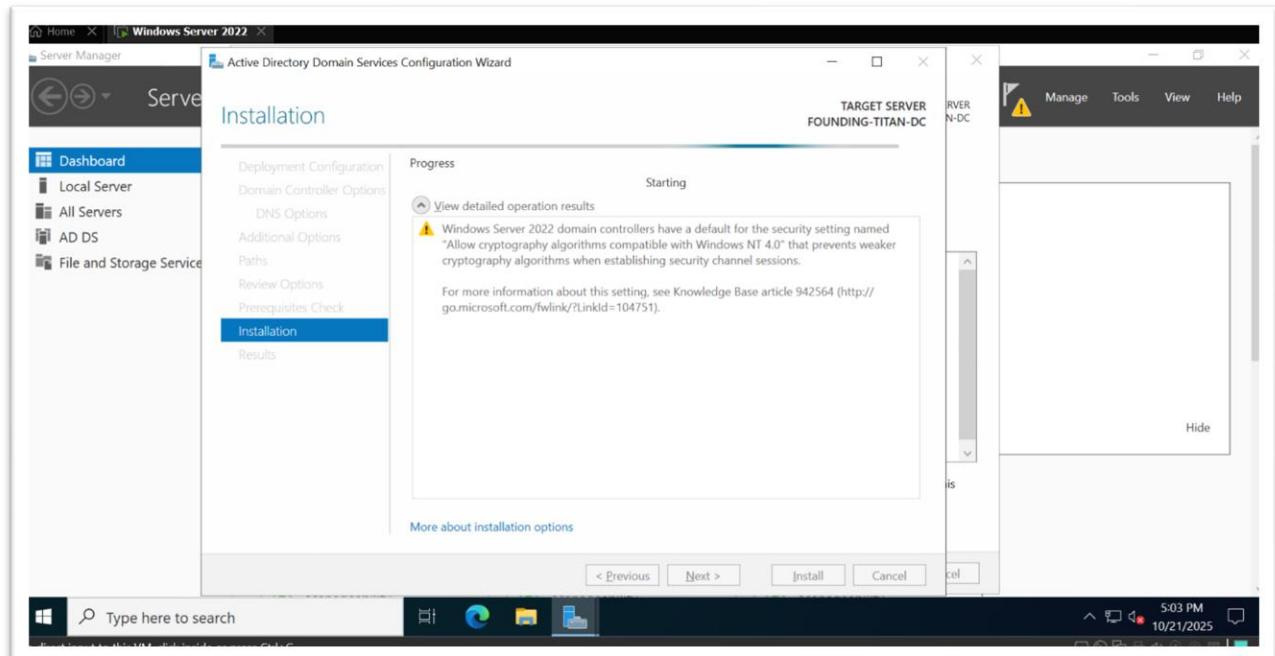
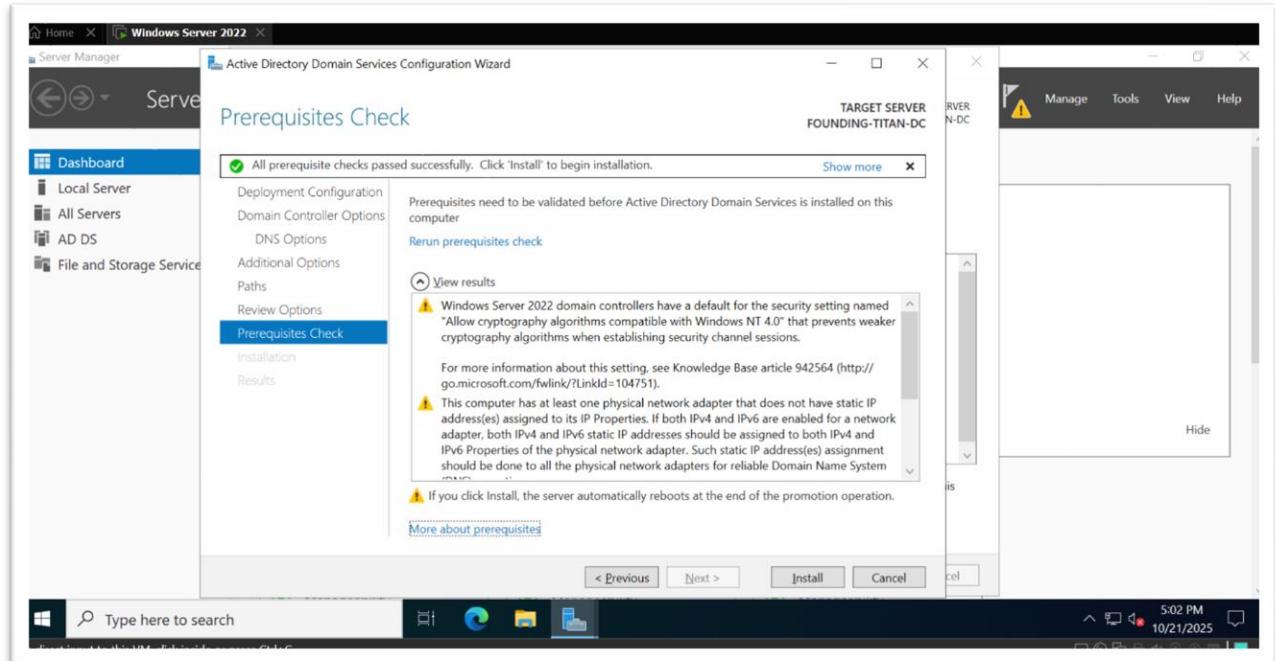


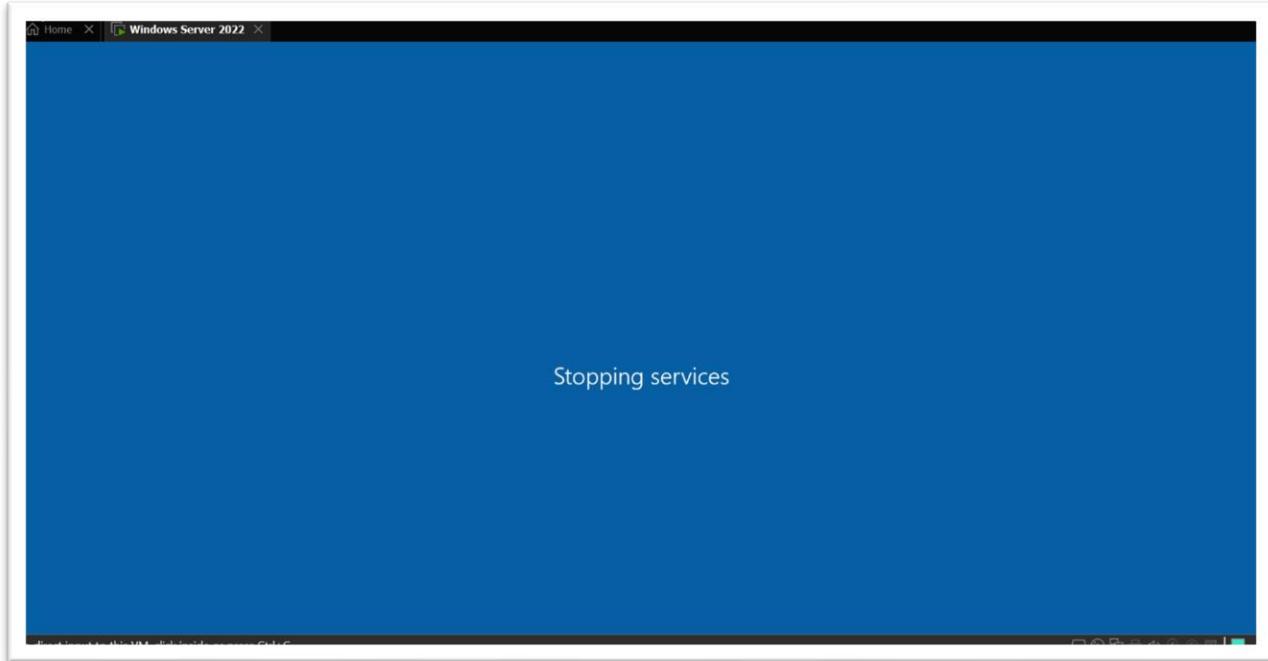
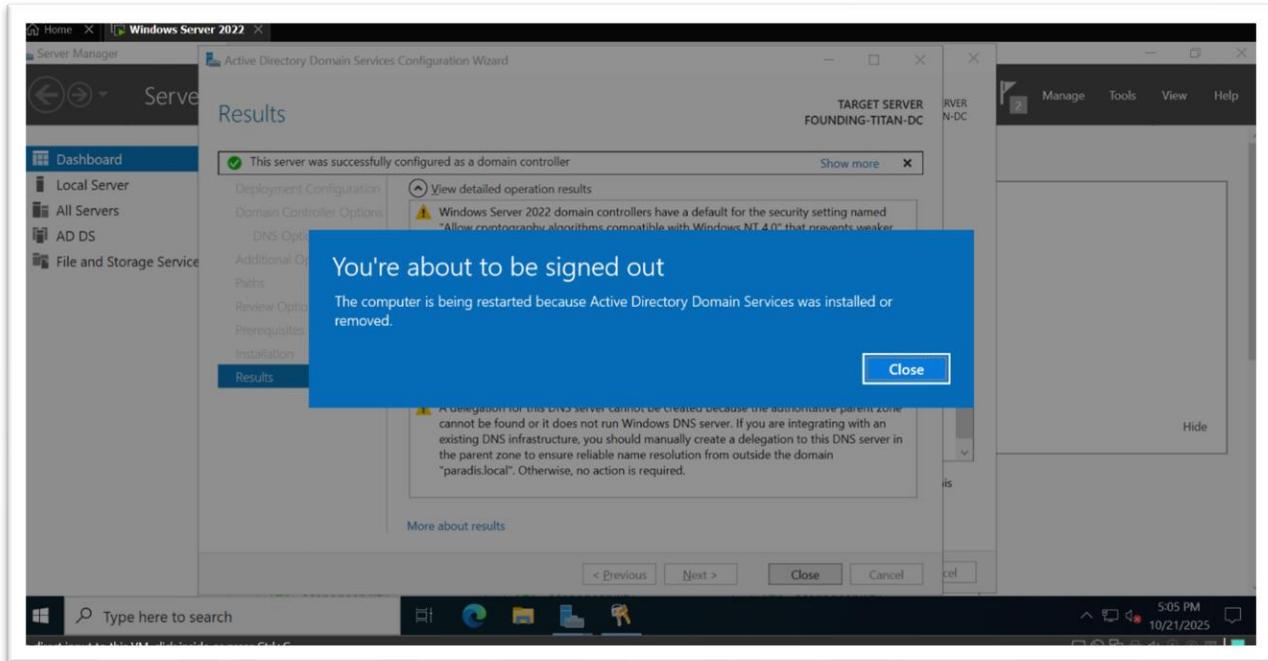




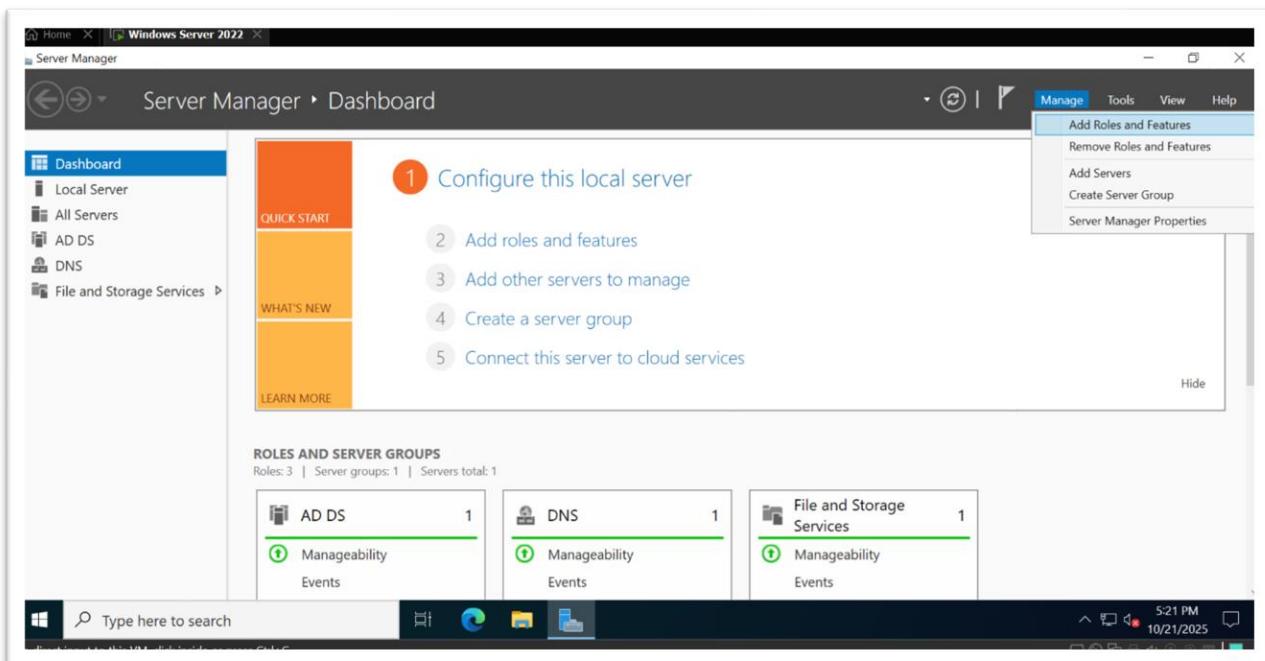
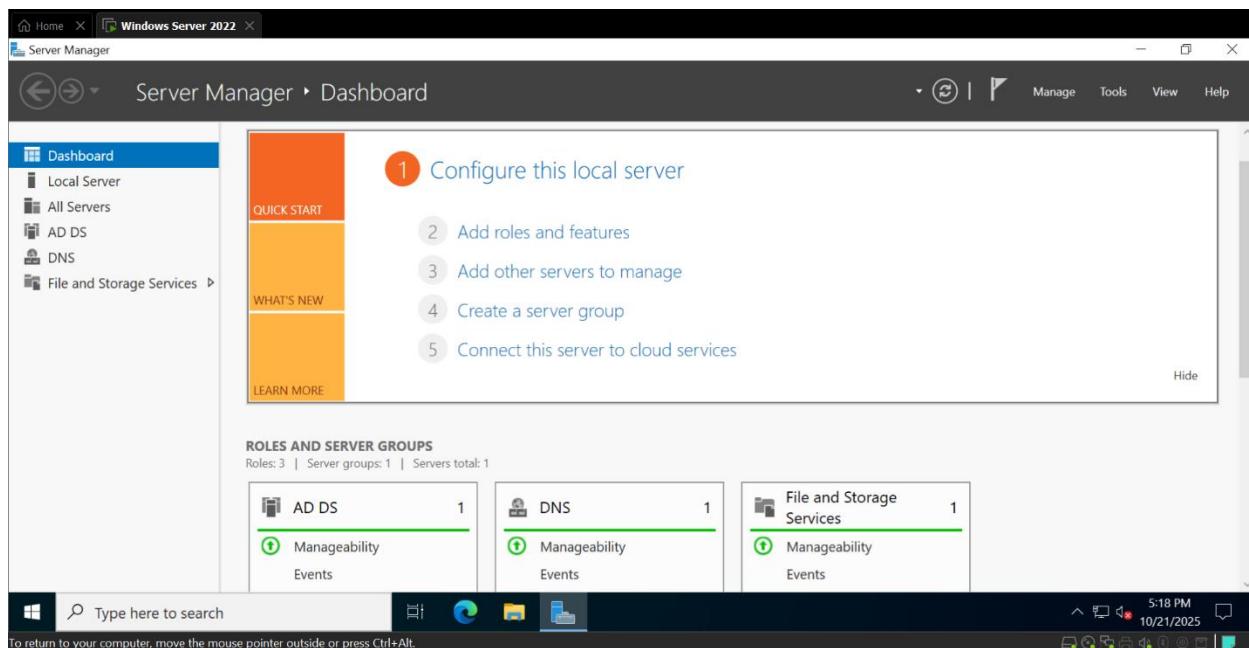


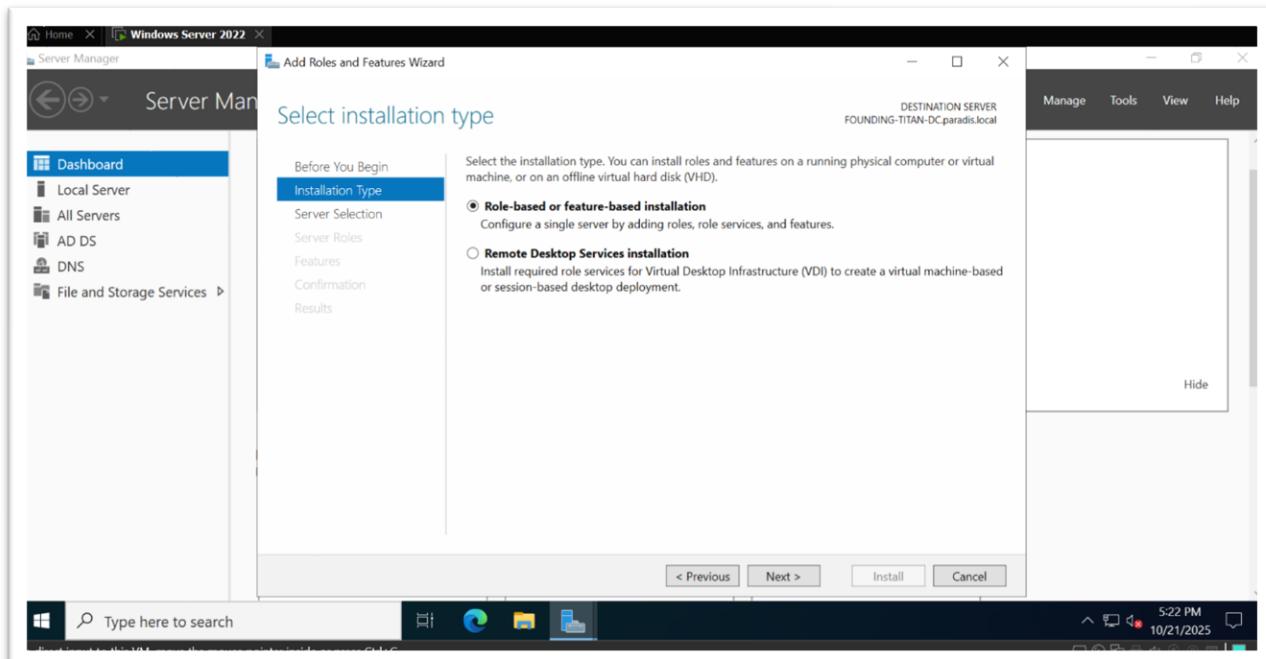
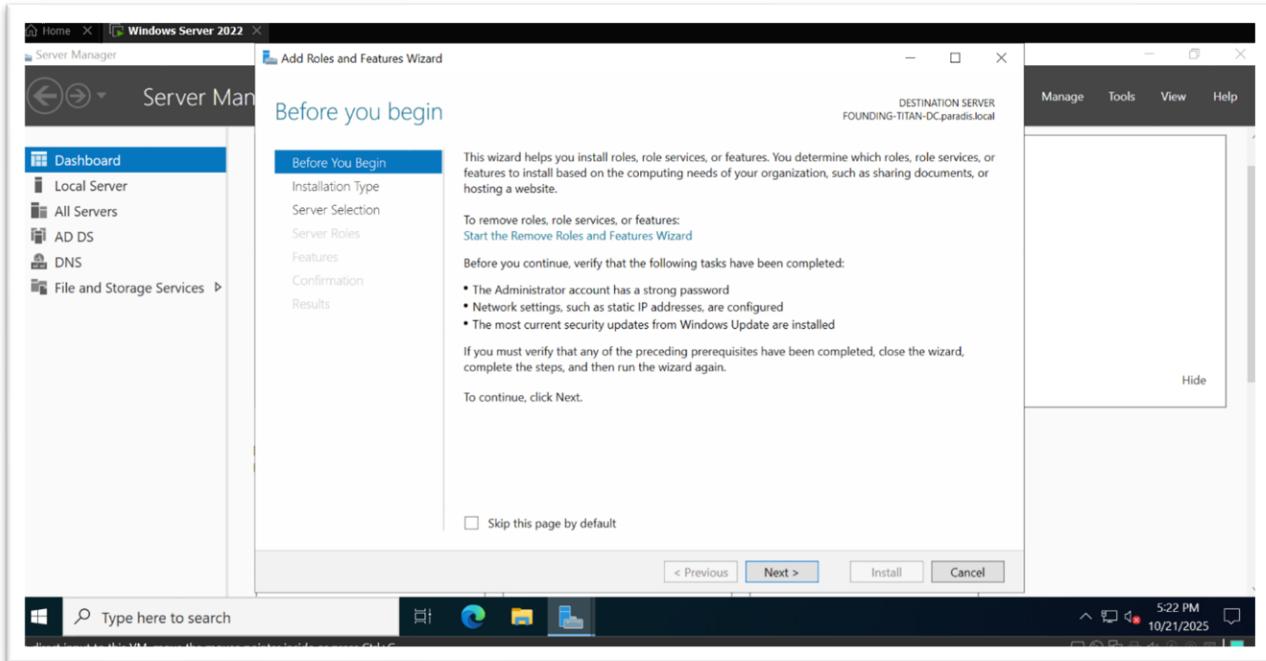


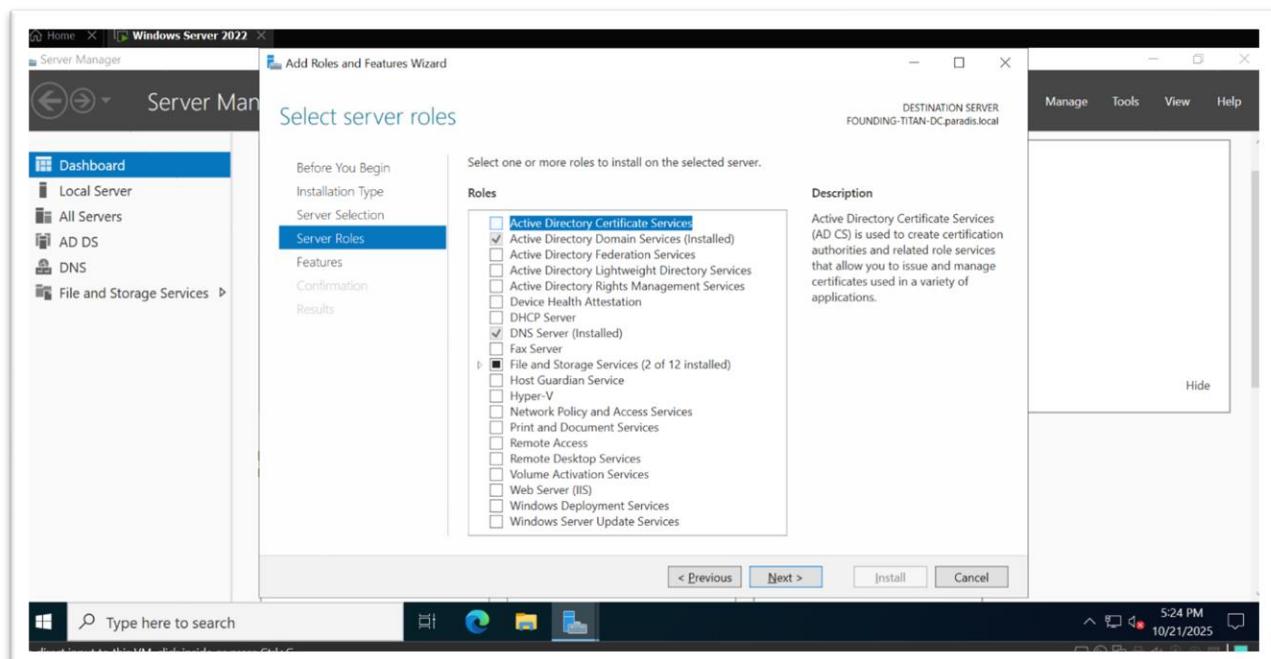
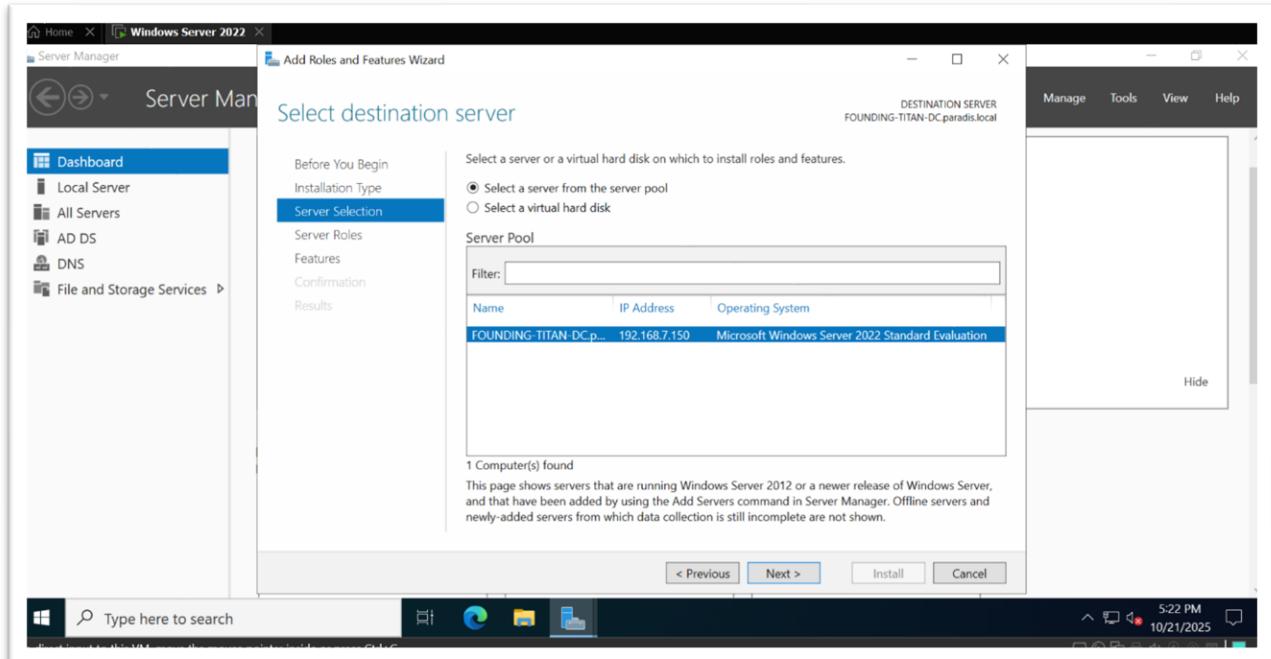


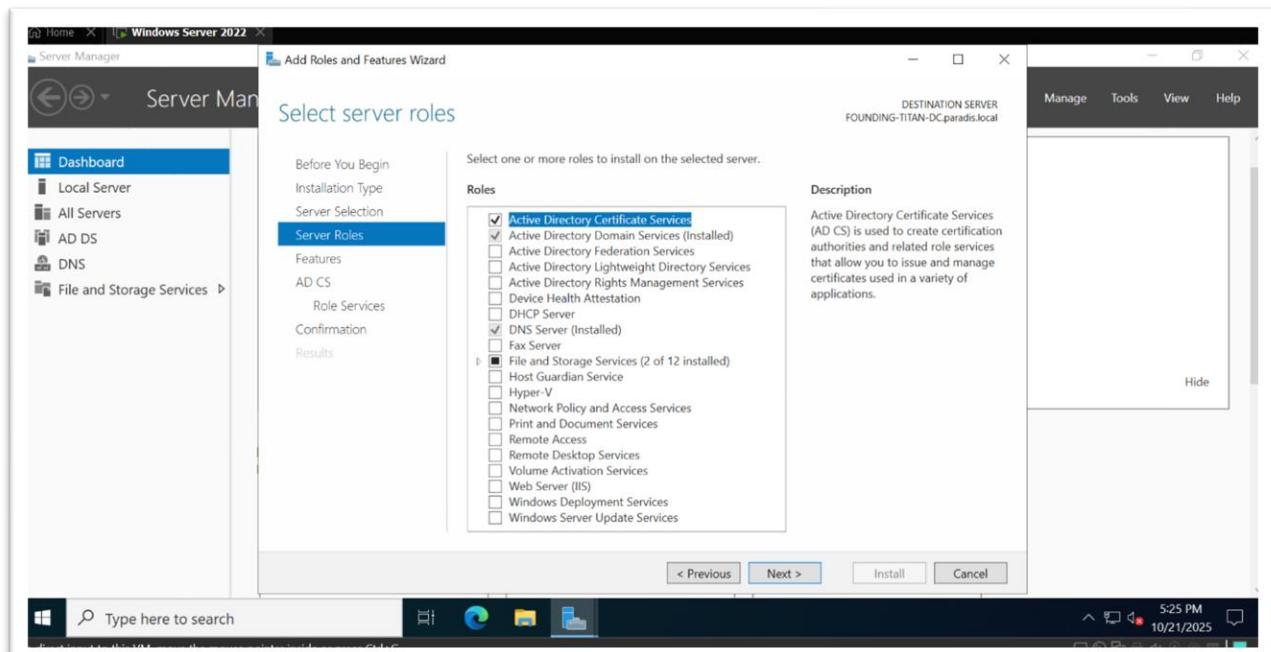
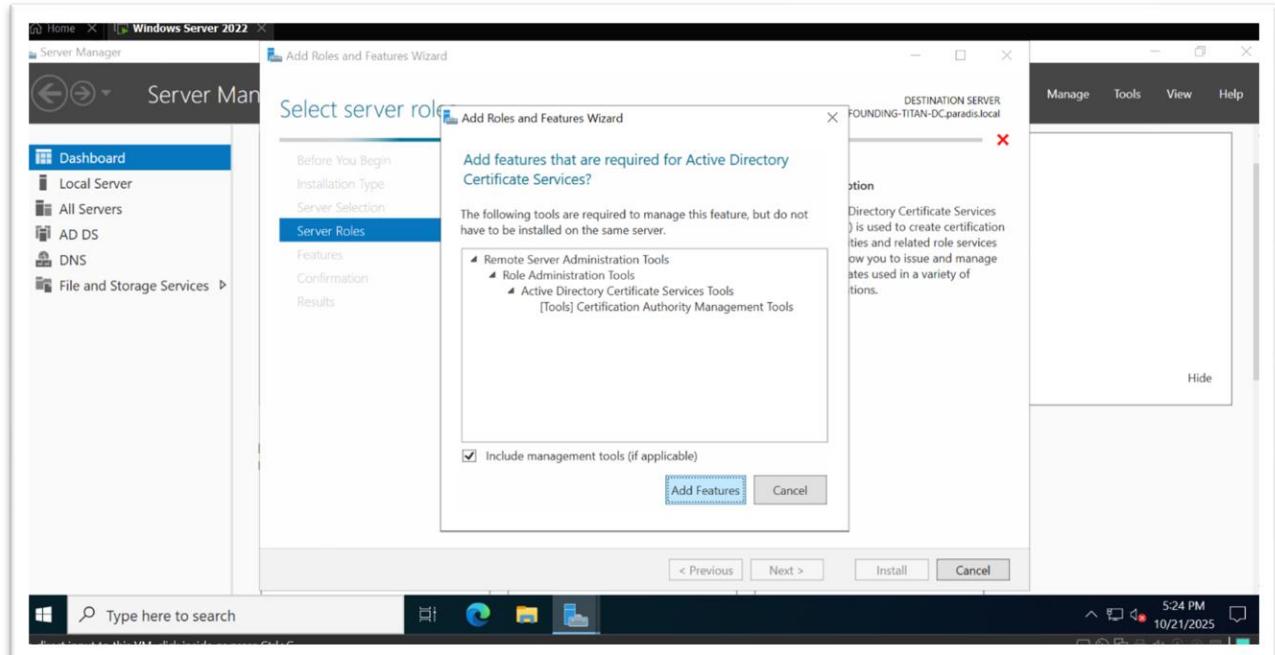


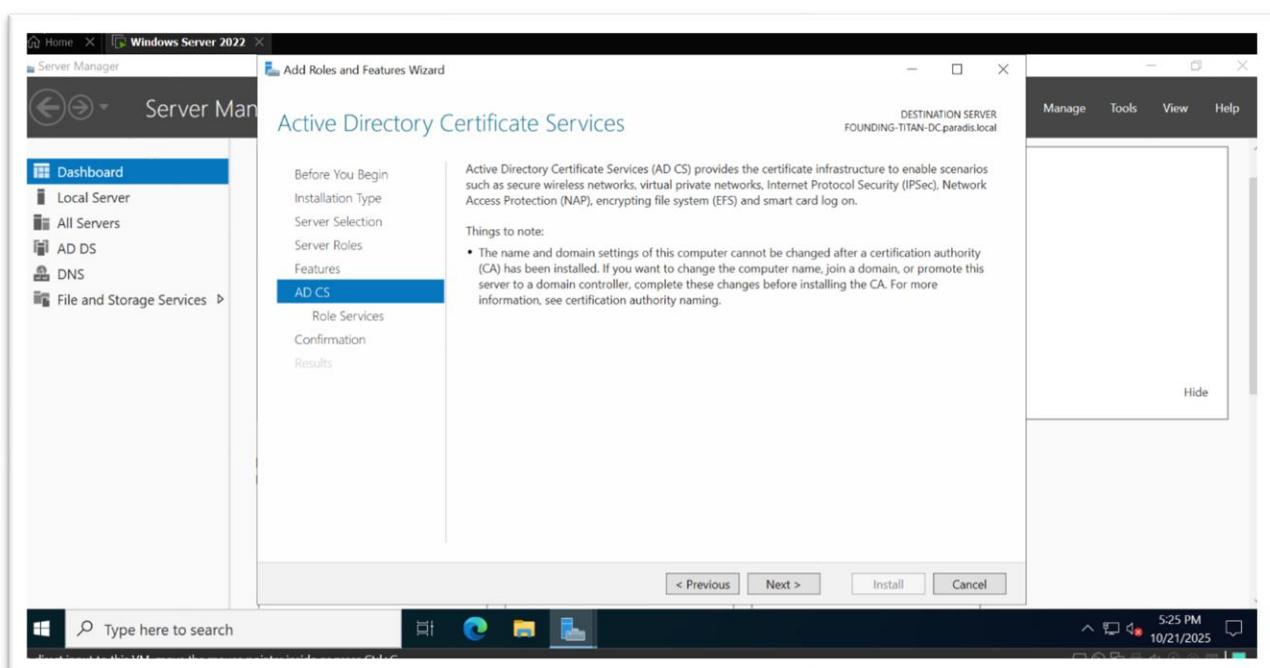
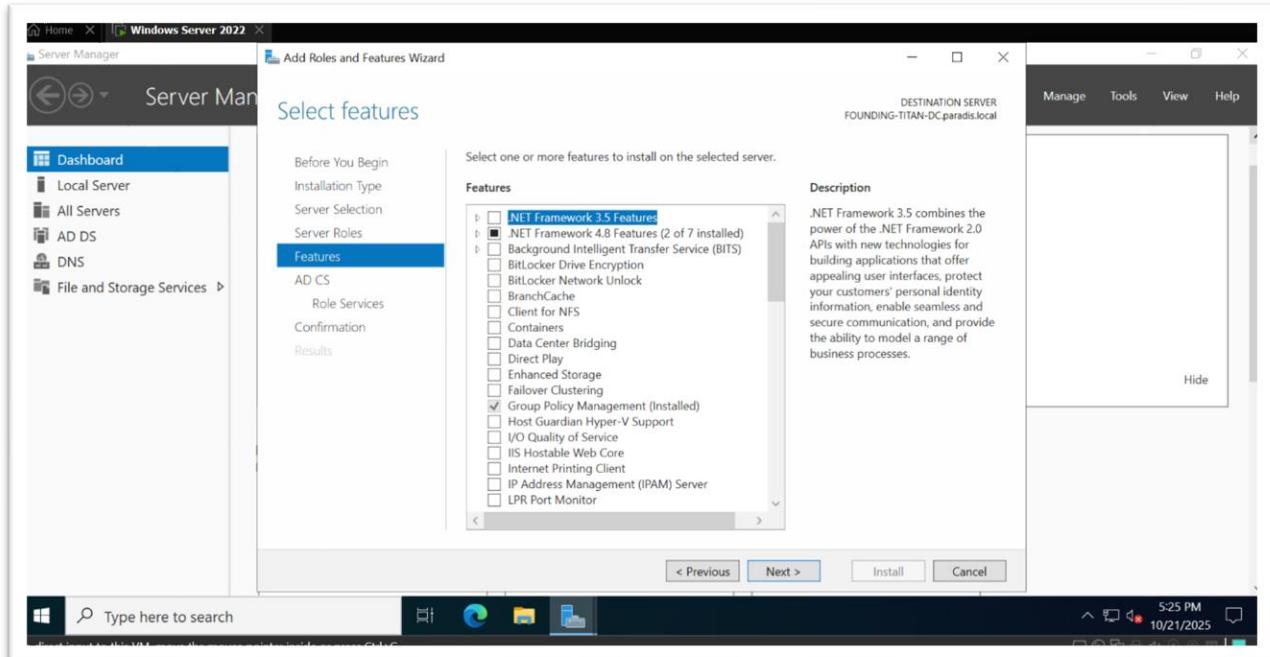
2. Add “Active Directory Certificate Services” role

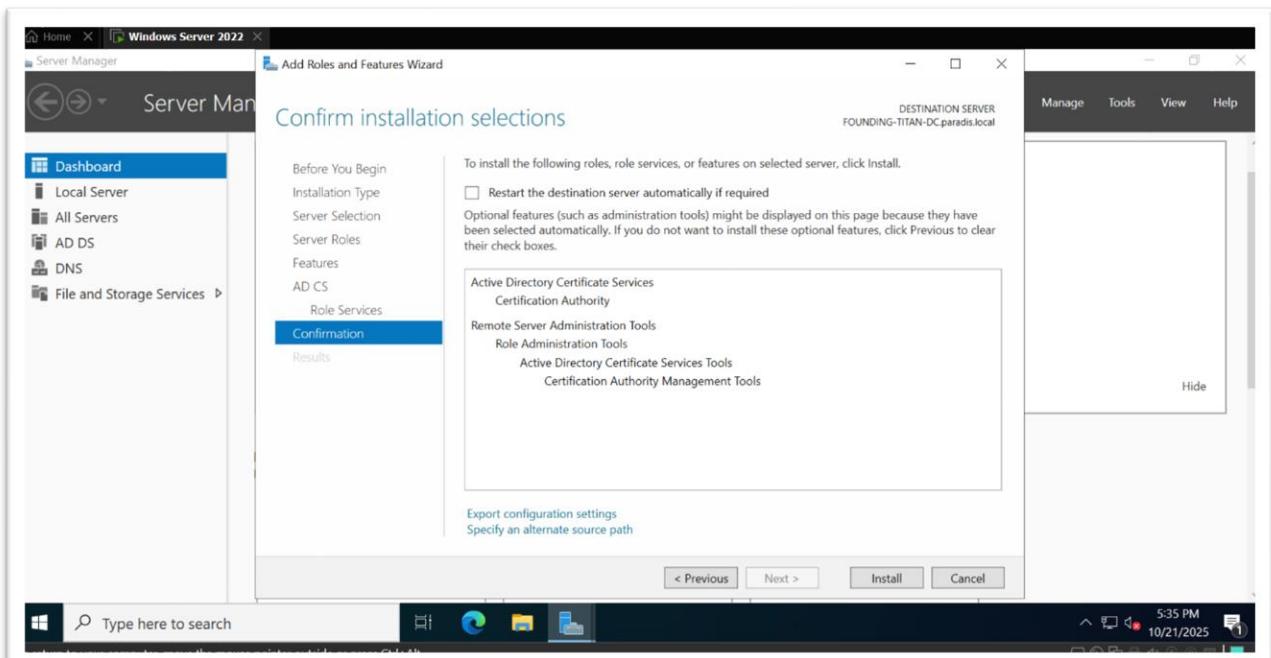
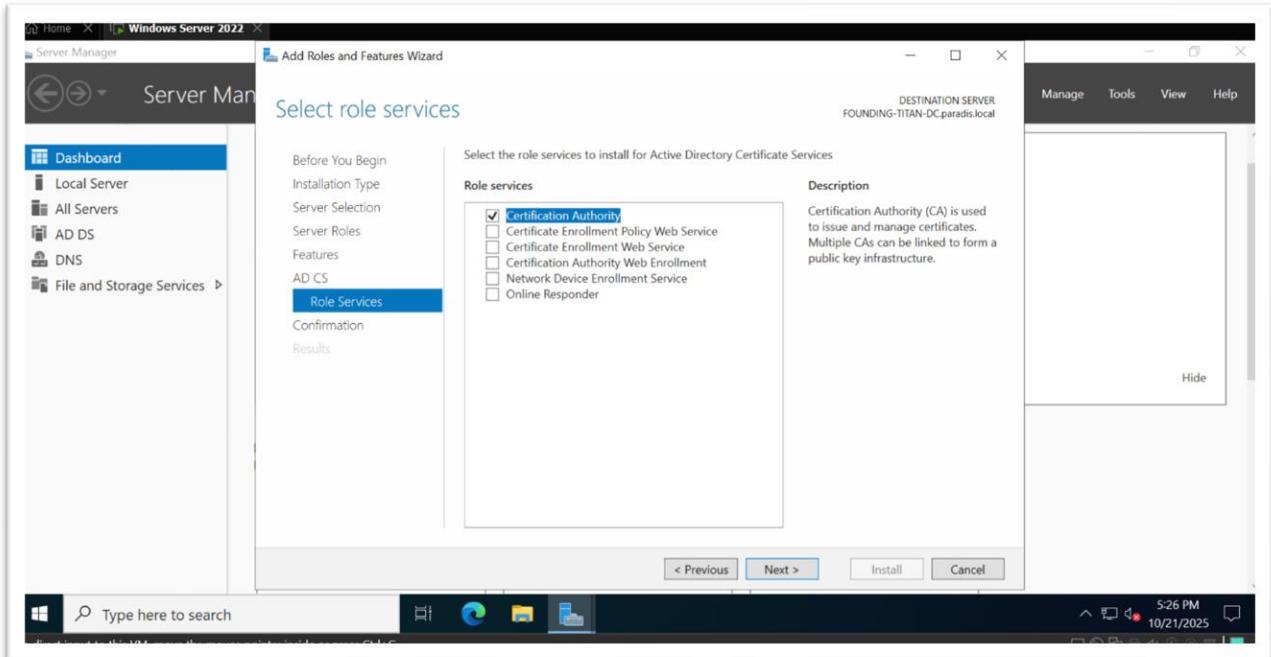


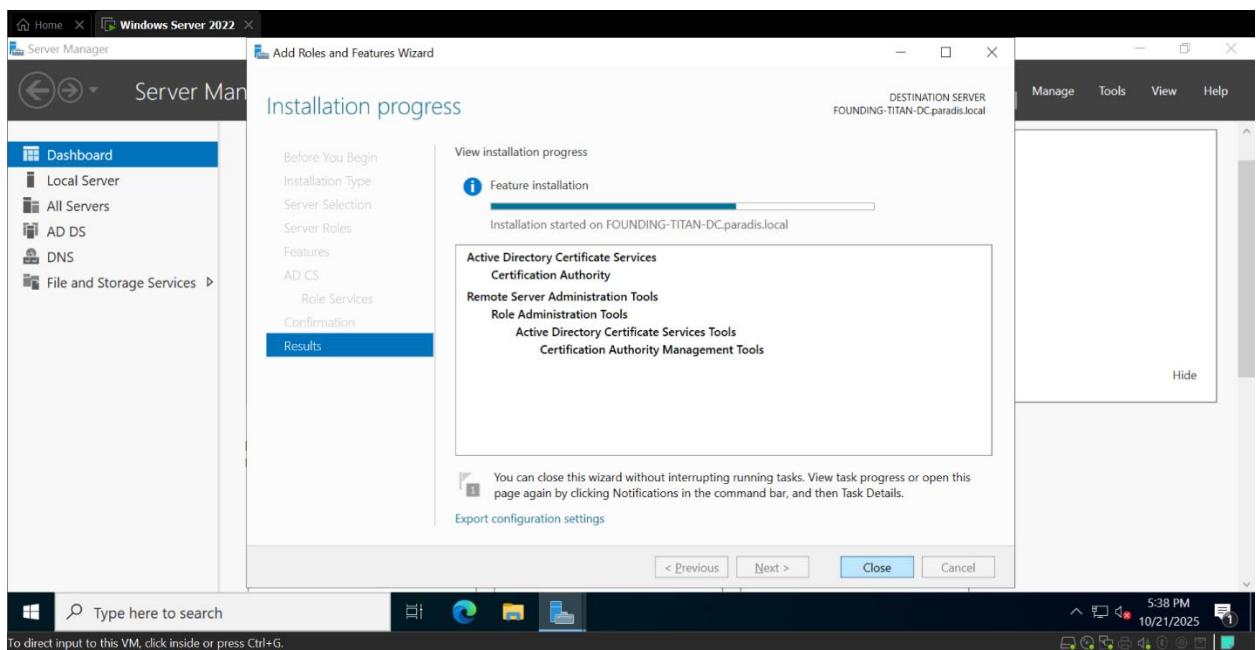
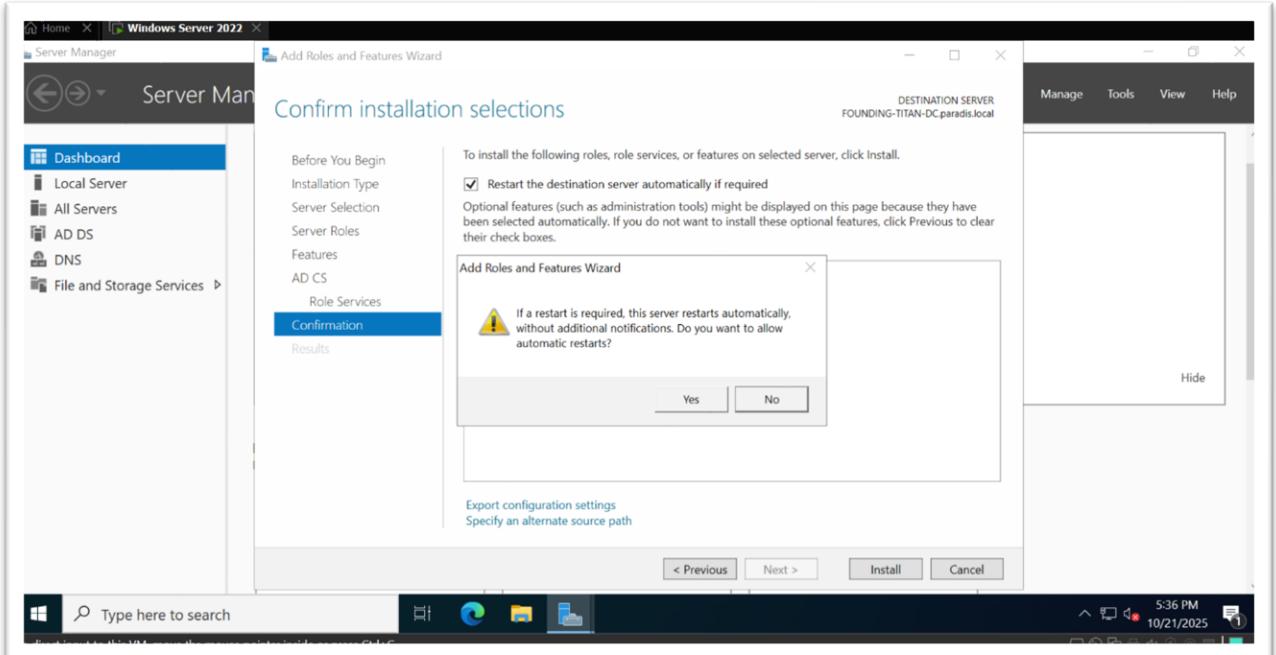


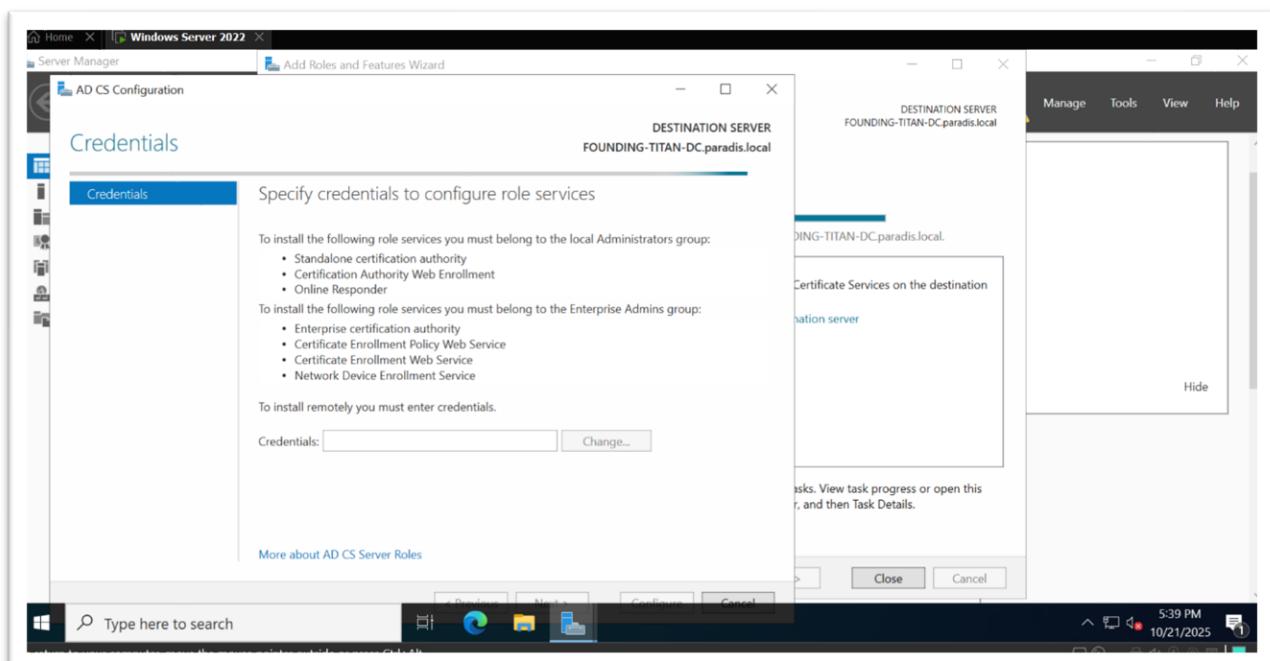
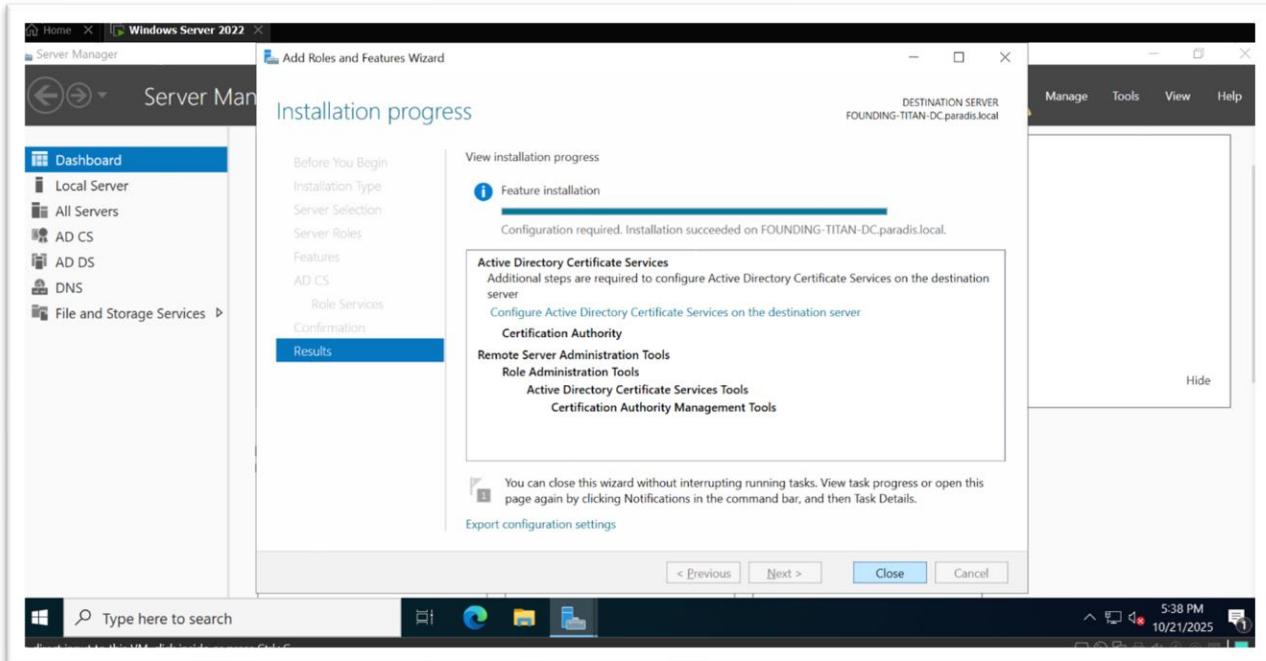


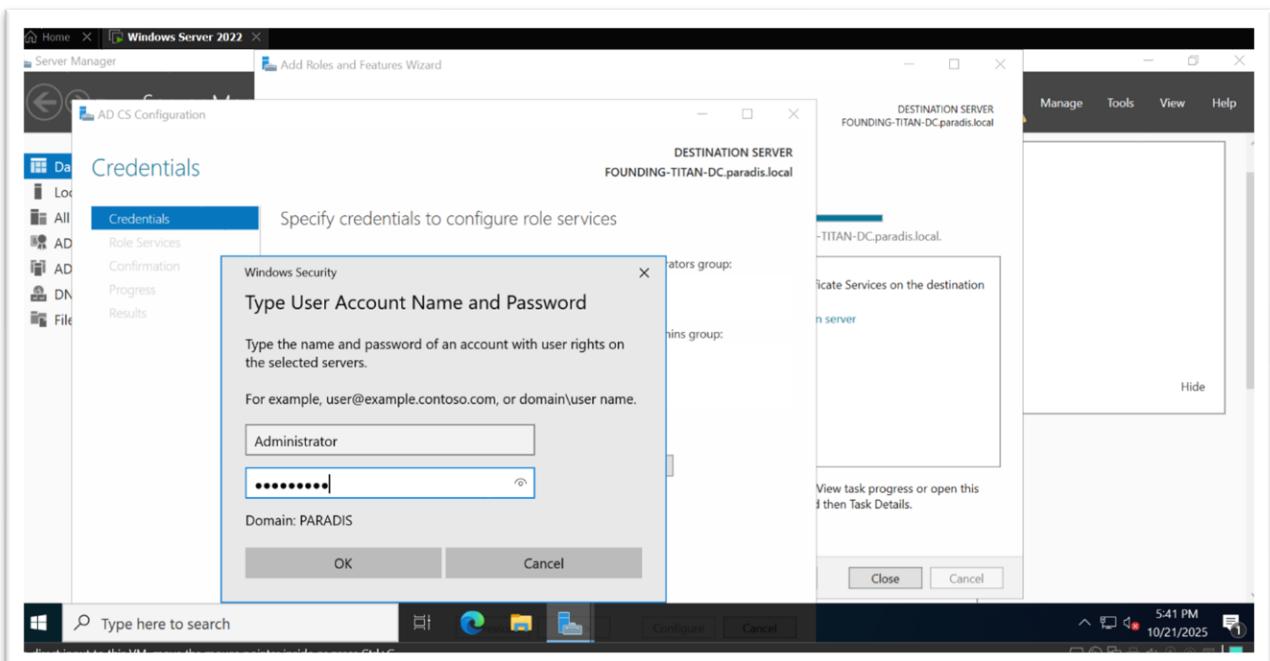
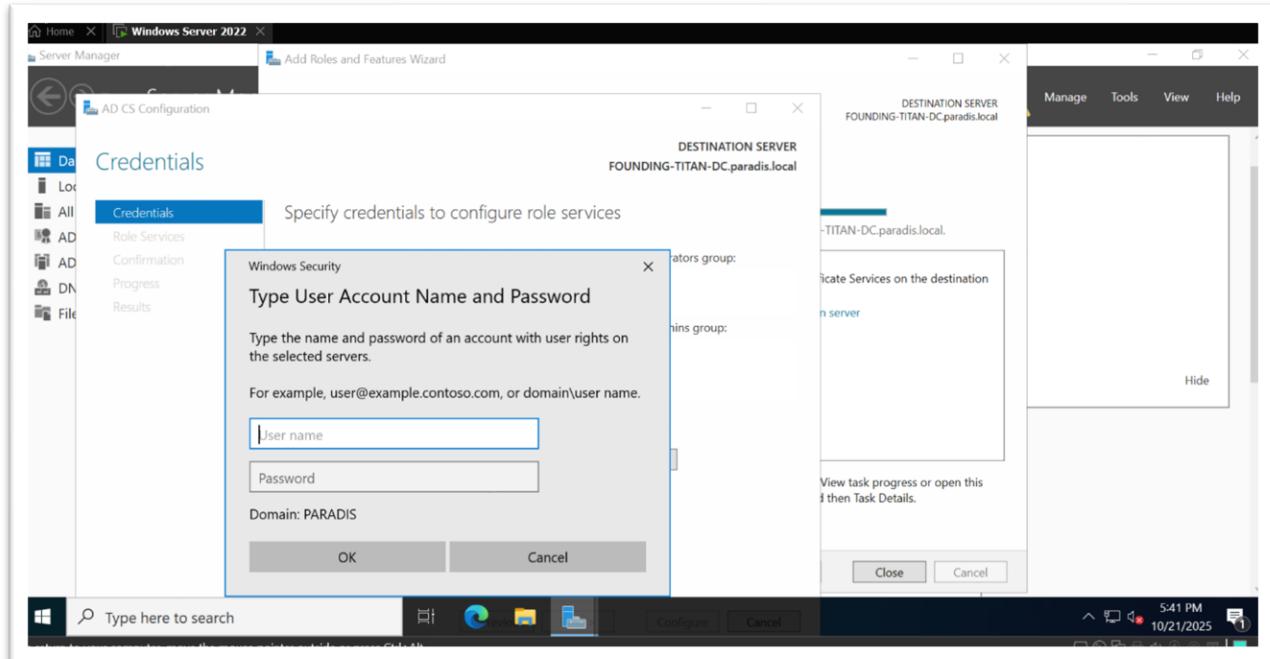


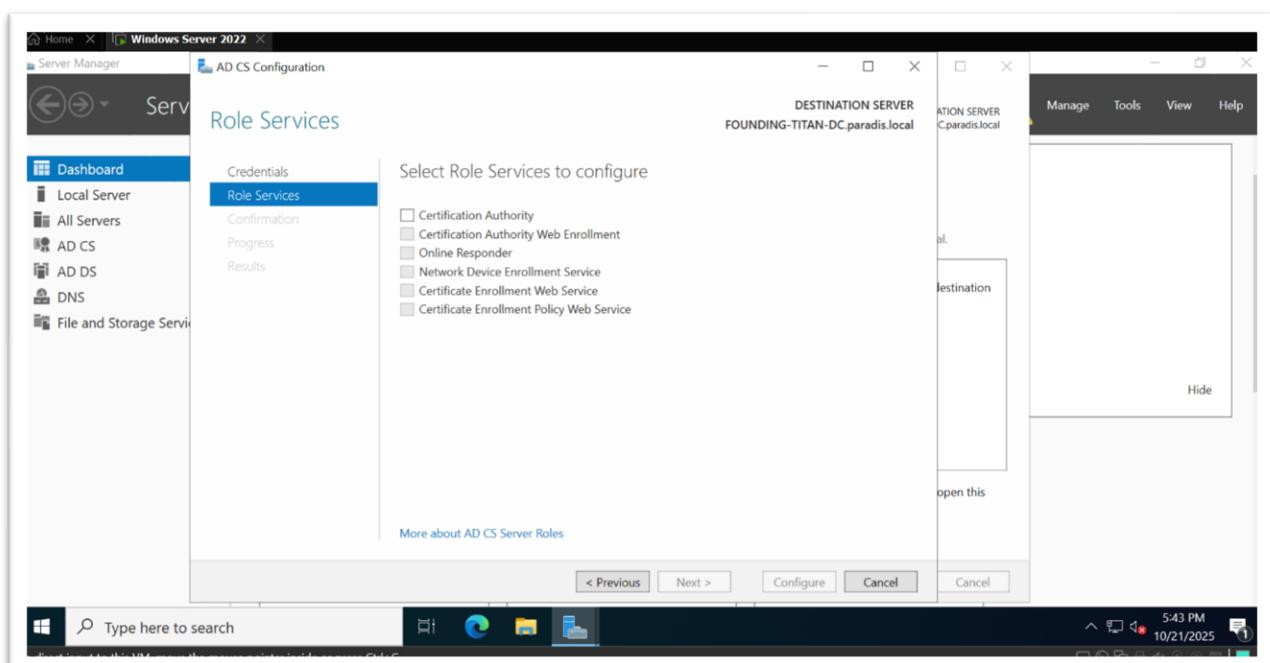
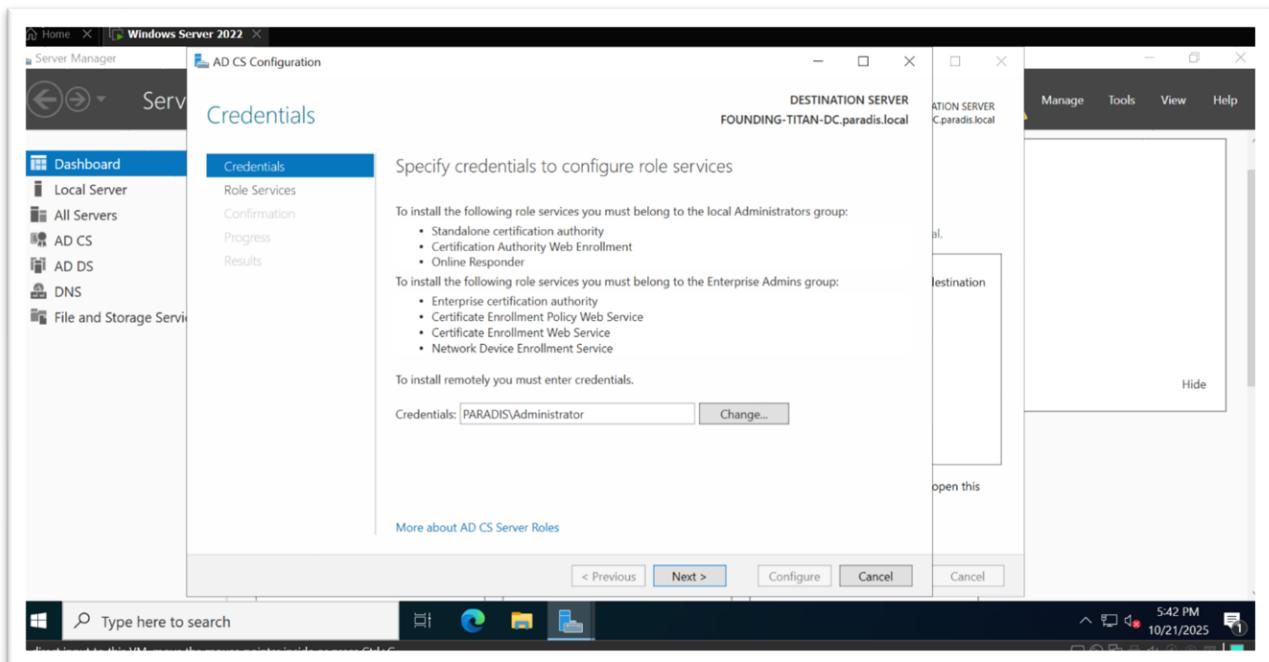


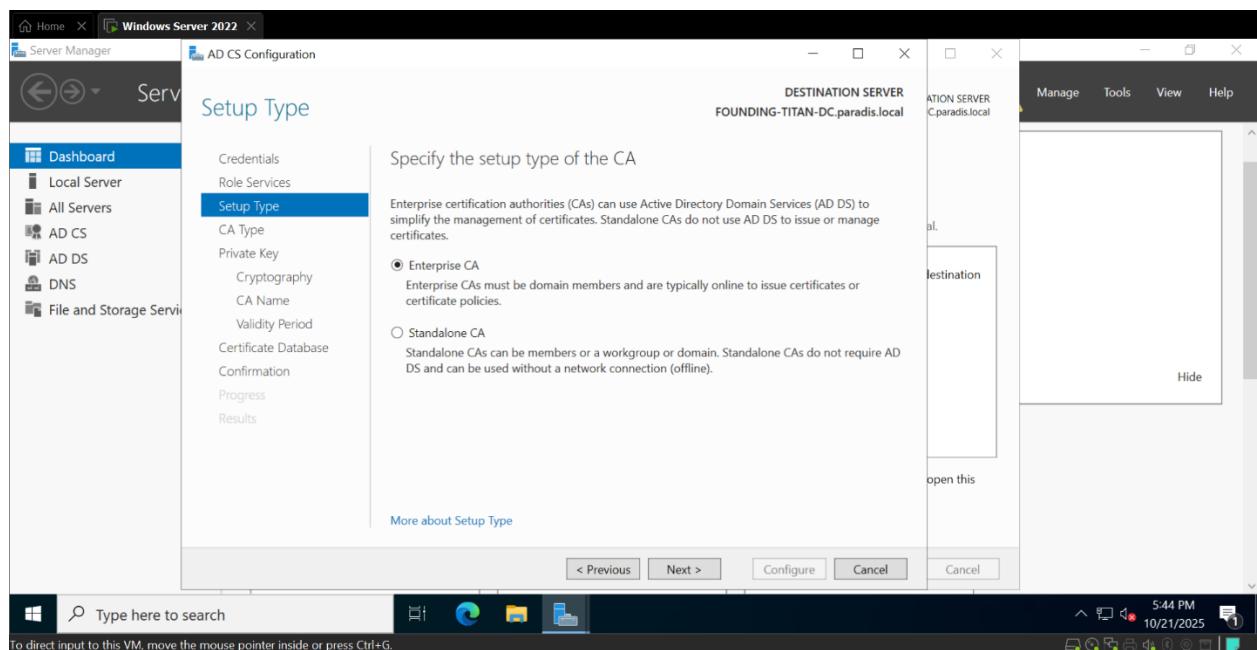
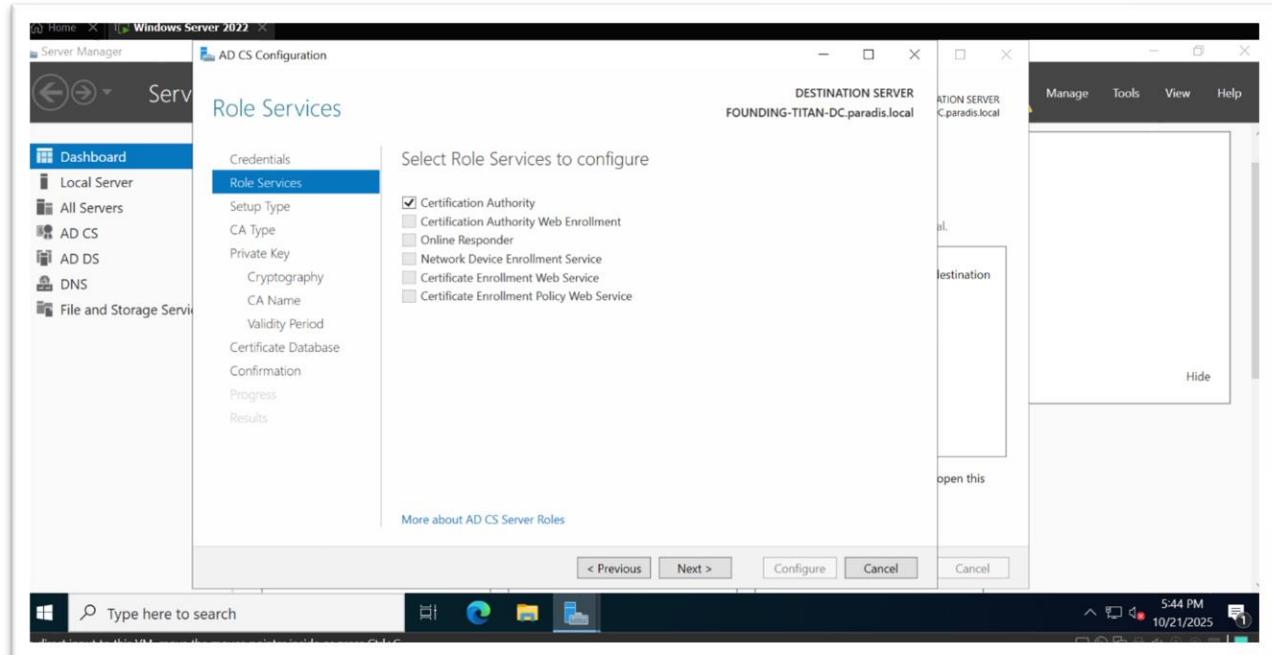


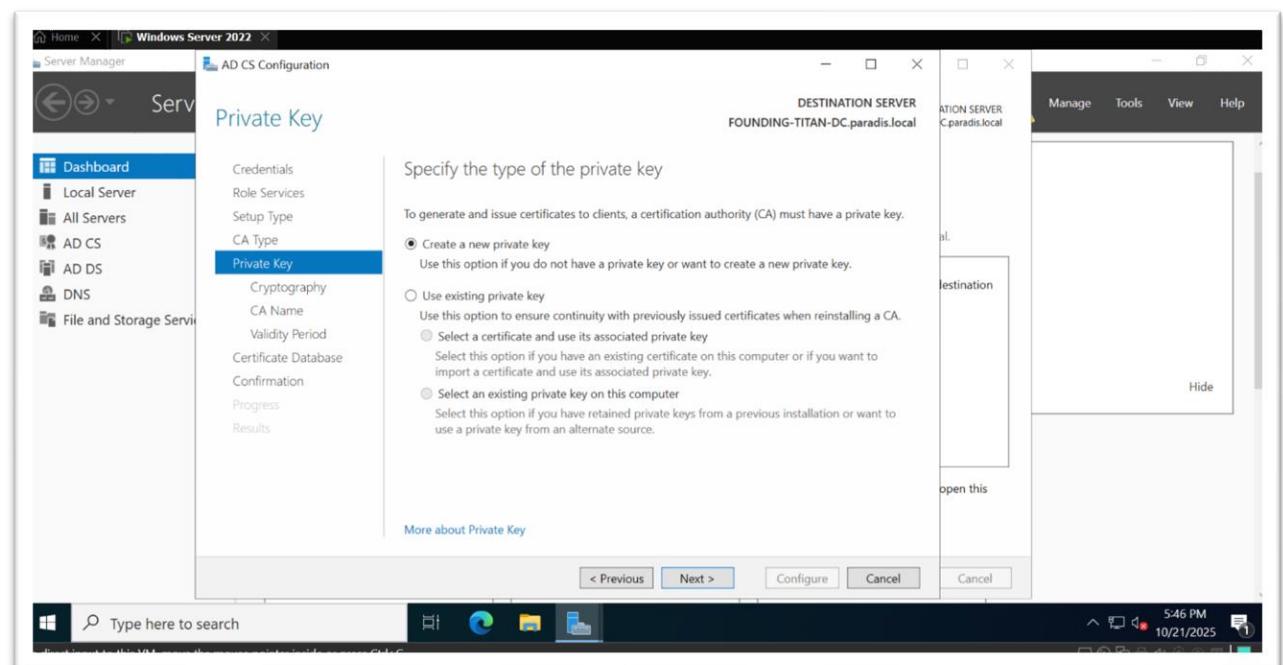
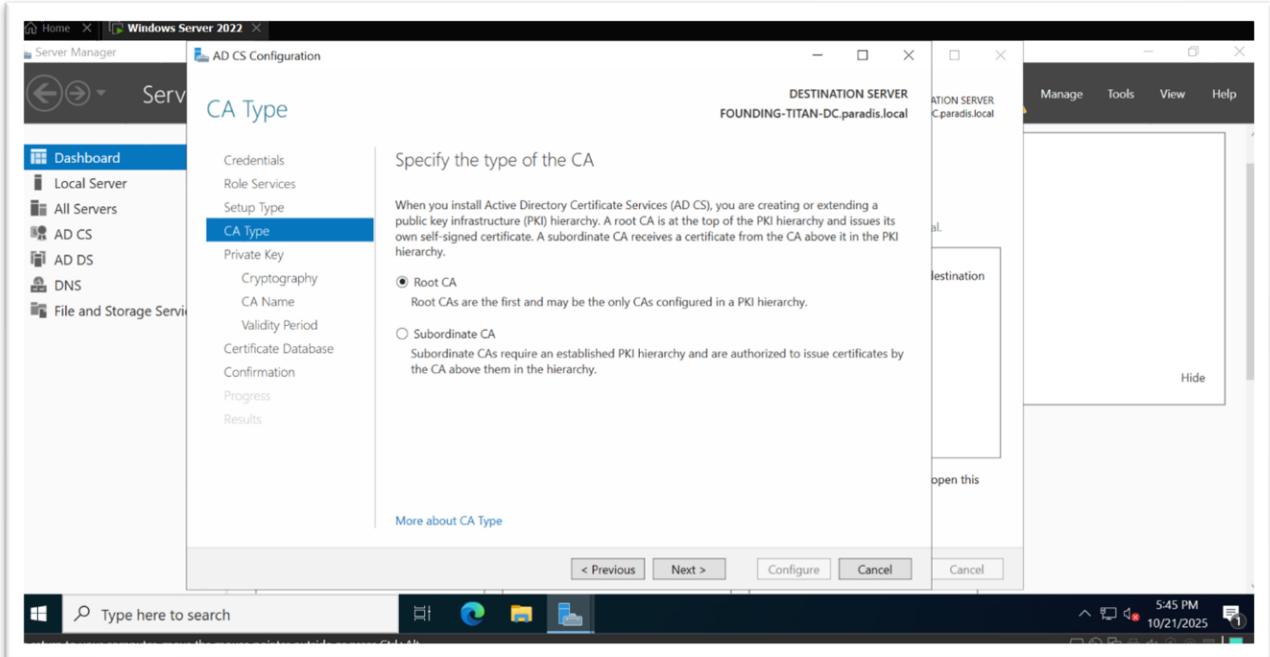


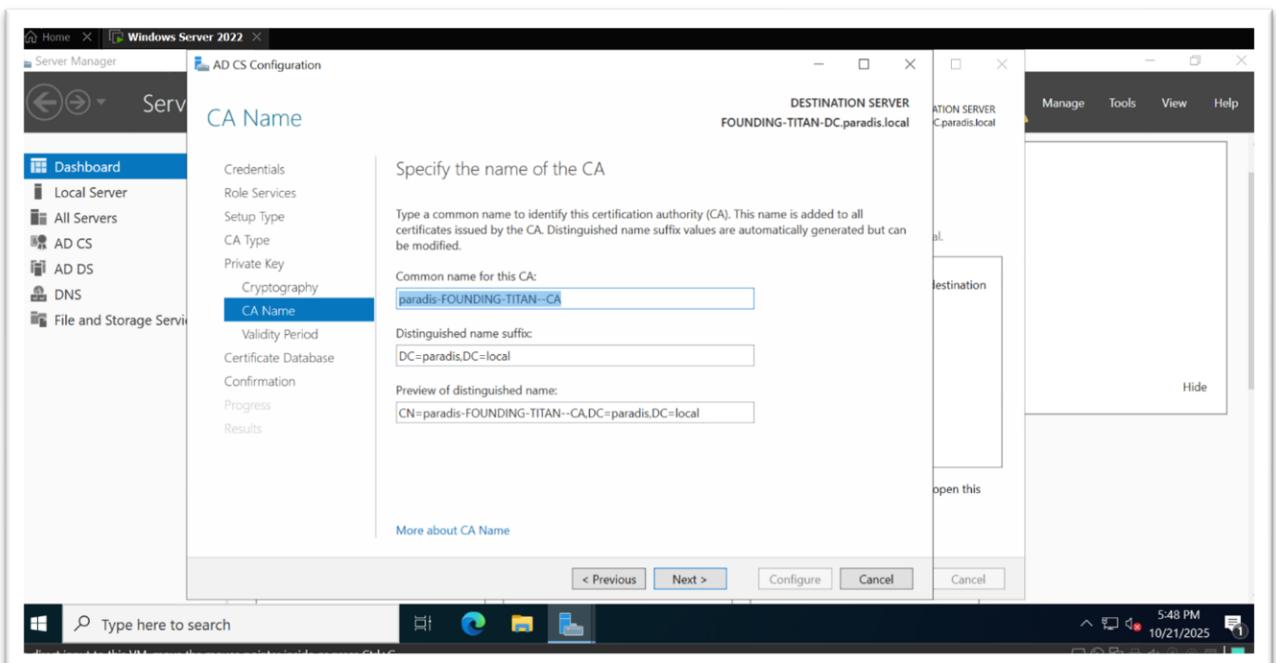
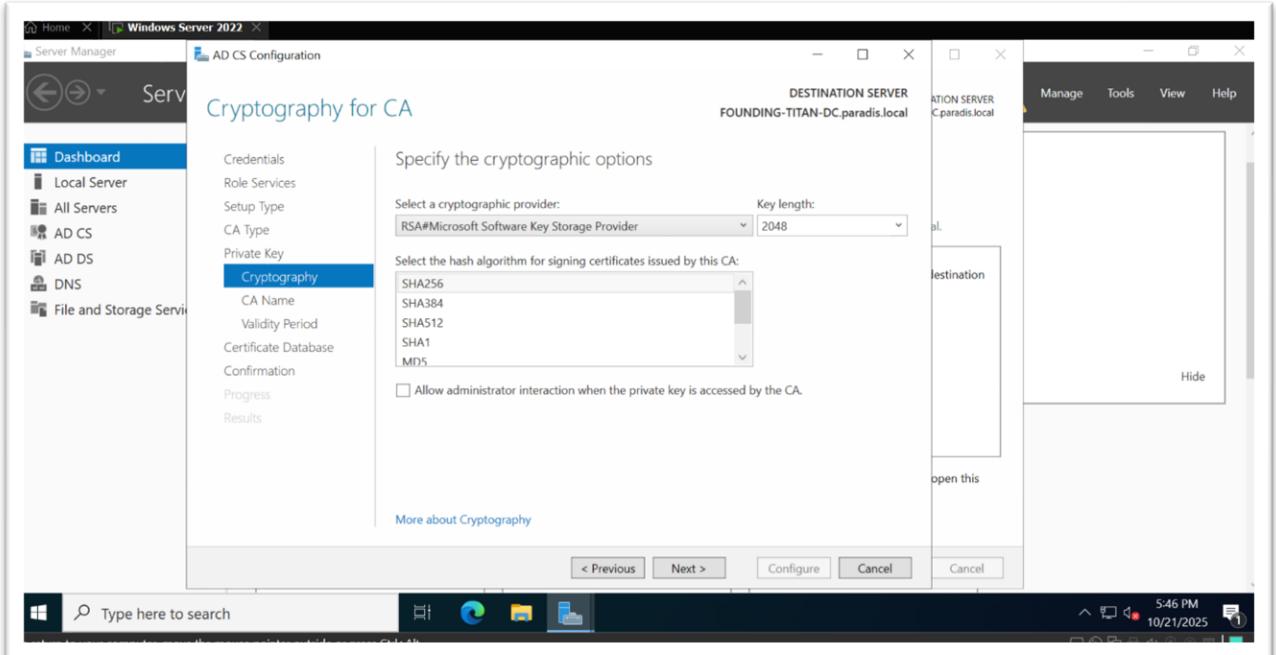


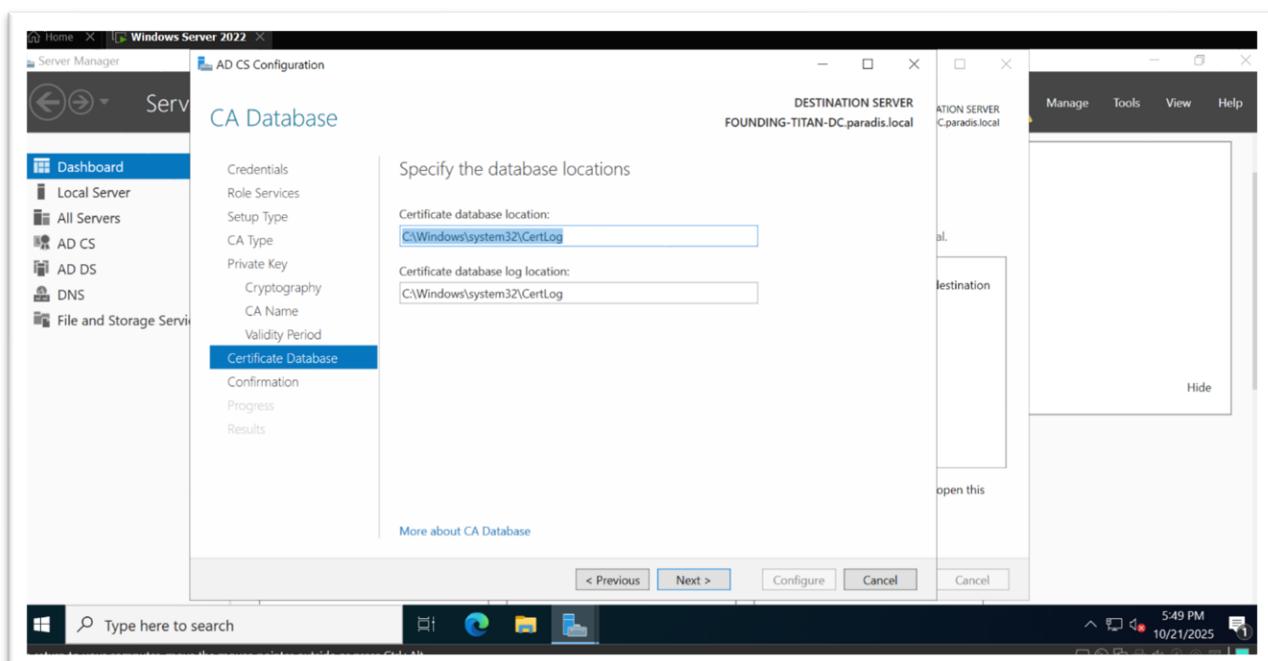
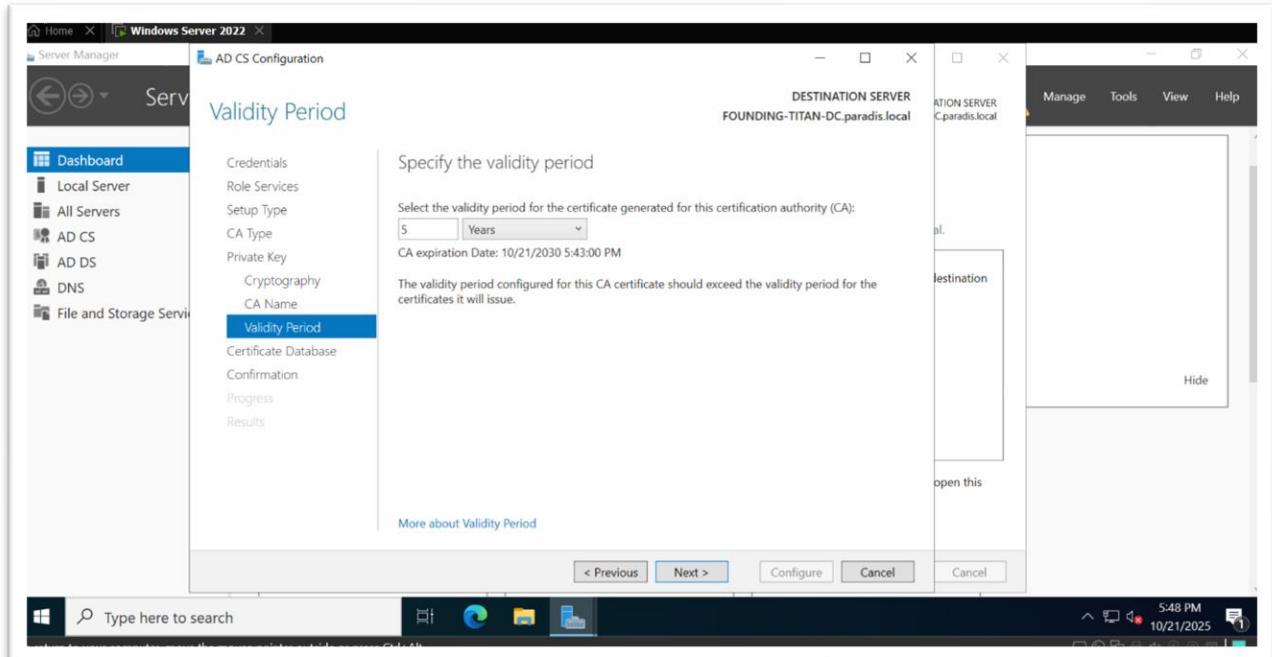


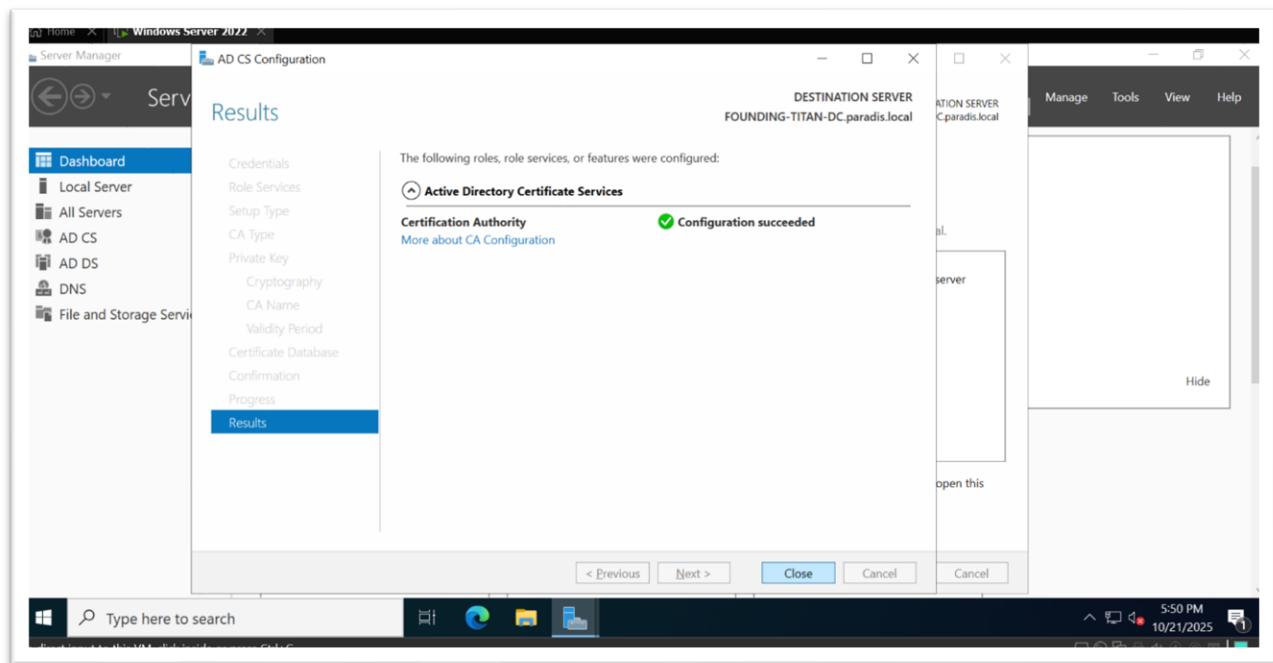
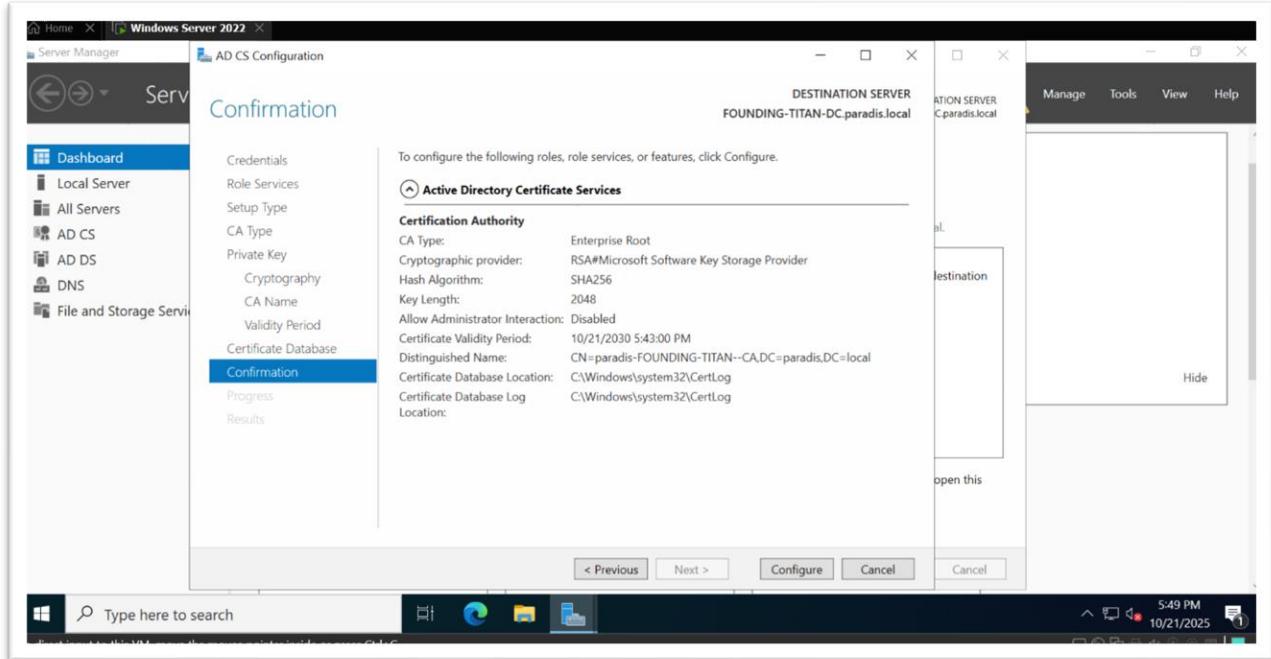












Step 3: Create Domain Users

