Active Directory (AD) is a core component of Microsoft’s Windows Server environment that

provides centralized management of users, computers, and network resources. It enables

administrators to organize and control access to information, enforce security policies, and

streamline network administration across an organization.

Setting up Active Directory is a crucial step in building a secure and efficient IT infrastructure. It

allows organizations to manage authentication, authorization, and directory-based services

through a single, unified system. Whether you’re deploying it in a small business or a large

enterprise, understanding the setup process ensures a stable and scalable environment.

This guide provides a step-by-step walkthrough for installing, configuring, and verifying

Active Directory Domain Services (AD DS) on a Windows Server. By following these steps, you

will learn how to:

 Prepare your server environment for AD installation

 Install the Active Directory Domain Services role

 Promote the server to a domain controller

 Configure DNS and domain settings

 Verify and manage your new domain

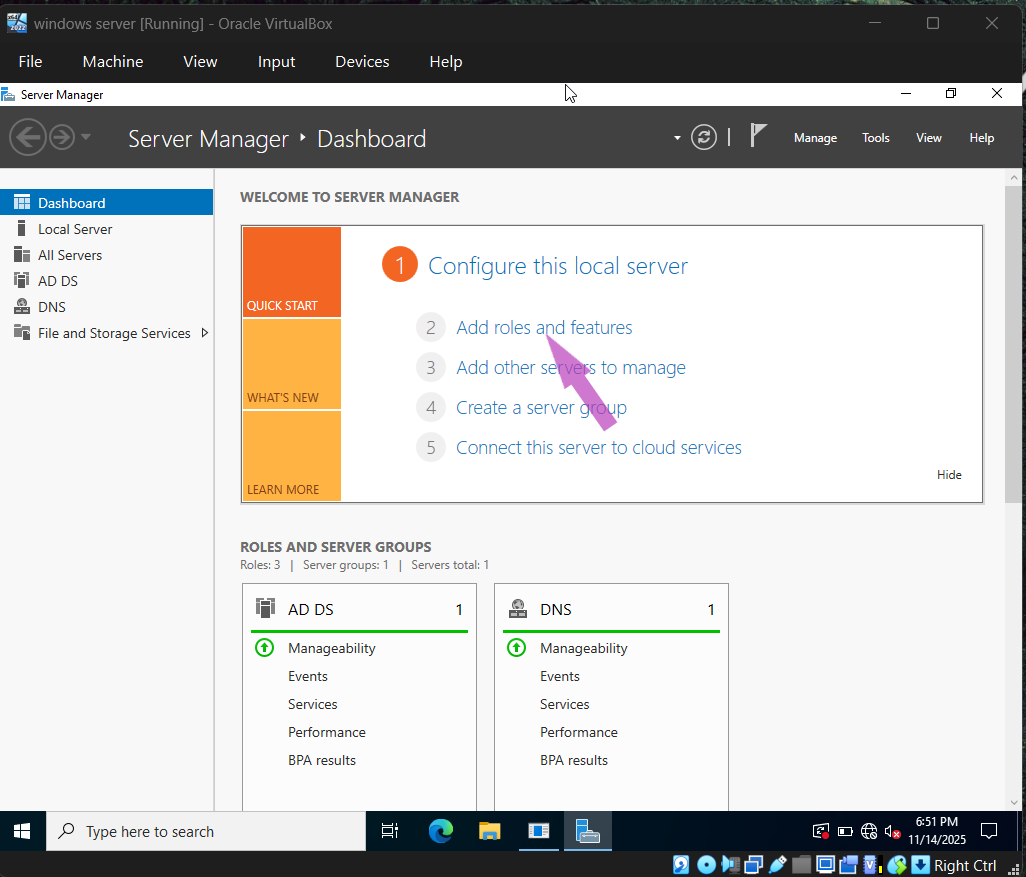
By the end of this guide, you will have a fully functional Active Directory domain ready to

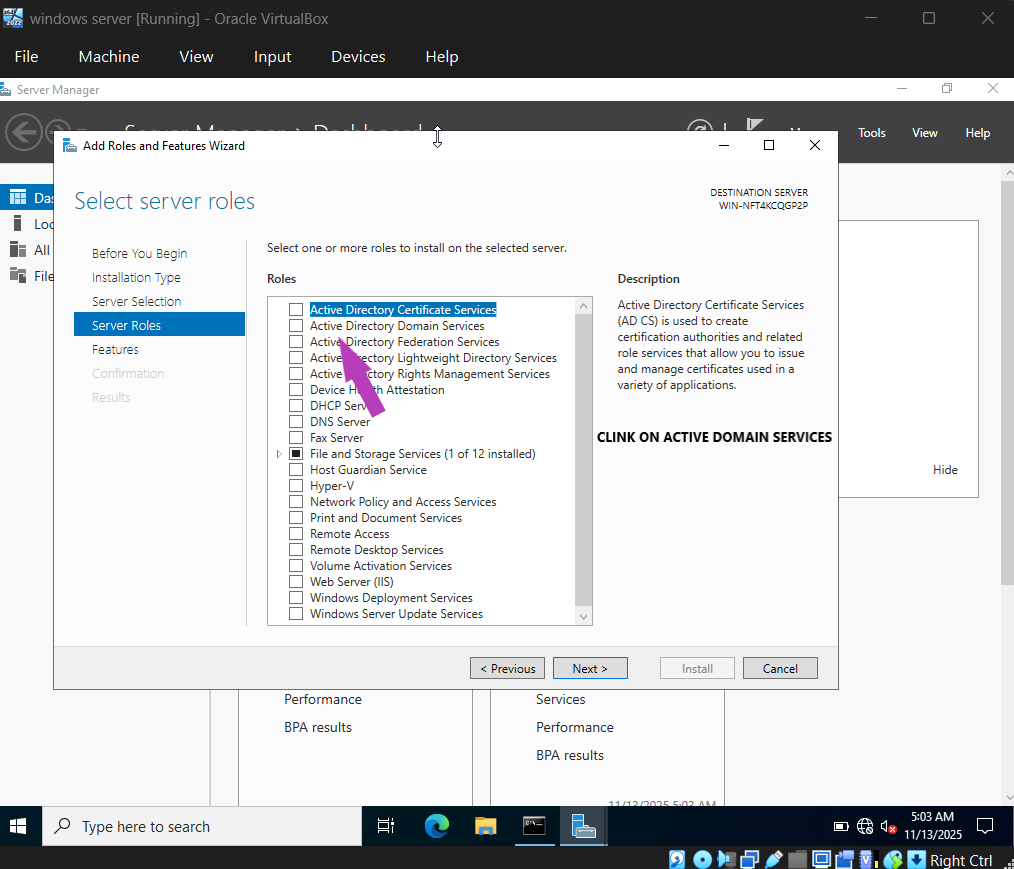
manage users, groups, and network resources within your organization.

On the server, we first need to install the AD, this can be done on the server manager dashboard

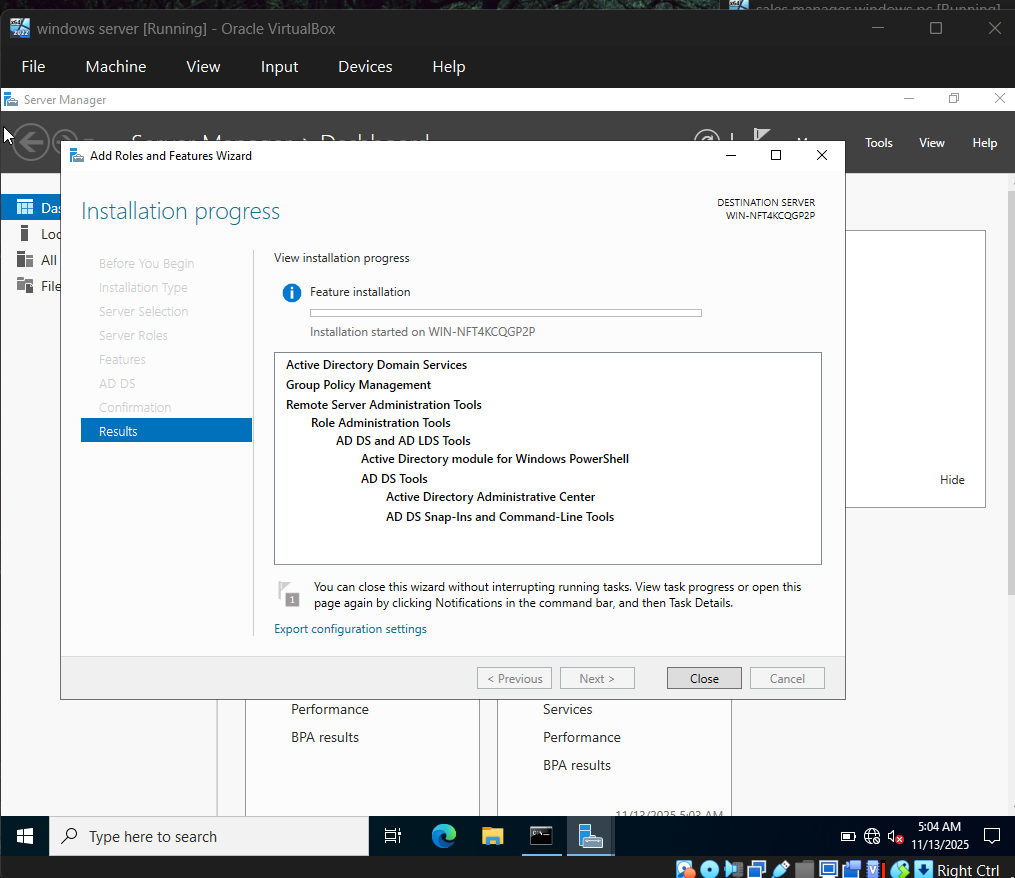
Click Manage>> add roles and features

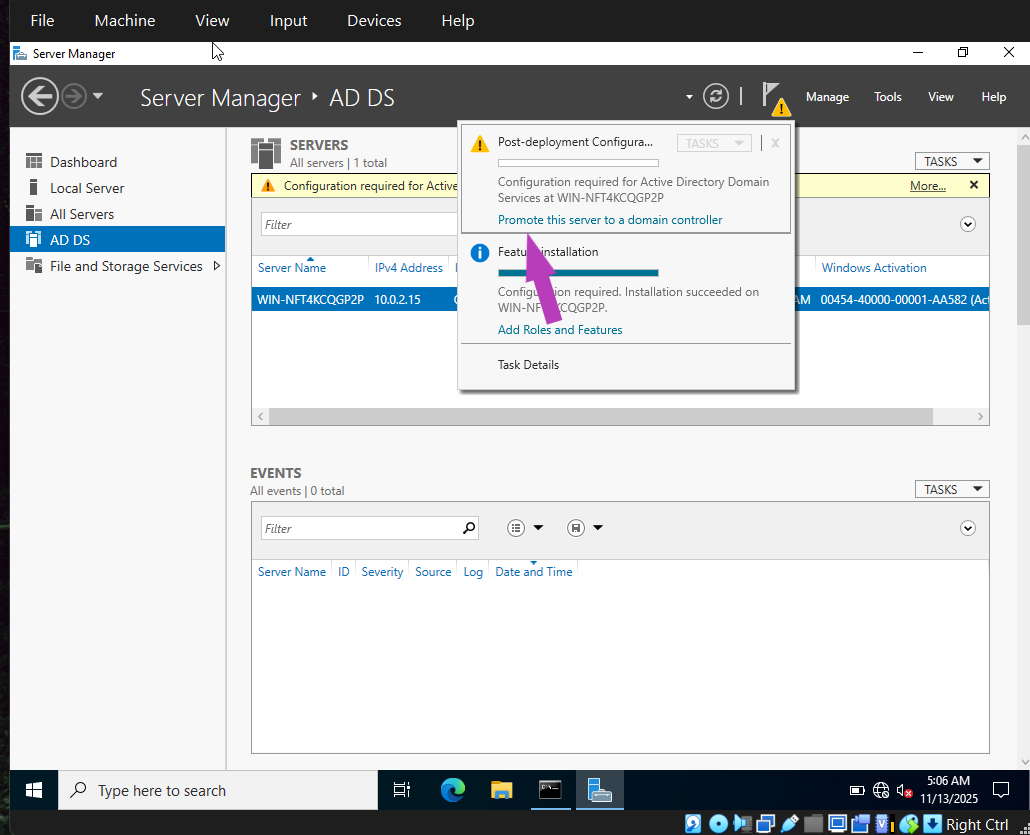
follow the prompts by clicking next

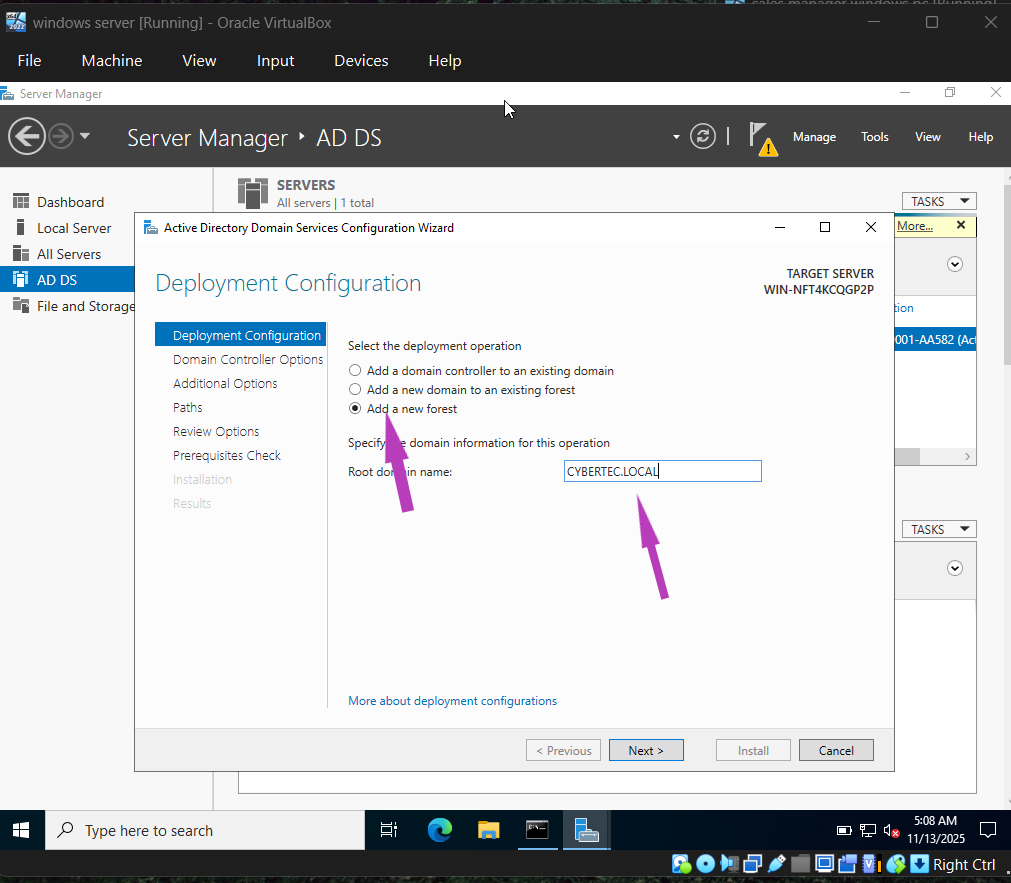


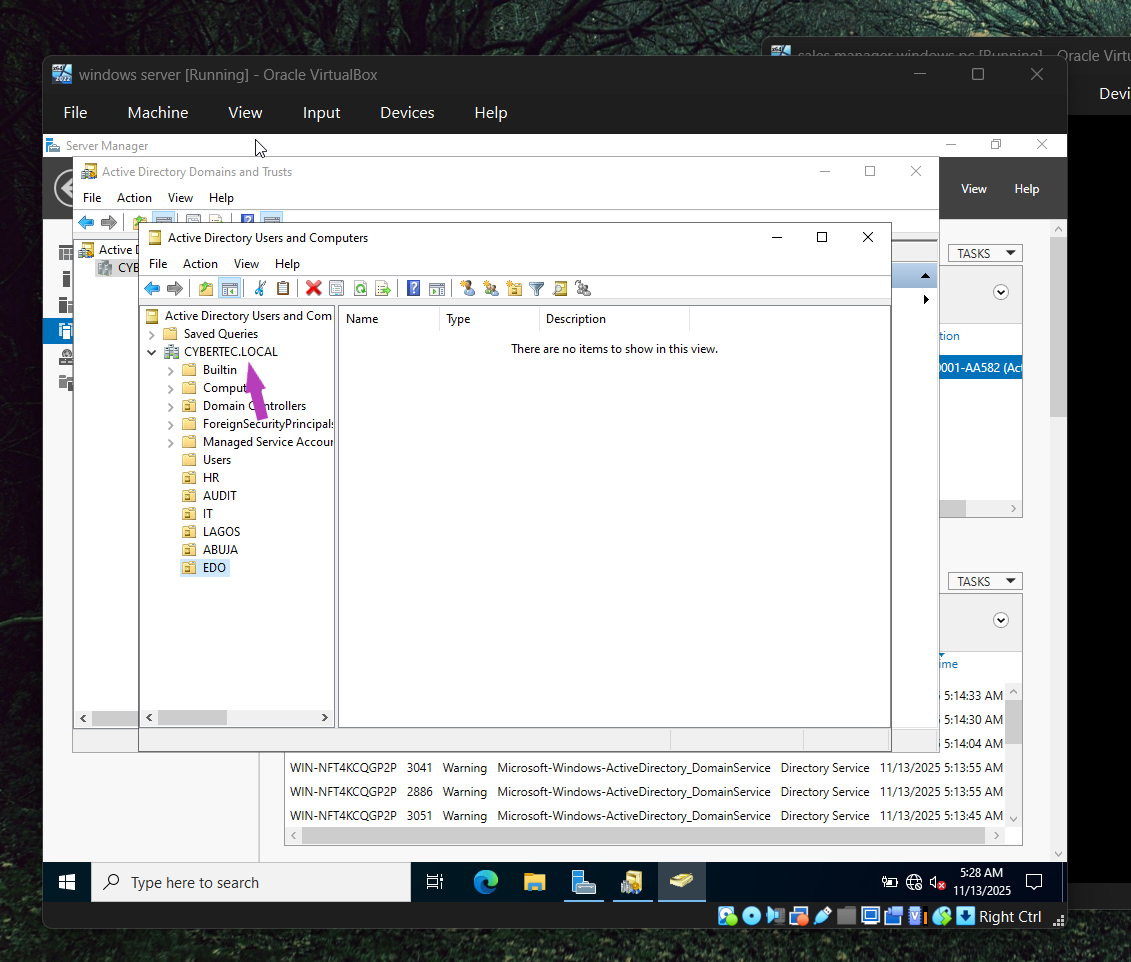
ickin

After clicking on active directory domain service, click on install

D



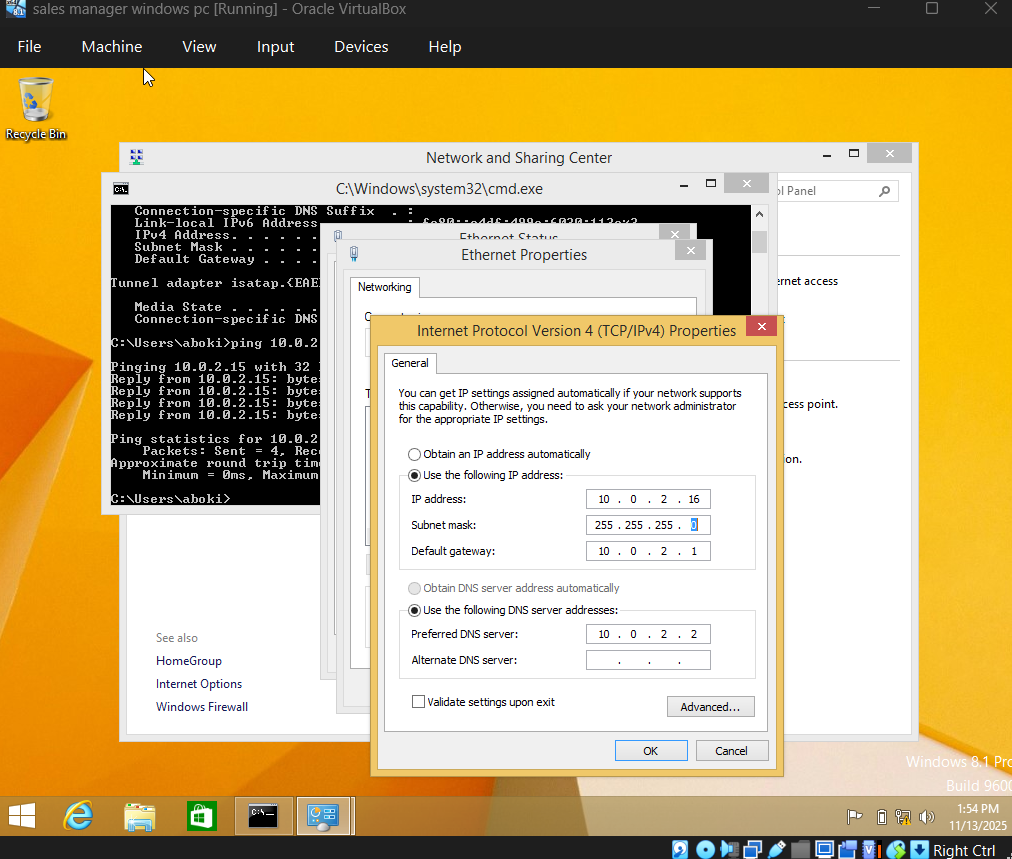
qq



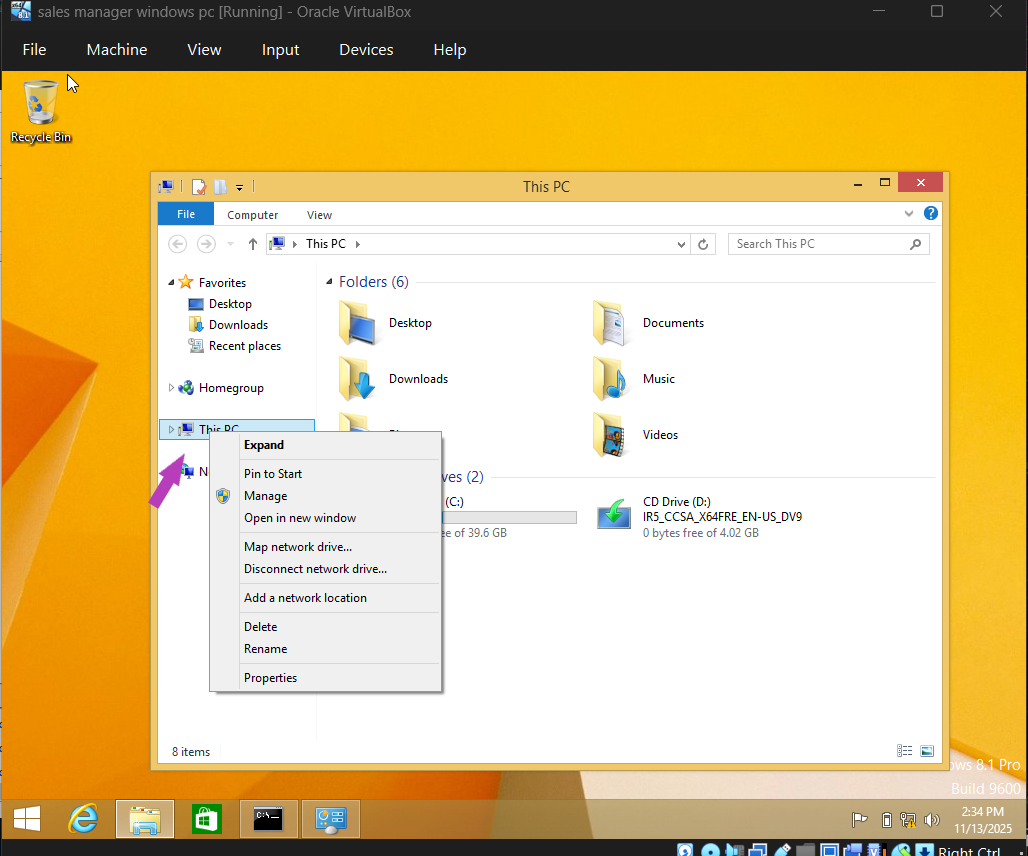
Here all you have to do is to create OUs on the domain you just created

As you can see I already created some, which are

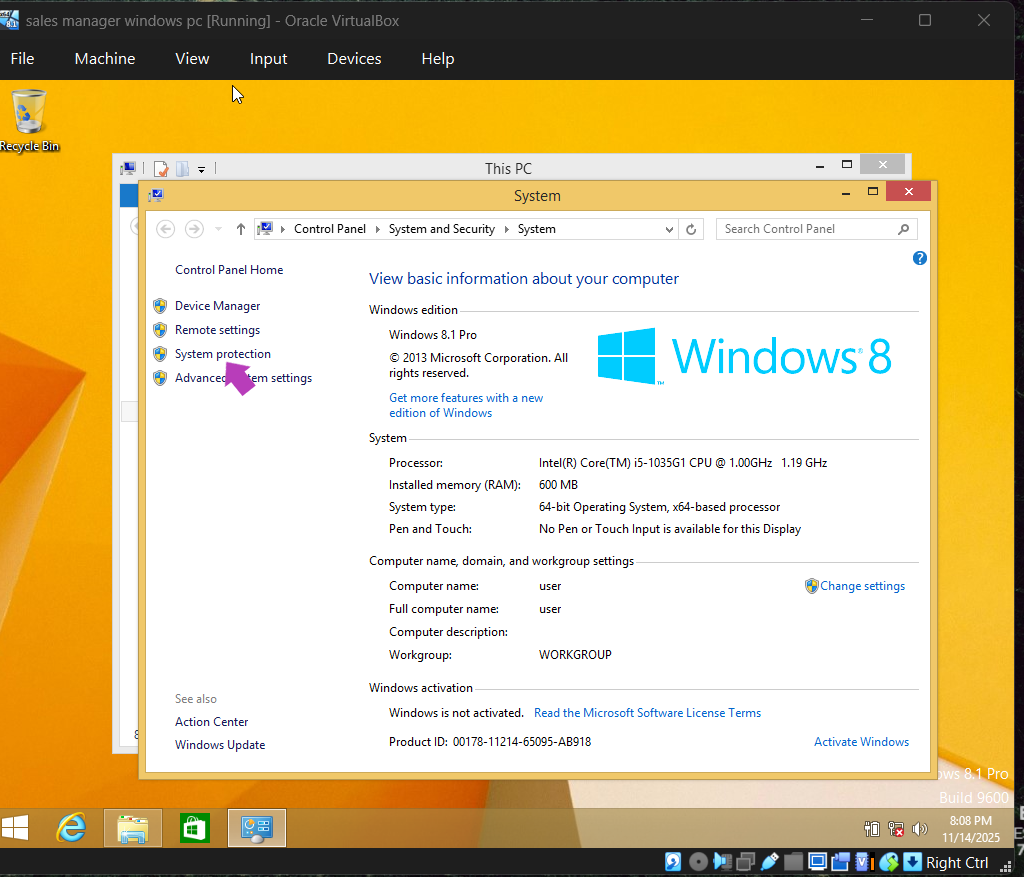
HR OU ,AUDIT OU ,IT OU ,LAGOS OU, ABUJA OU, EDO OU

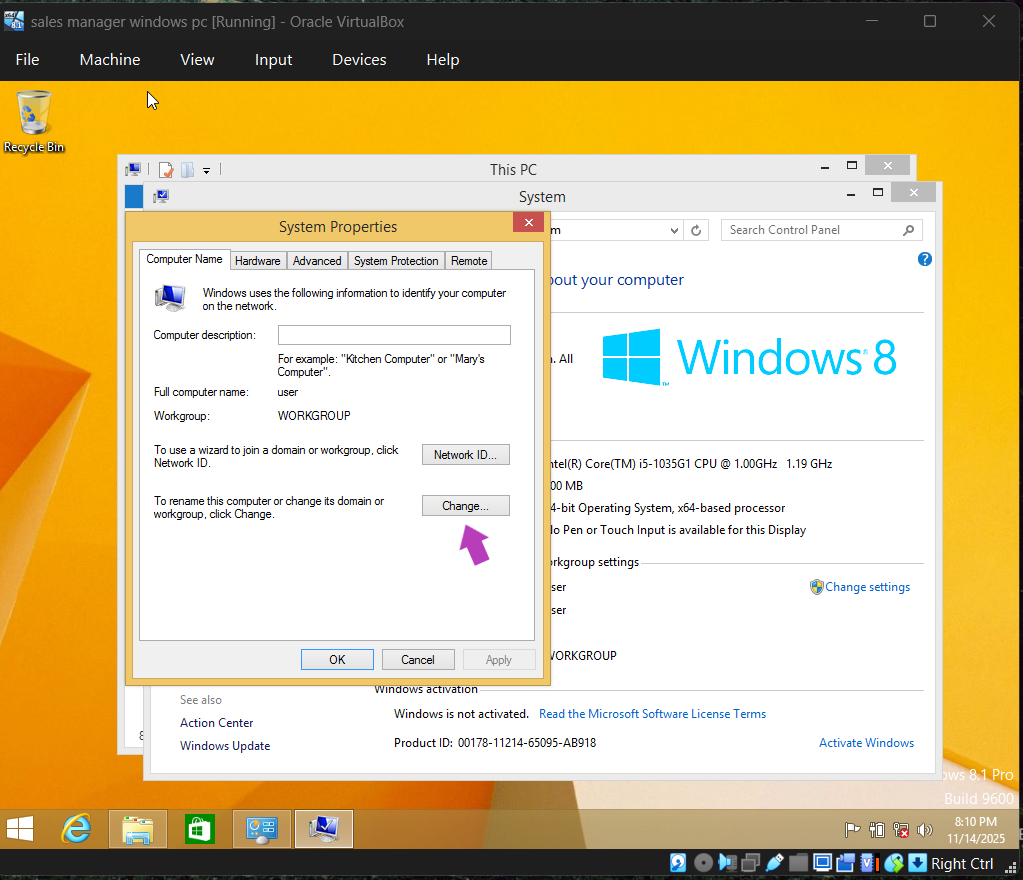


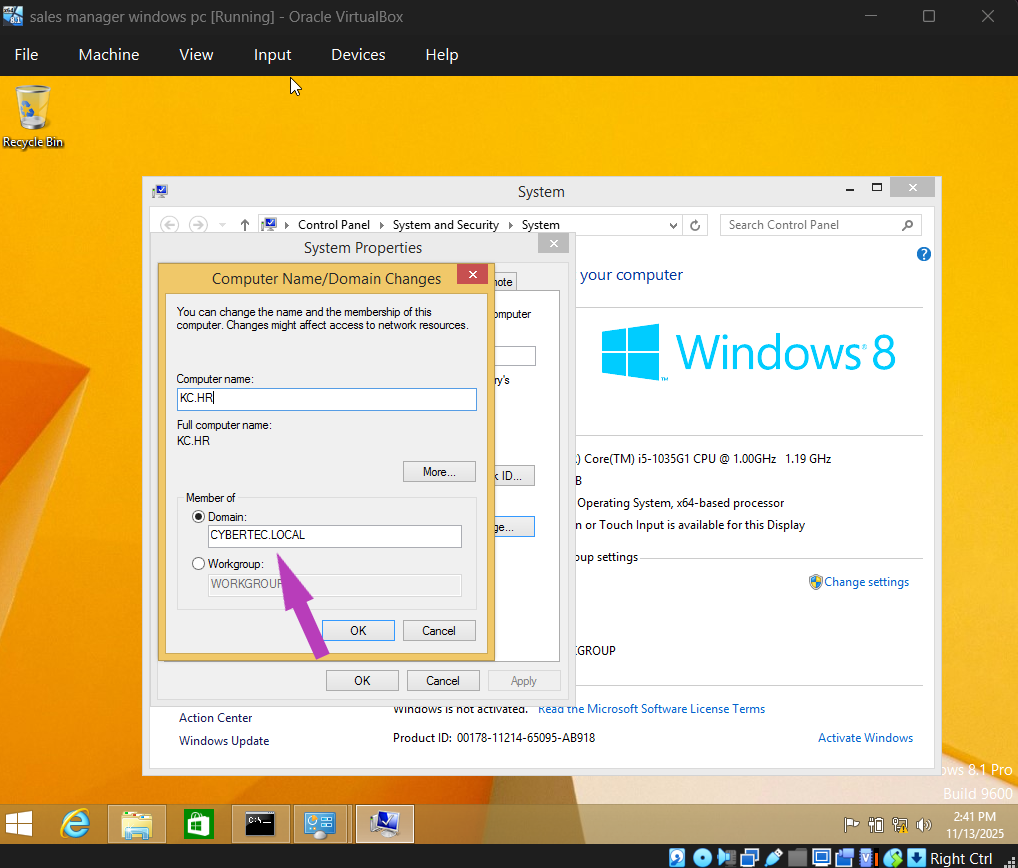
Configure your IPv4 on your windows pc and make sure to fill in the IPv4 address of your windows server on the preferred DNS server

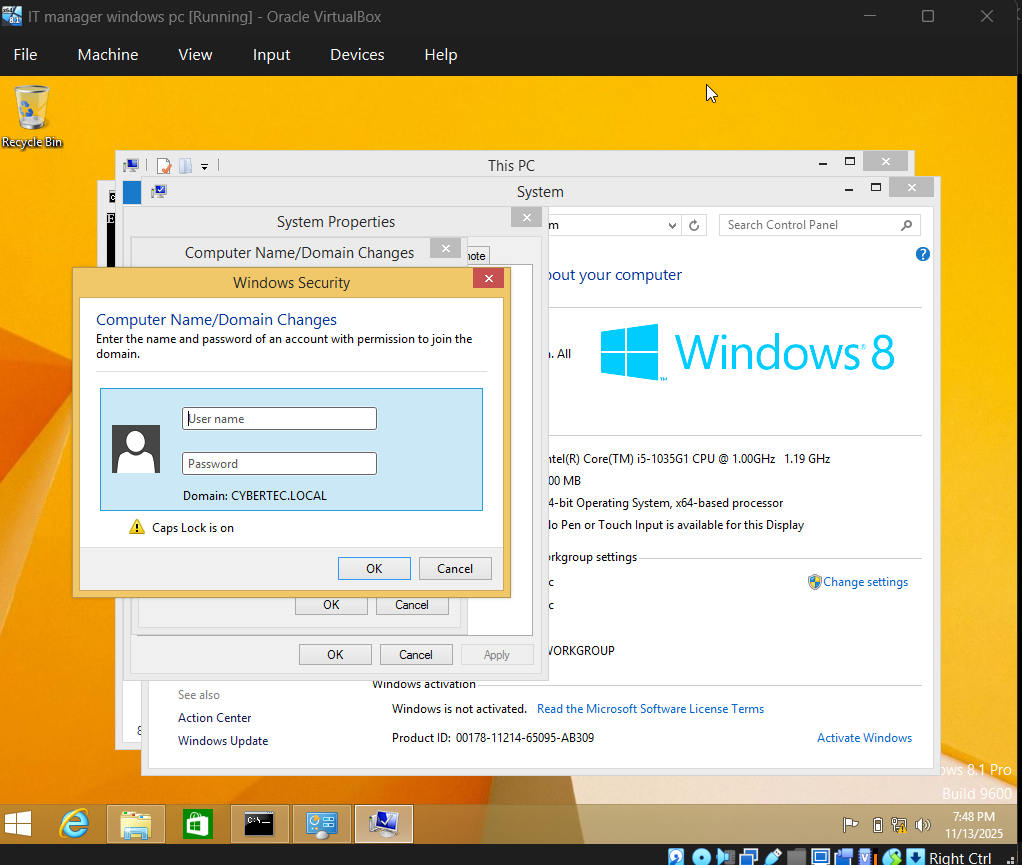


Cick on this pc on your windows pc and click on Properties

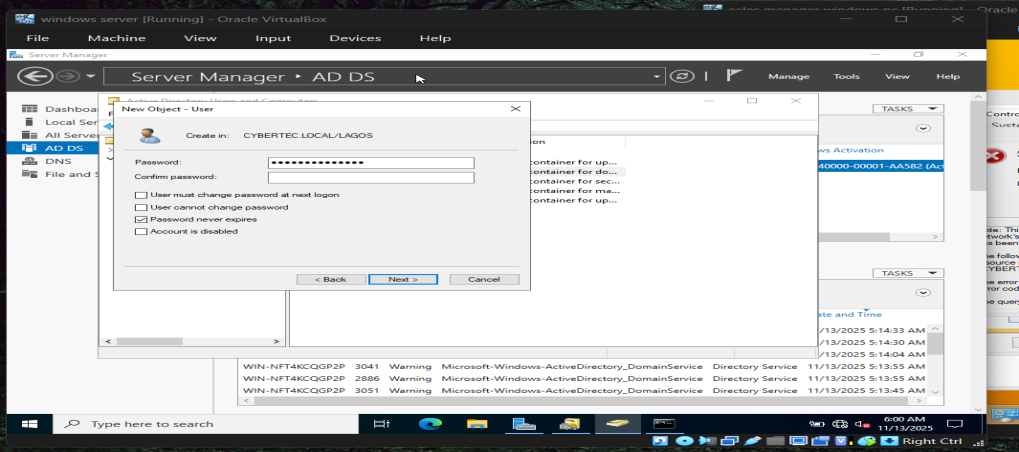


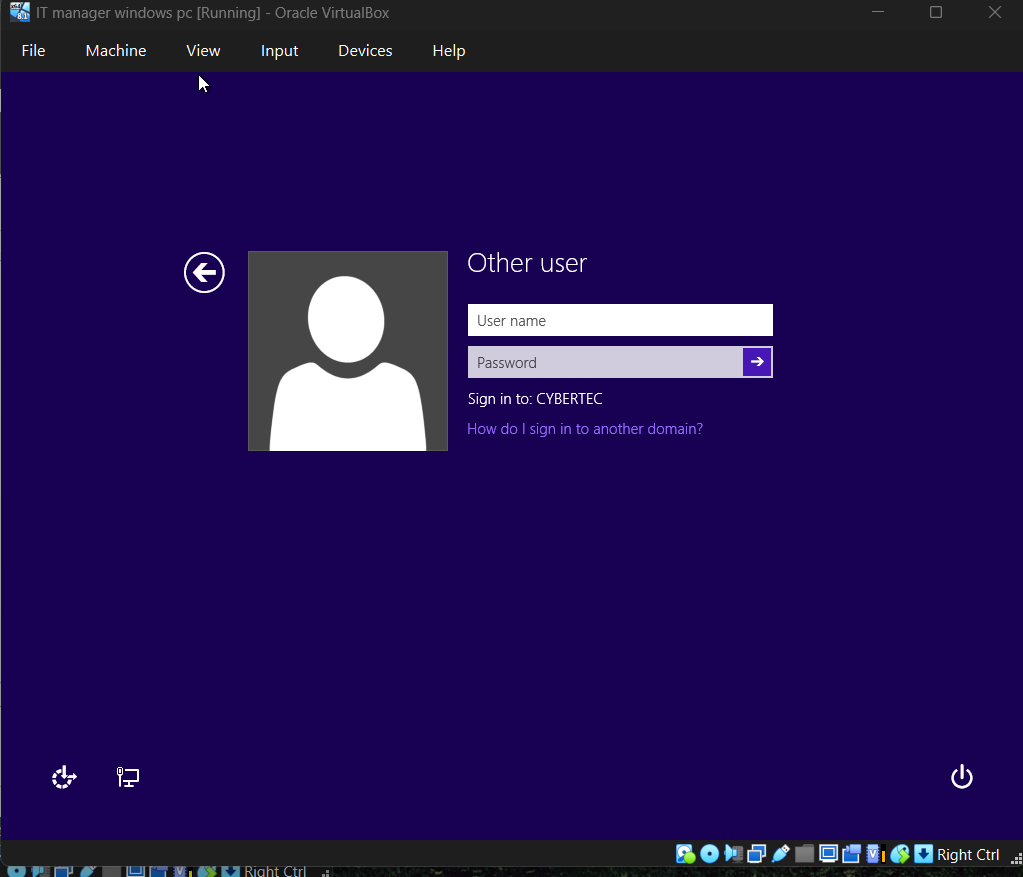




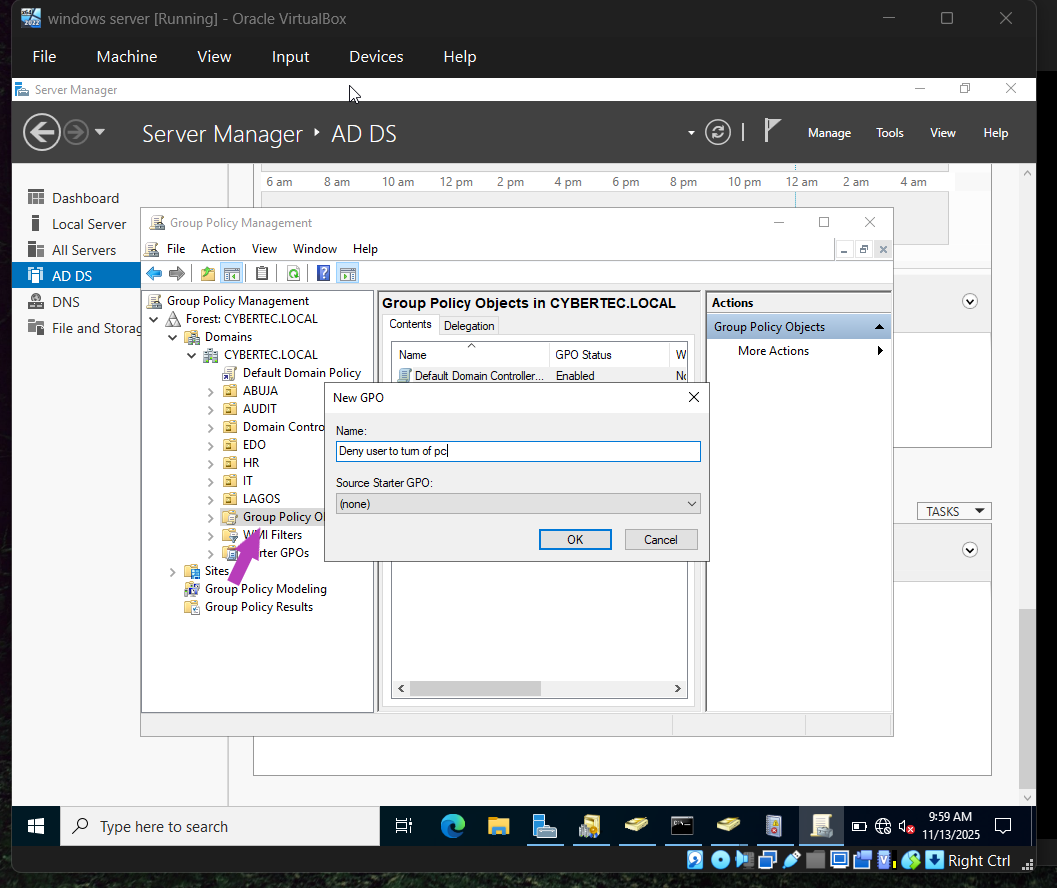


Here you will have to insert the user you created on the windows server

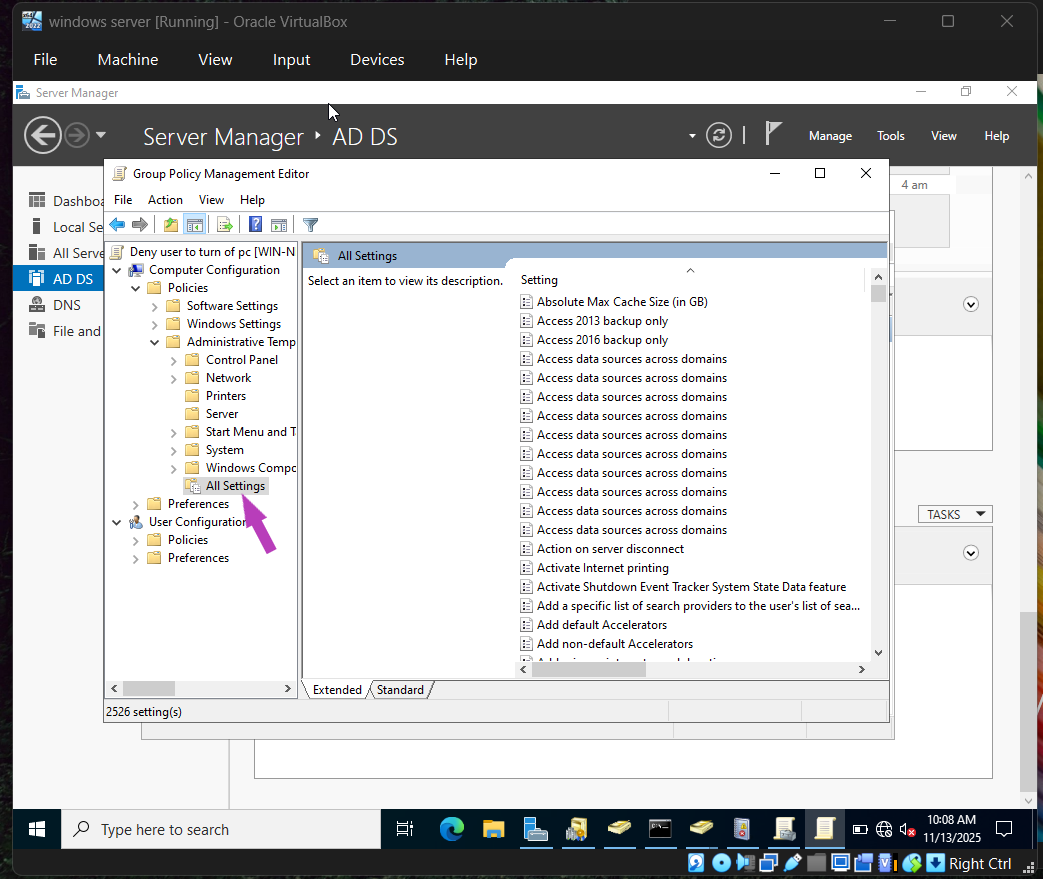




After doing that, your pc wil be resarted and you will need to login the new user

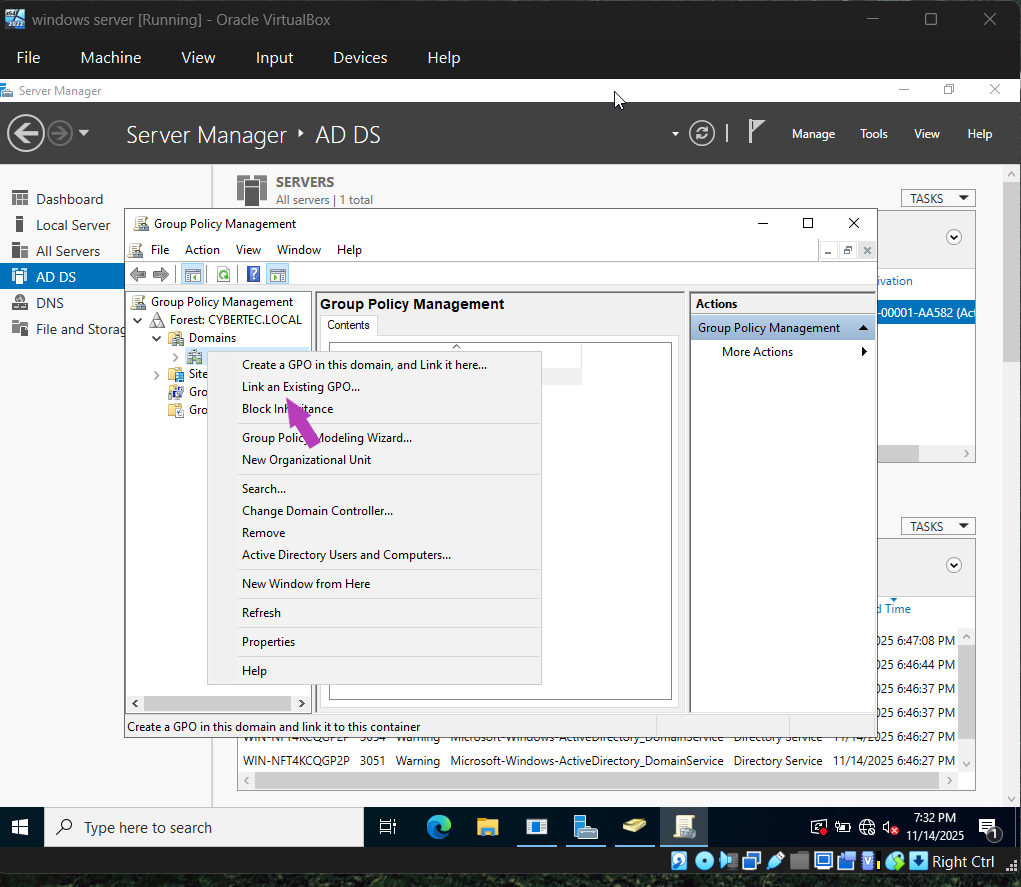


CICK ON TOOLS, Then select group policy management and then expand the forest you created, click on the option I pointed to create a new policy

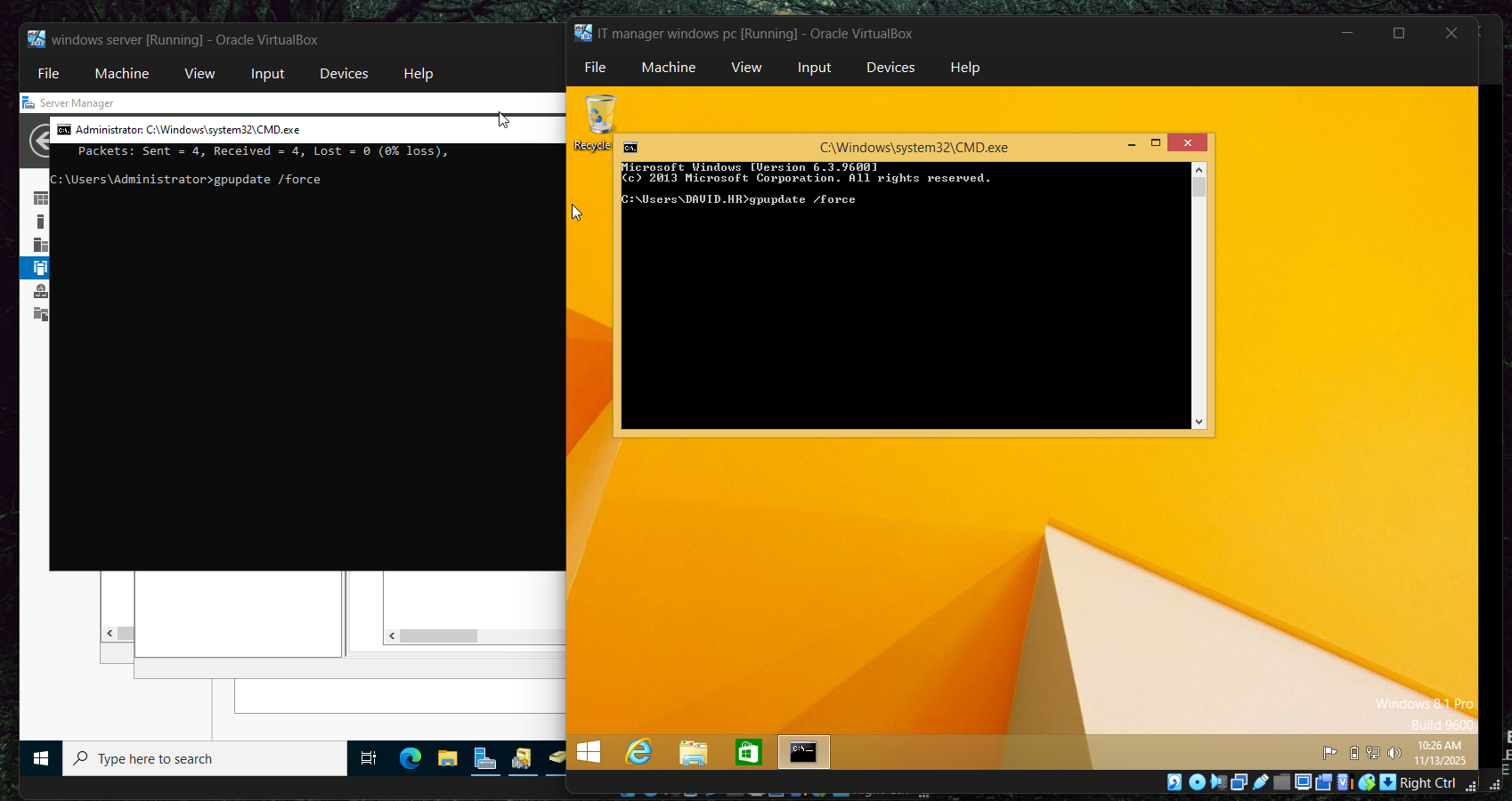




Make sure to create the policy on both the User and Computer configuration



Link the policy to your Domain



Force upate the GP setting or restart your pc and windows server





The first screenshot shows that the user was able to shutdown the windows pc before the policy was implemented the second screenshot shows that the user has been denied access to that by the policy