NETWORK OPERATING SYSTEM

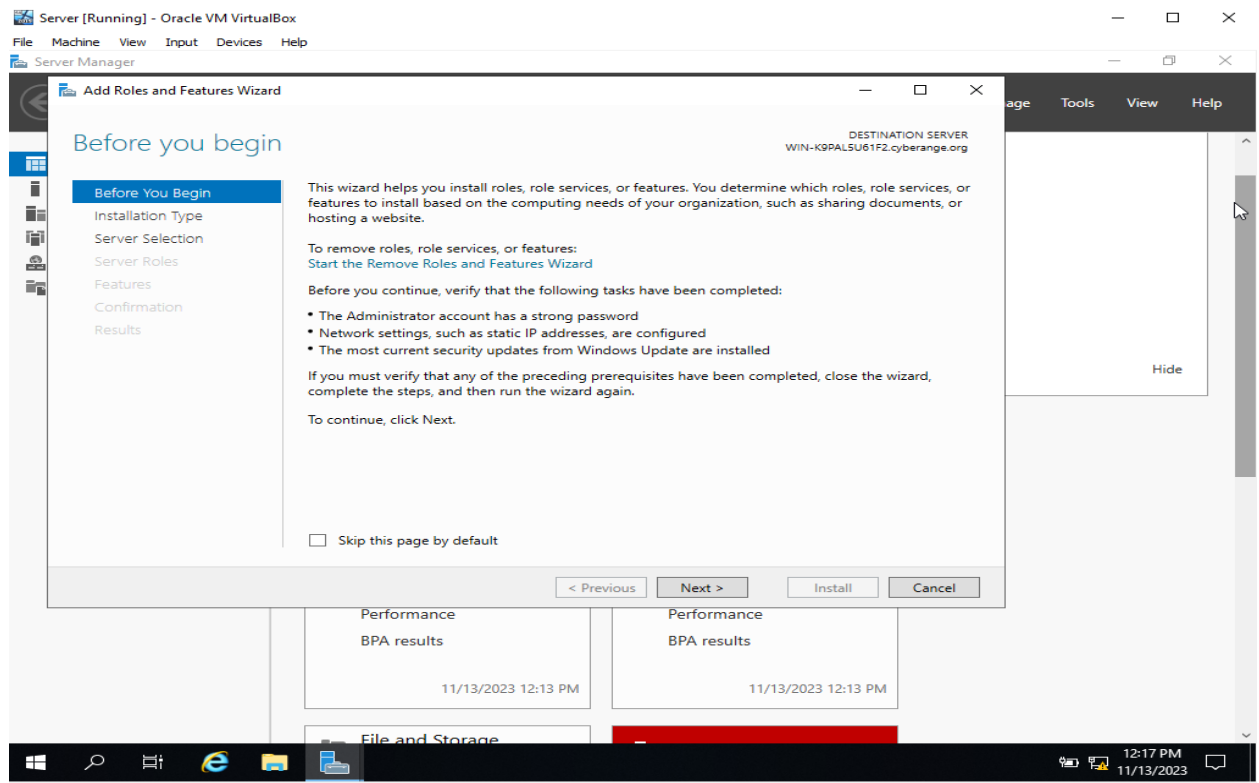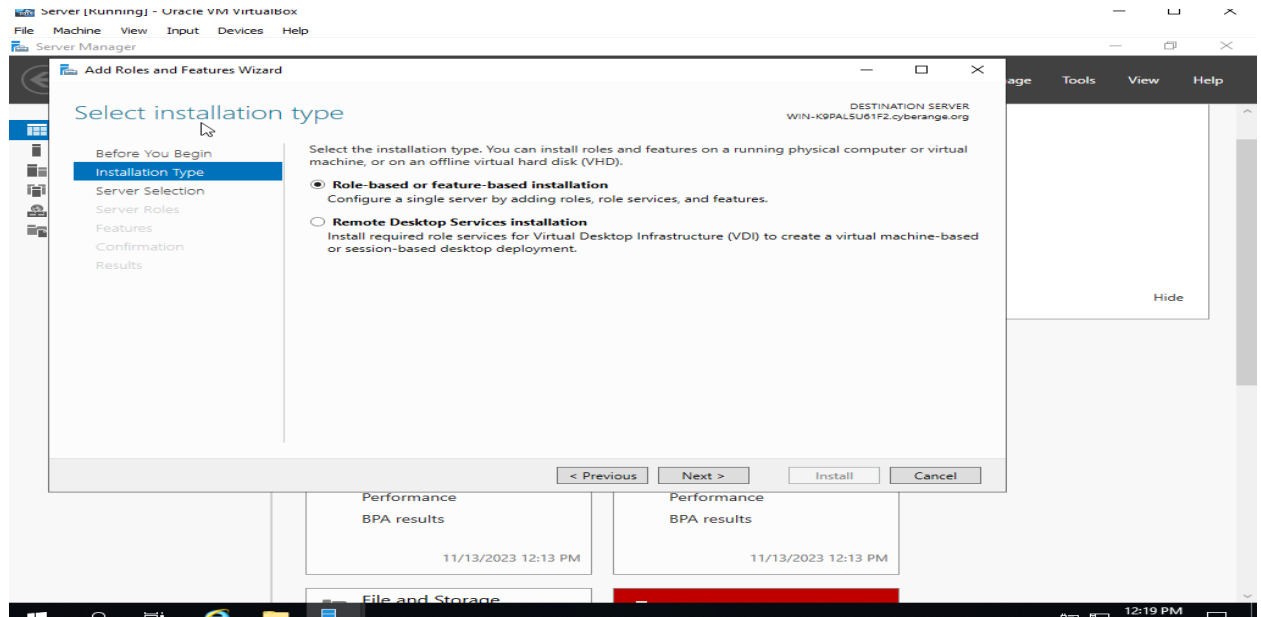## Active Directory configuration

By

DEWTON KIPROP

After the installation of windows server in the virtual box, start the machine, log in and navigate to tools at the top right corner.
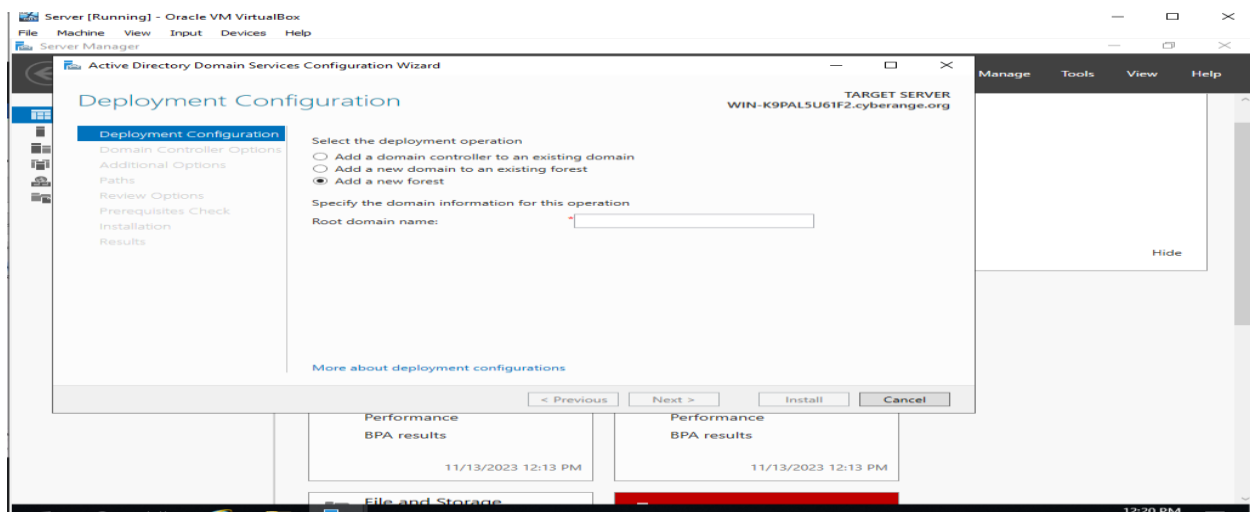
Look for add roles and features after creating the domain and you've managed to link windows 10 the domain created.
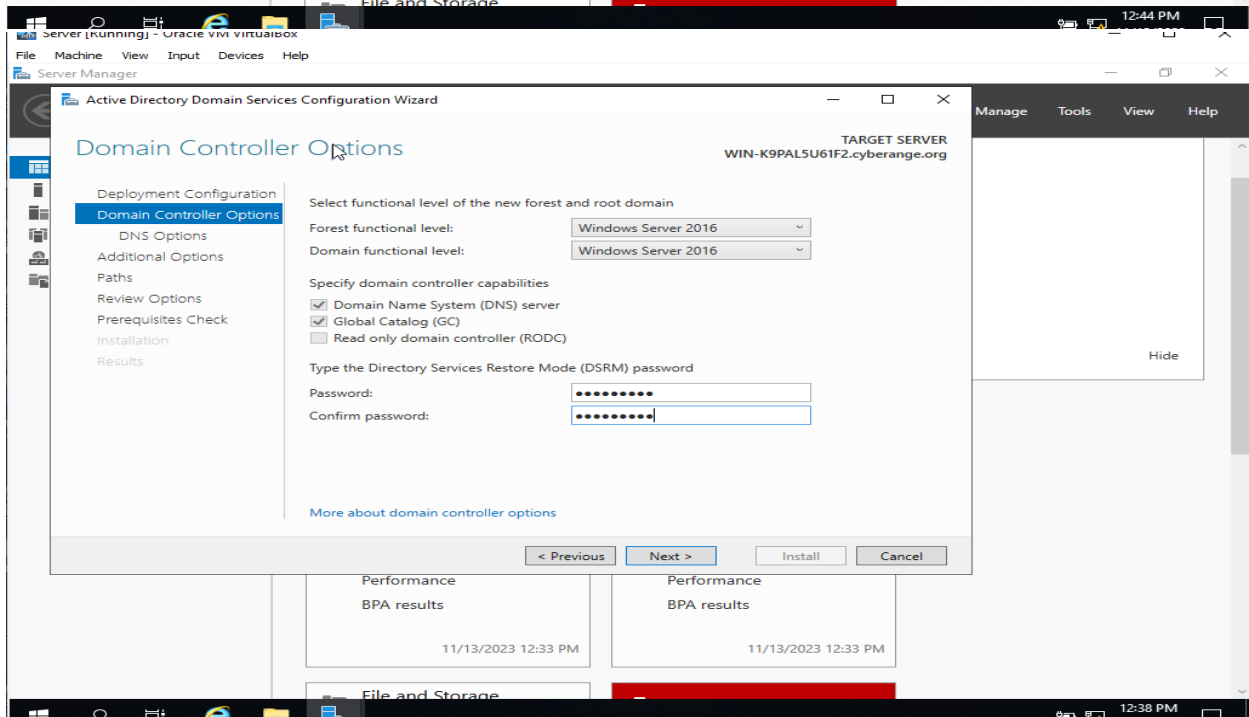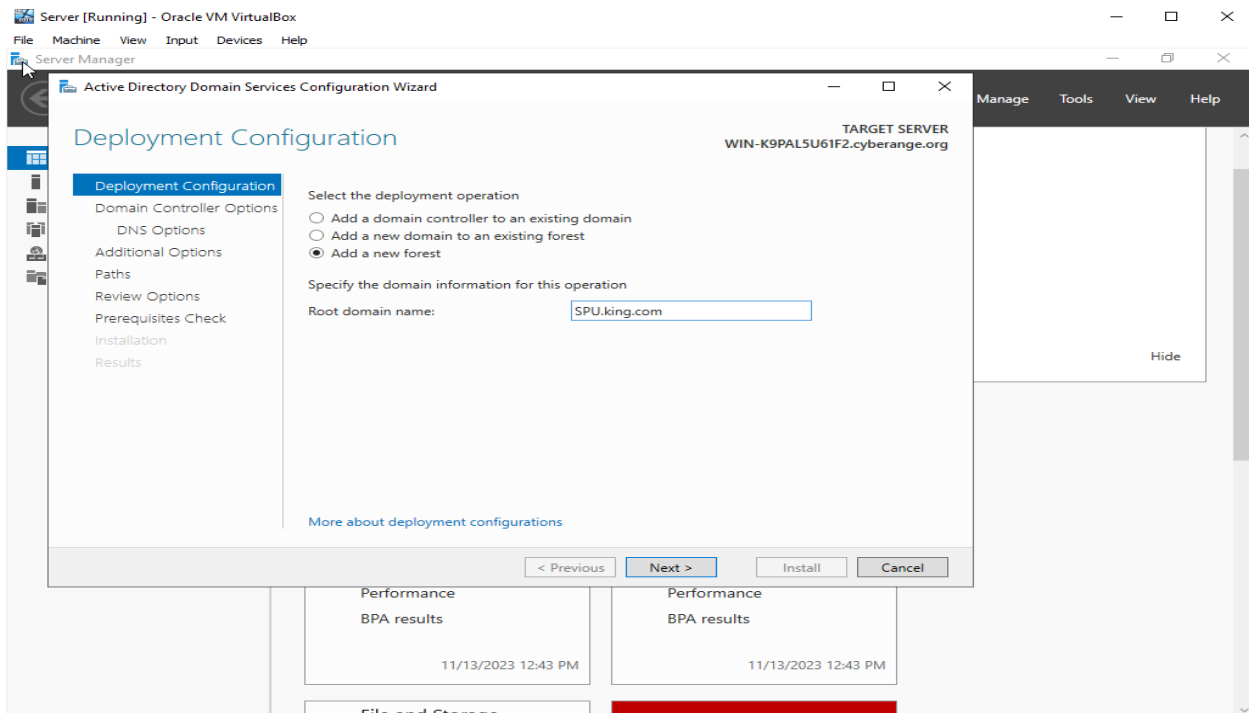
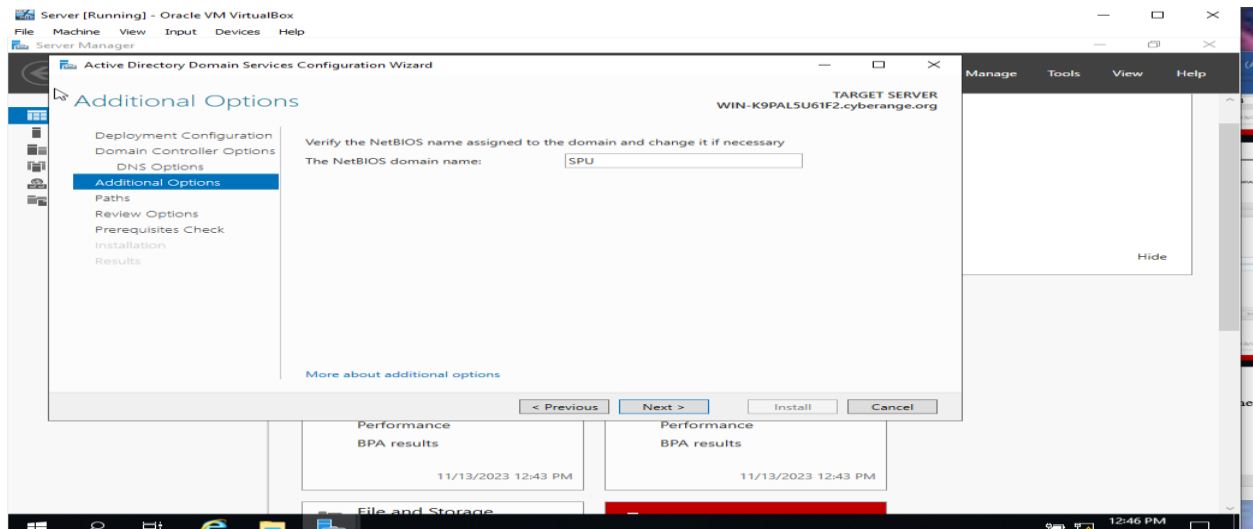➢ Navigate now to the active directory domain services Windows configuration.

➢ Configure server domain name to be "SPU"

Server [Running] - Oracle VM VirtualBox

File   Machine   View   Input   Devices   Help

Server Manager

Active Directory Domain Services Configuration Wizard

Deployment Configuration

TARGET SERVER
WIN-K9PAL5U61F2.cyberange.org

Deployment Configuration
Domain Controller Options
    DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results

Select the deployment operation
○ Add a domain controller to an existing domain
○ Add a new domain to an existing forest
● Add a new forest

Specify the domain information for this operation

Root domain name: SPU.king.com

More about deployment configurations

< Previous   Next >   Install   Cancel

Performance   Performance
BPA results   BPA results

        11/13/2023 12:43 PM   11/13/2023 12:43 PM

File and Storage

12:44 PM

Server [Running] - Oracle VM VirtualBox

File   Machine   View   Input   Devices   Help

Server Manager

Active Directory Domain Services Configuration Wizard

Domain Controller Options

TARGET SERVER
WIN-K9PAL5U61F2.cyberange.org

Deployment Configuration
Domain Controller Options
    DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2016
Domain functional level: Windows Server 2016

Specify domain controller capabilities
☑ Domain Name System (DNS) server
☑ Global Catalog (GC)
☐ Read only domain controller (RODC)

Type the Directory Services Restore Mode (DSRM) password

Password: ●●●●●●●●
Confirm password: ●●●●●●●●

More about domain controller options

< Previous   Next >   Install   Cancel

Performance   Performance
BPA results   BPA results

        11/13/2023 12:33 PM   11/13/2023 12:33 PM
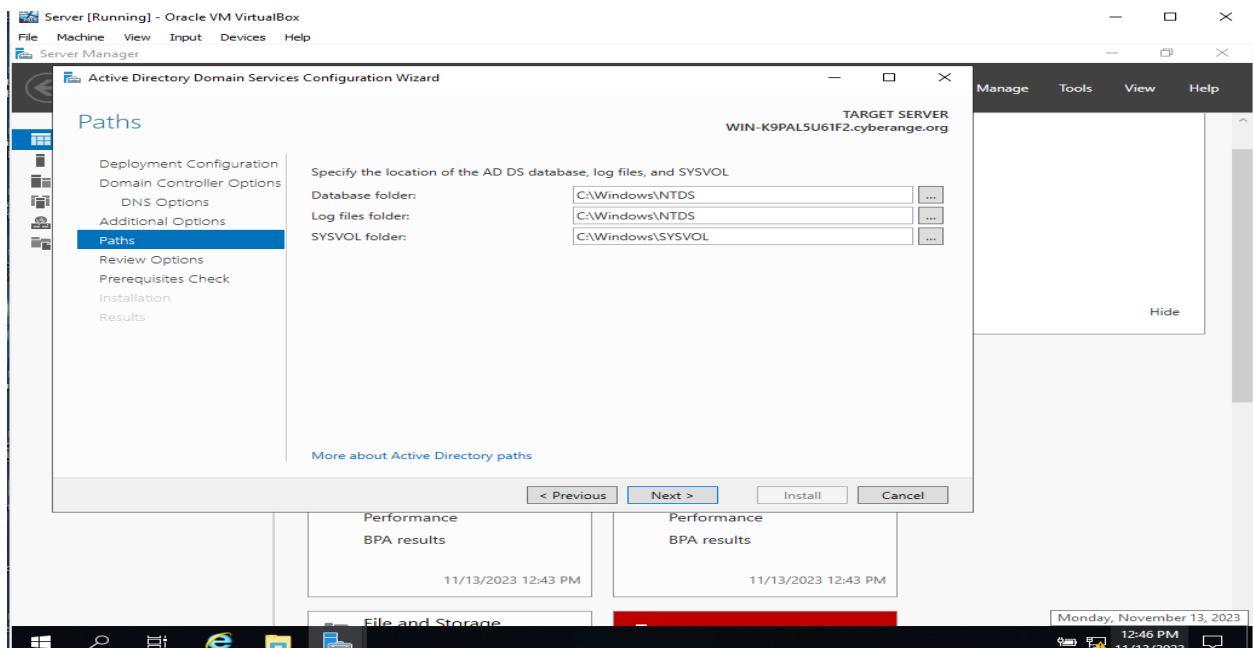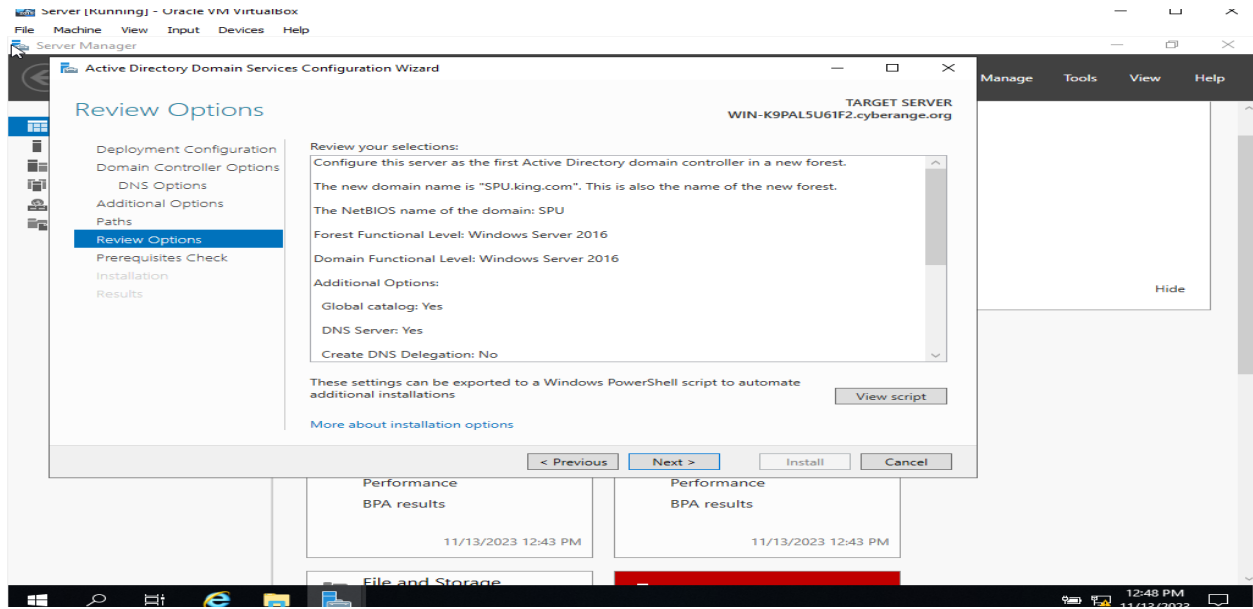
File and Storage

12:38 PM
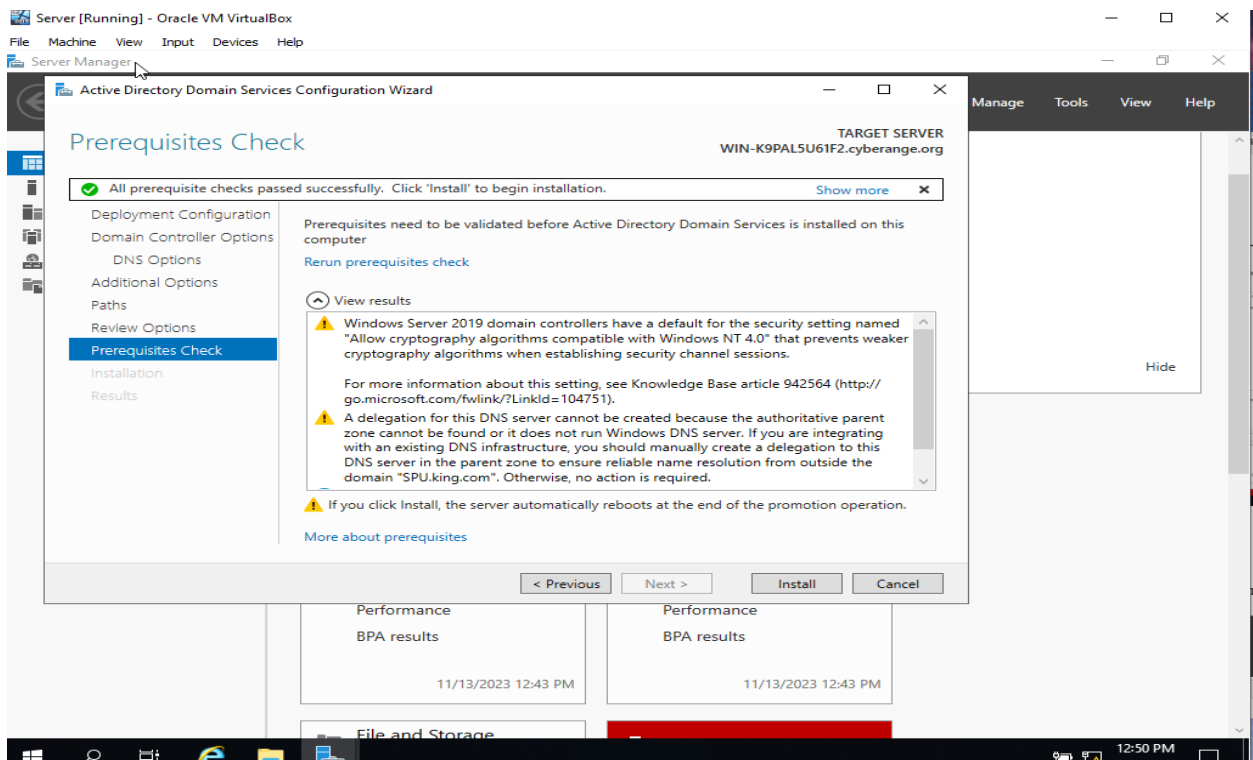
Path configuration

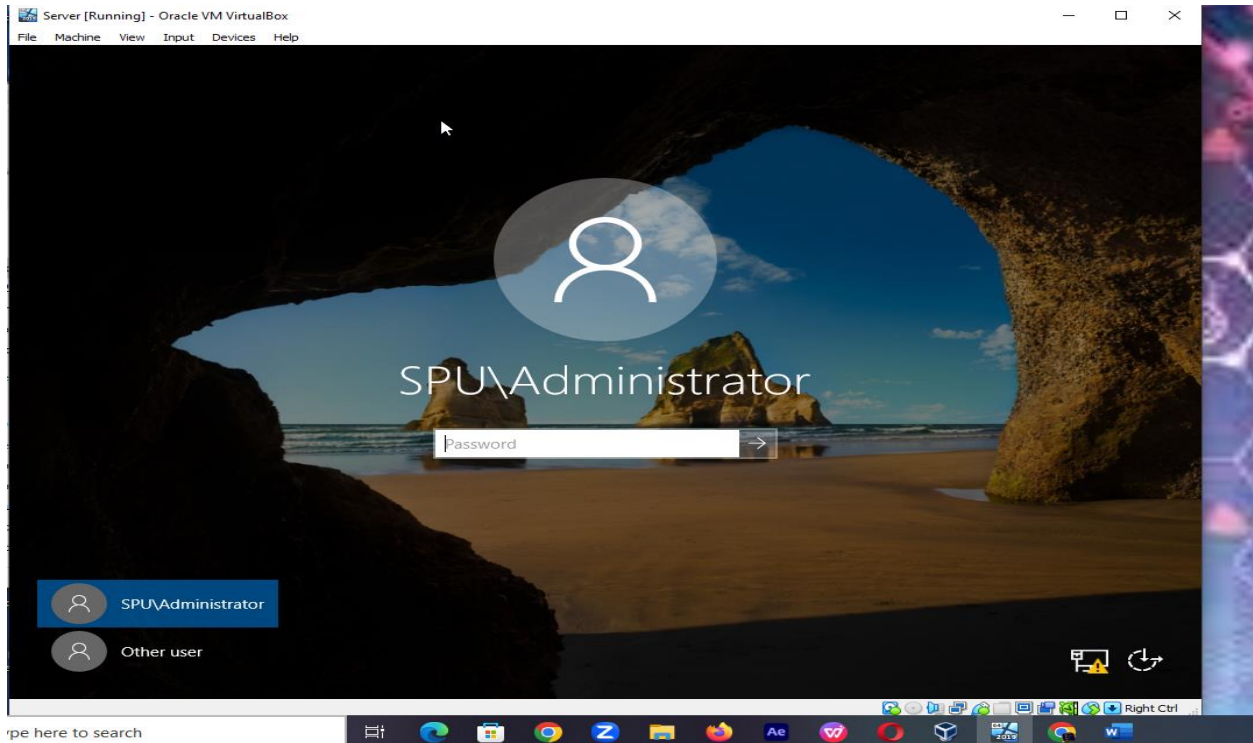**Here you configure the path but for our case we leave it as default.**

Review options

Prerequisites check

**Final domain change to spu**

To restrict the logon of users at specific times and days on a Windows Server, you can use Group Policy settings.

➢ Open Group Policy Management: Press Windows Key + R to open the Run dialog, type gpmc.msc, and press Enter. This will open the Group Policy Management Console.

➢ Create or Edit a Group Policy Object (GPO): Navigate to the domain or organizational unit (OU) where you want to apply the policy. Right-click on it and select "Create a GPO in this domain, and Link it here" or "Edit" if a GPO already exists.

➢ Navigate to Logon Hours Settings: In the Group Policy Management Editor, navigate to Computer Configuration -> Windows Settings -> Security Settings -> Account Policies -> Logon Hours.

➢ Set Logon Hours: Double-click on "Logon Hours" to open its properties.

➢ Here, you can define the allowed logon hours for users by specifying the hours during which users are allowed to log on to the server. You can set different logon hours for each day of the week.

➢ Configure Logon Restrictions: In addition to specifying logon hours, you can also configure other logon restrictions such as "Access Denied" and "Force Logoff When Logon Hours Expire".

➢ Apply the Group Policy Object:

➢ Once you have configured the logon hours settings, close the Group Policy Management Editor. The policy will be automatically applied to the users within the scope of the GPO.

➢ Test the Policy: Test the policy by attempting to log on to the server using user accounts affected by the logon hours restrictions. Ensure that the logon is allowed only during the specified hours and days.

➢ Restricting logon of users at specific times and days.
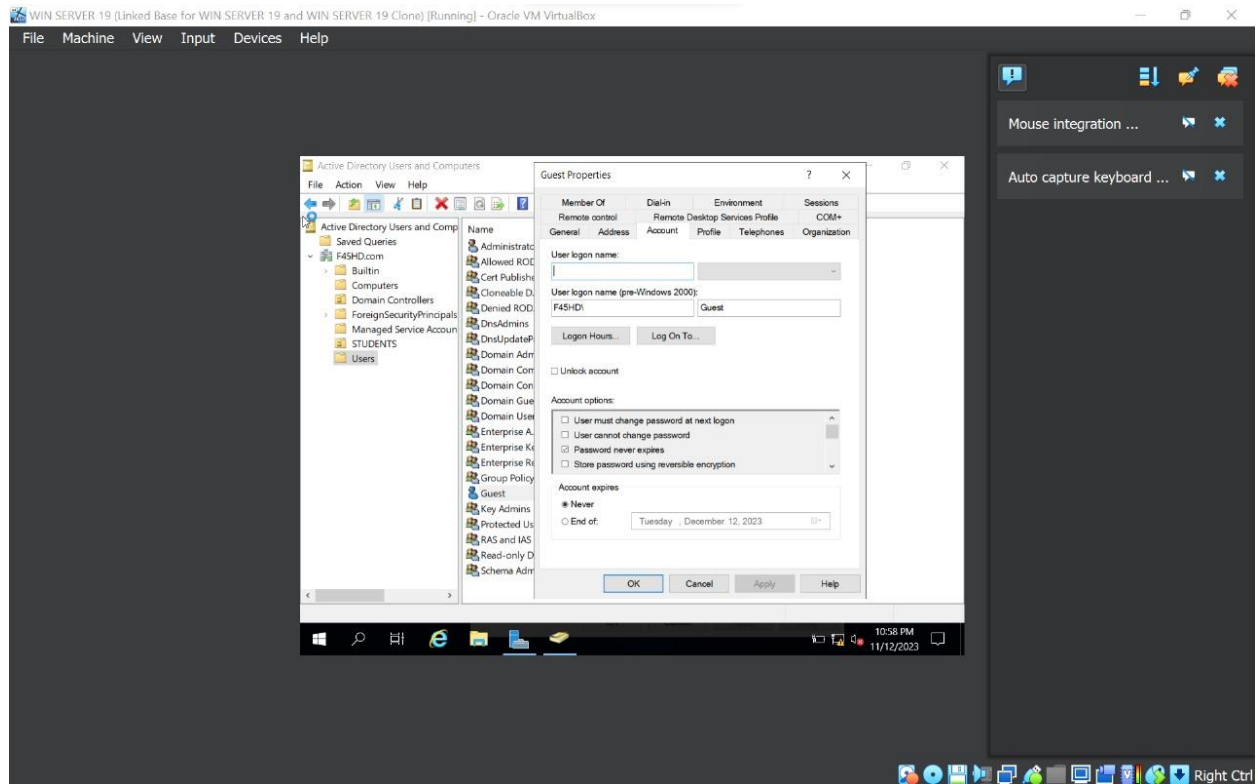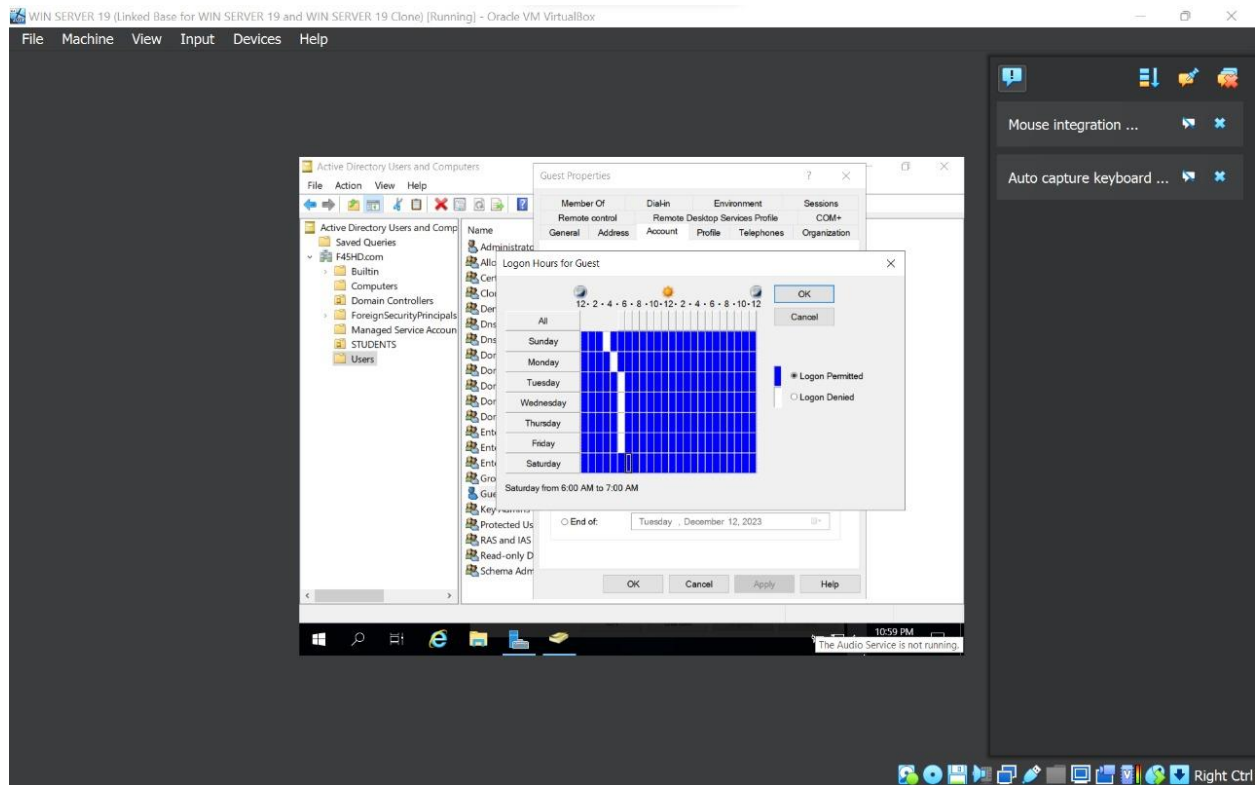
Create STUDENTS OU in Active Directory

➢ Open Active Directory Users and Computers: On your Windows Server, go to the Start menu, type "Active Directory Users and Computers" in the search bar, and press Enter to open the Active Directory Users and Computers (ADUC) console.

➢ Navigate to the Domain: In the ADUC console, expand the domain node to which you want to add the new OU. This could be your domain name, such as "example.com".

➢ Create the STUDENTS OU: Right-click on the domain node or any existing OU where you want to create the new OU (e.g., Users), then select "New" and choose "Organizational Unit".

➢ Enter "STUDENTS" as the name for the new OU and click "OK" to create it.

➢ Verify the Creation: Once created, you should see the "STUDENTS" OU listed under the domain node or the parent OU you selected.

➢ Optional: Set Permissions and Delegate Control: If needed, you can set permissions on the new OU or delegate control to specific users or groups to manage objects within it.

Right-click on the OU, select "Delegate Control", and follow the wizard to specify the
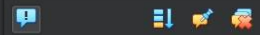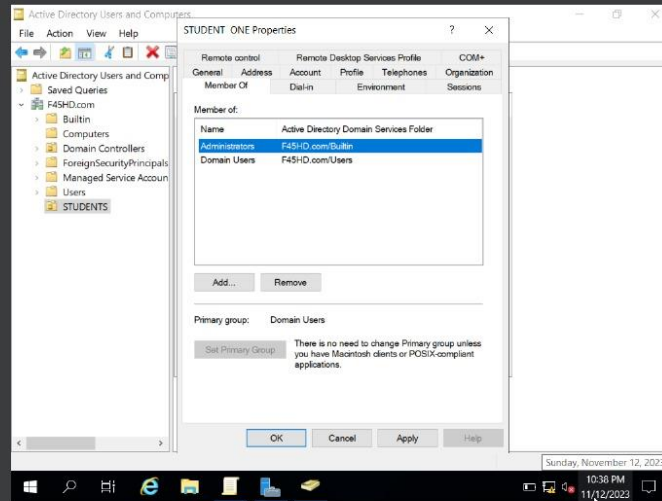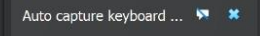permissions.
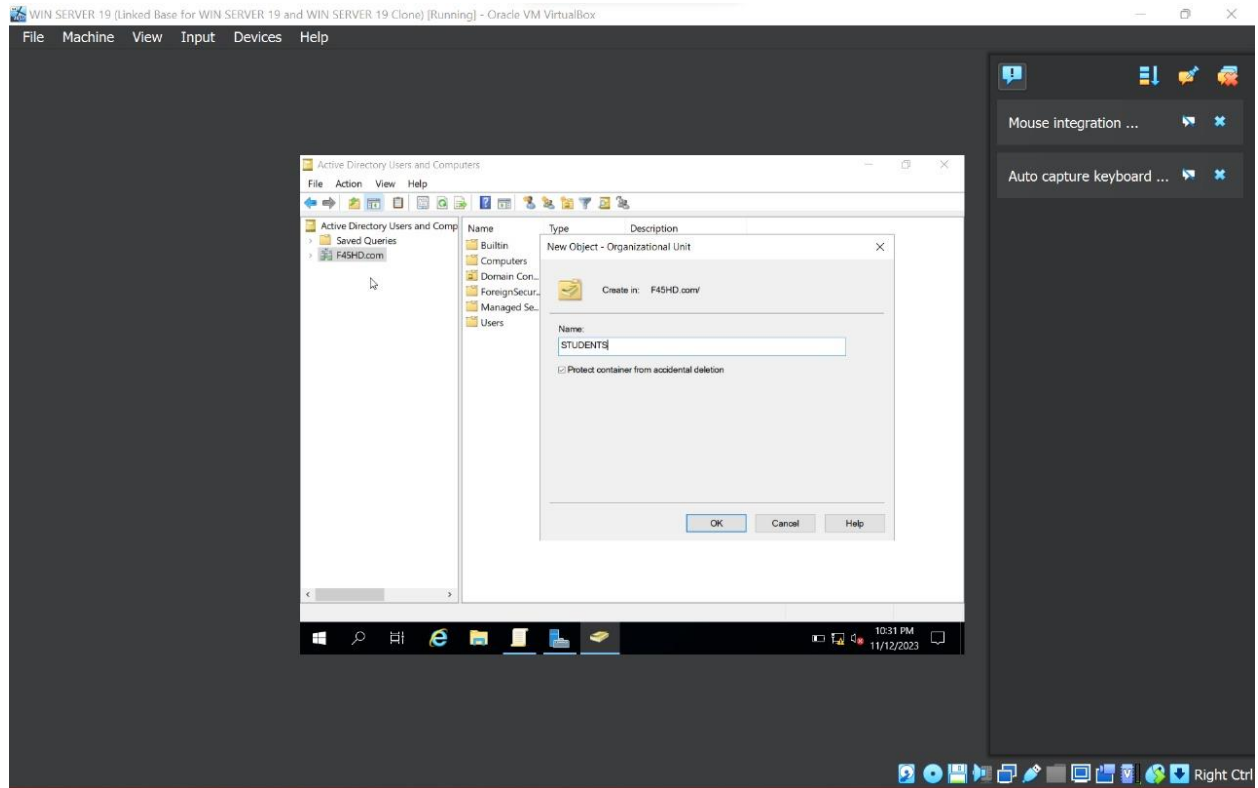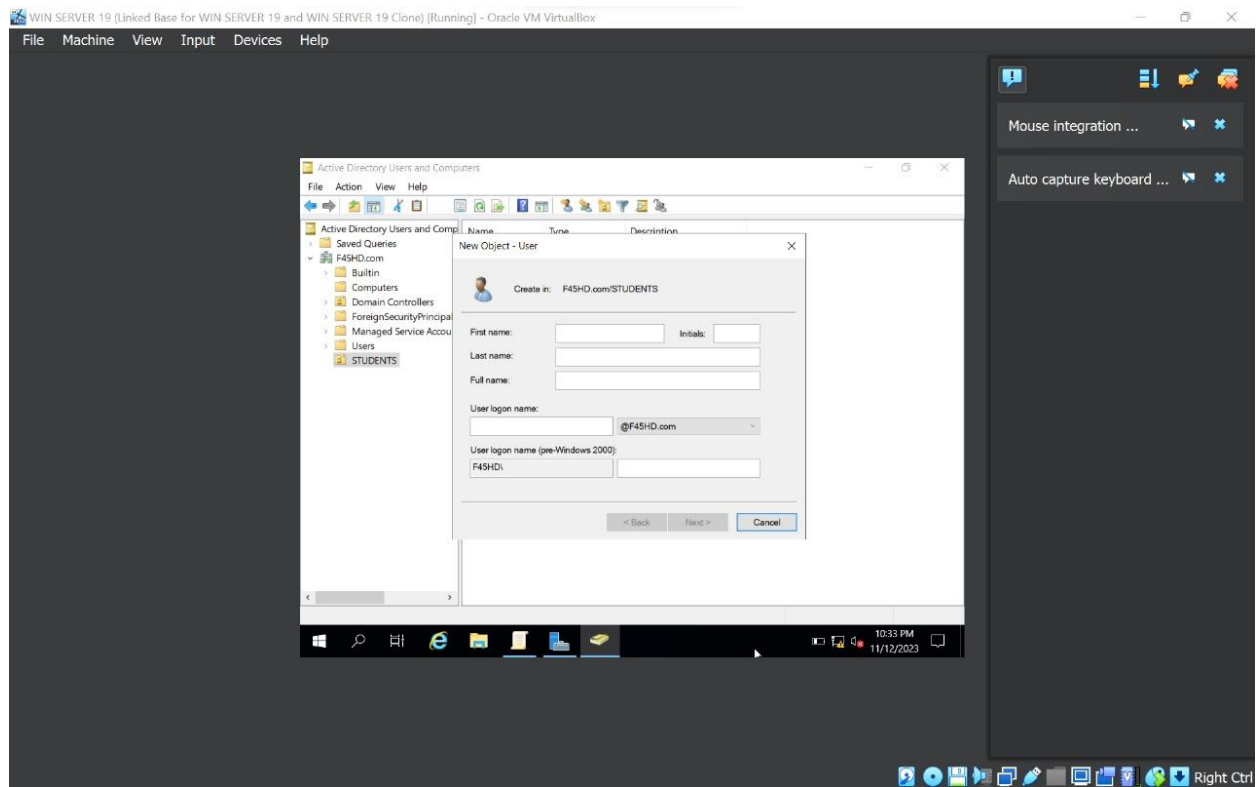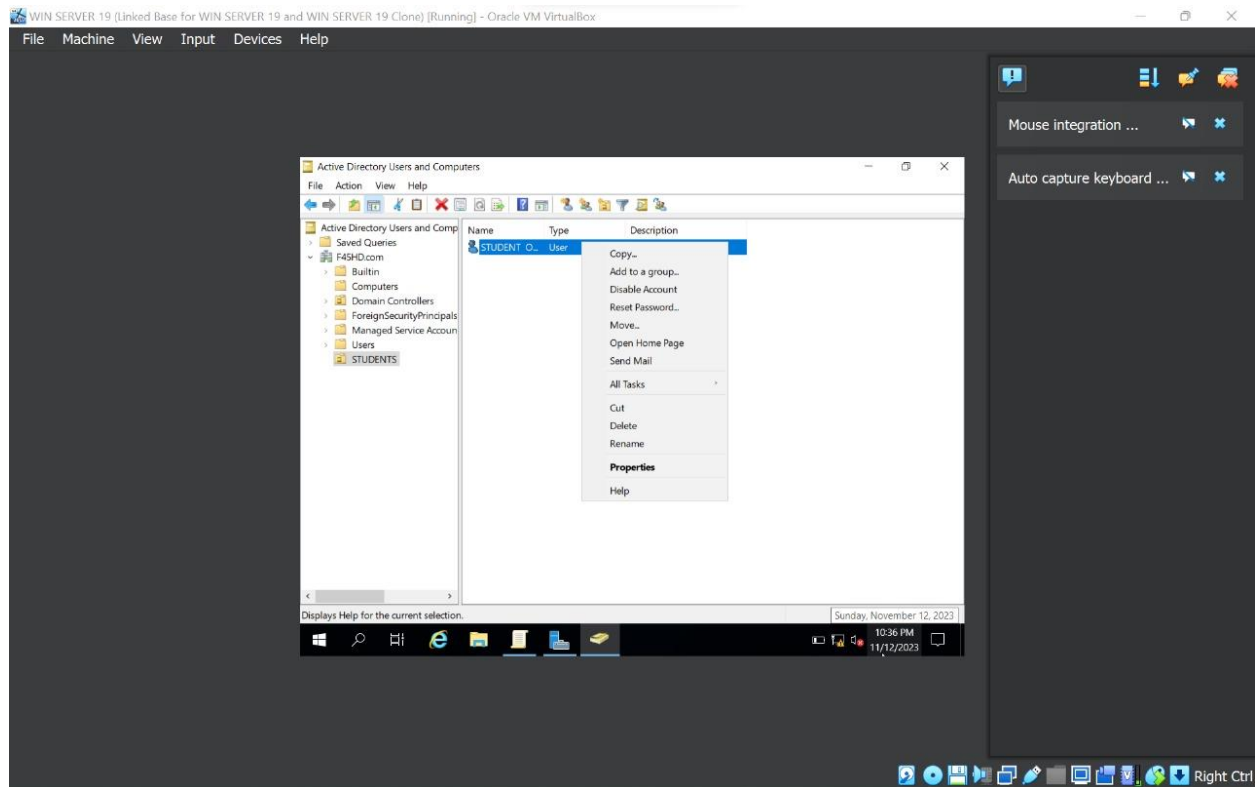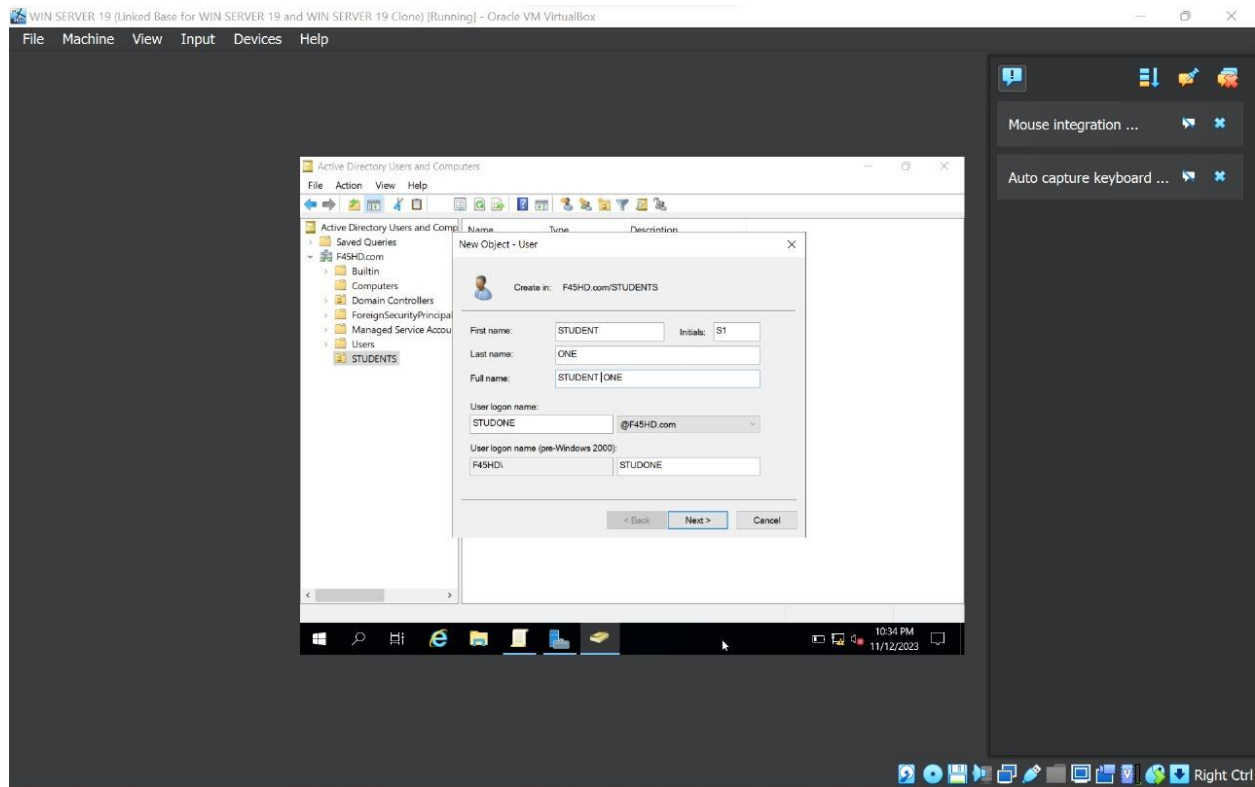
Create a user account in the student OU and add it to the Administrator group

➢ Create a New User Account: Right-click on the "STUDENTS" OU and select "New" > "User" to open the New Object - User wizard.

➢ Enter the necessary details for the new user account, such as First name, Last name, and User logon name (e.g., username@domain.com).

➢ Set a password for the user account and configure any additional settings as needed. Click "Next" and then "Finish" to create the user account.

➢ Add User to the Administrators Group: Once the user account is created, locate the user account within the "STUDENTS" OU.

❖ Right-click on the user account and select "Properties".

❖ In the Properties dialog box, go to the "Member Of" tab.

❖ Click on the "Add" button to add the user to a group.

❖ Type "Administrators" in the "Enter the object names to select" field and click "Check Names" to validate.

➢ Once validated, click "OK" to add the user to the Administrators group.

➢ Click "Apply" and then "OK" to save the changes.

➢ Verify Membership:

➢ To verify that the user has been added to the Administrators group, you can double-click on the group and check the list of members.