Windows Server

Jitendra Singh Tomar

INDEX

Server Operating System (OS)

A Server Operating System (Server OS) is a specialized operating system designed to run on servers and provide essential services and resources to client devices (like computers, printers, phones, etc.) over a network.

A Server OS is the backbone of an enterprise IT environment. It is built for reliability, performance, and secure multi-user operations, unlike client OSes which are optimized for individual user experience.

Key Characteristics of a Server OS:

- Multi-user support
  - Can handle simultaneous connections from multiple clients.
- Resource sharing
  - Provides shared access to files, printers, databases, and applications.
- Network services
  - Hosts services like DNS, DHCP, web, email, and Active Directory.
- Security
  - Offers advanced security mechanisms, access control, auditing, and role-based permissions.
- Scalability
  - Optimized to handle high performance and large workloads (RAM, CPU, I/O).
- Remote management
  - Can be managed remotely via tools like PowerShell, RDP, or management consoles.

Common Examples of Server OS:

- Windows Server (2022, 2019, 2016...)
- Ubuntu Server
- Red Hat Enterprise Linux (RHEL)
- CentOS Stream / Rocky Linux
- SUSE Linux Enterprise Server (SLES)
- macOS Server (deprecated)

Typical Roles a Server OS Can Perform:

- Active Directory Domain Controller
- File Server
- Web Server (IIS, Apache, NGINX)
- Email Server (Exchange, Postfix)
- Database Server (SQL Server, MySQL, PostgreSQL)
- Virtualization Host (Hyper-V, KVM, VMware)

Client Operating System (OS)

- A Client Operating System (Client OS) is an operating system designed for end-user devices, like desktops, laptops, tablets, or mobile phones.
- It allows users to interact with hardware and software, perform day-to-day tasks, and connect to servers in a networked environment.
- A Client OS is meant for the end-user.
- It provides a user-friendly interface and supports applications and functions that help users complete personal or work-related tasks.
- It can connect to a server OS, but does not provide network-wide services.

Key Characteristics of a Client OS

- User-focused
  - Designed for ease of use, graphical interfaces, and daily personal or business tasks.
- Single-user environment
  - Primarily supports one active user session at a time.
- Application-centric
  - Runs common applications like browsers, word processors, games, email clients, etc.
- Multimedia support
  - Strong support for audio, video, graphics, and touchscreen input.
- Limited network services
  - Can access network resources but doesn't typically provide them (e.g., not a DNS or DHCP provider).
- Lightweight security
  - Basic security features like antivirus, firewalls, user authentication.
- Automatic updates
  - Frequently updated for new features, security patches, and bug fixes.

Examples of Client Operating Systems:

- Microsoft Windows 11, 10, 8.1
- macOS (Ventura, Monterey, etc.)
- Linux Desktop OS (Ubuntu Desktop, Fedora Workstation)
- Chrome OS
- Mobile: Android, iOS

Common Uses of a Client OS:

- Browsing the internet
- Writing documents and emails
- Watching videos or listening to music
- Playing games
- Using business productivity software
- Connecting to enterprise networks (e.g., logging into a domain)

Server Operating System (Server OS) VS a Client Operating System (Client OS)

Feature	Server OS	Client OS
Purpose	Designed to manage network resources, services, and multiple users.	Designed for end-users to perform daily tasks like browsing, word processing, media, etc.
Examples	Windows Server 2022, Windows Server 2019, Ubuntu Server, Red Hat Enterprise Linux	Windows 11, Windows 10, macOS, Ubuntu Desktop
User Access	Supports multiple simultaneous users and remote access sessions.	Generally used by one user at a time (local login).
Resource Management	Handles heavy workloads (e.g., file sharing, web hosting, virtualization, database).	Optimized for performance and responsiveness for individual users.
Security Features	Includes advanced features like Active Directory, Group Policy, DHCP, DNS, RADIUS, file auditing.	Includes basic security features like Defender, BitLocker, firewall, and Windows Hello.
Hardware Support	Supports high-end hardware like multi-core CPUs, large RAM, RAID arrays, network adapters.	Supports consumer-level hardware like graphics cards, webcams, Bluetooth, etc.
Licensing Cost	Usually more expensive; often requires CALs (Client Access Licenses).	Less expensive and often comes pre-installed on PCs.
GUI	Often minimal or optional; optimized for remote/command-line management.	Full graphical interface with user-friendly features.
Update Cycle	Updates are controlled and tested for enterprise environments.	More frequent updates geared toward consumer needs.
Examples of Use Cases	Domain controller, file/print server, web server, database server, RDP host.	Web browsing, document editing, email, media playback, light gaming.

Windows Server Operating Systems (Server OS)

Version	Release Year	Key Features / Notes
Windows NT 3.1 Advanced Server	1993	First server OS based on NT architecture
Windows NT 3.5 Server	1994	Enhanced network support
Windows NT 3.51 Server	1995	Improved stability
Windows NT 4.0 Server	1996	GUI similar to Windows 95
Windows 2000 Server	2000	Introduced Active Directory
Windows Server 2003	2003	Improved scalability and AD enhancements
Windows Server 2003 R2	2005	Enhanced storage and identity management
Windows Server 2008	2008	Introduced Server Core and Hyper-V
Windows Server 2008 R2	2009	Built on Windows 7 kernel, 64-bit only
Windows Server 2012	2012	Introduced Metro-style UI, improved Hyper-V
Windows Server 2012 R2	2013	Enhanced storage and networking features
Windows Server 2016	2016	Nano Server, Shielded VMs, Docker support
Windows Server 2019	2018	Hybrid cloud, System Insights, improved security
Windows Server 2022	2021	Secured-core server, Azure integration, TLS 1.3
Windows Server 2025 (Upcoming)	Expected 2025	Preview available; aligns with LTSC model

Windows Client Operating Systems (Client OS)

Version	Release Year	Key Features / Notes
Windows 1.0	1985	First GUI OS from Microsoft
Windows 2.0	1987	Overlapping windows support
Windows 3.0 / 3.1 / 3.11	1990–1993	Widespread adoption of GUI OS
Windows 95	1995	Start menu, plug-and-play
Windows 98 / 98 SE	1998–1999	Improved USB support
Windows ME (Millennium Edition)	2000	Consumer OS, unstable reputation
Windows XP	2001	Very popular, long support cycle
Windows Vista	2007	Improved UI (Aero), poor performance issues
Windows 7	2009	Highly stable and widely used
Windows 8	2012	Metro UI, removed Start menu
Windows 8.1	2013	Return of Start button, stability fixes
Windows 10	2015	Windows as a Service (WaaS), continuous updates
Windows 11	2021	Modern UI, centered Start menu, TPM 2.0 required

Windows Server OS Versions & Details:

- *Windows NT 3.1 Advanced Server (1993)*
  - First server OS based on NT architecture, Basic file and print services.
  - Supported limited hardware and small networks.
- *Windows NT 4.0 Server (1996)*
  - Introduced GUI similar to Windows 95.
  - Integrated Internet Information Services (IIS) for web hosting.
  - Basis for early enterprise environments.
- *Windows 2000 Server (2000)*
  - Introduced Active Directory (AD), First OS supporting true domain management.
  - Features like Group Policy, Kerberos authentication, and NTFS improvements.
- *Windows Server 2003 / 2003 R2*
  - Improved AD management (forest and domain functional levels).
  - Volume Shadow Copy, Enhanced IIS 6.0, and Better scalability.
  - R2 added file replication and branch office improvements.
- *Windows Server 2008 / 2008 R2*
  - Server Core (minimal GUI install option), Hyper-V virtualization introduced.
  - Read-Only Domain Controller (RODC), PowerShell 2.0, BitLocker, Failover Clustering.
  - R2 was 64-bit only and based on Windows 7 kernel.
- *Windows Server 2012 / 2012 R2*
  - Introduced Modern UI, Storage Spaces, and IPAM (IP Address Management).
  - Hyper-V Replica for disaster recovery.
  - Dynamic Access Control, NIC teaming, and PowerShell 4.0.
  - R2 added Workplace Join, Web Application Proxy, and Enhanced Hyper-V features.
- *Windows Server 2016*
  - Nano Server (headless, lightweight installation).
  - Shielded VMs and Host Guardian Service for VM protection.
  - Windows Containers and Docker support.
  - Storage Spaces Direct, Just Enough Administration (JEA).
  - Improved security and Azure integration.
- *Windows Server 2019*
  - Hybrid cloud support with Azure Arc and Azure Backup.
  - Windows Admin Center (WAC) introduced.
  - Storage Migration Service, System Insights, and Cluster Sets.
  - Enhanced ATP (Advanced Threat Protection) and Shielded Linux VMs.
  - Enhanced RDP and Edge browser support.
- *Windows Server 2022*
  - Focus on security, hybrid cloud, and performance.
  - Secured-core server, TLS 1.3, AES-256 SMB encryption.
  - Enhanced support for Azure Arc, hotpatching, and faster networking.
  - Nested virtualization for AMD, SMB over QUIC (for secure file sharing).
  - Integration with Azure Automanage and Windows Admin Center.
- *Windows Server 2025* (Upcoming - LTSC)
  - Public preview available in 2024; GA expected in 2025.
  - Enhanced AI integration, cloud management features, and modern UI.

- Focus on deep Azure hybrid features, management APIs, and new Hyper-V capabilities.

Common Roles in All Server OS Versions:

Role	Description
AD DS	Active Directory Domain Services for domain management
DNS	Domain Name System for name resolution
DHCP	IP address allocation in the network
File and Storage Services	File server, DFS, quota management
Hyper-V	Virtualization platform
Web Server (IIS)	Hosting websites and web apps
Remote Desktop Services (RDS)	Virtual desktops and remote access
Print Services	Manage shared network printers

Installation Options:

- *Server with Desktop Experience*
  - Full GUI,
  - Suitable for administrators who prefer GUI tools.
- *Server Core*
  - Minimal interface
  - Command-line (PowerShell) only,
  - Secure and lightweight.
- *Nano Server (2016 only)*
  - Ultra-light,
  - Remote-managed
  - Used for containers and microservices.

Windows Server Editions

Windows Server 2016 Editions

Edition	Description
Datacenter	Full feature set for large-scale virtualization (unlimited VMs), Storage Spaces Direct, Shielded VMs, Software-defined networking.
Standard	Same core features as Datacenter but limited to 2 VMs and no advanced storage/networking features.
Essentials	Designed for small businesses with up to 25 users and 50 devices. No virtualization rights.
MultiPoint Premium Server *(retired)*	Multi-user shared desktop experience; rarely used in enterprises.

Windows Server 2019 Editions

Edition	**Description**
Datacenter	Ideal for **high-density virtual environments** and hybrid cloud. Includes all advanced features.
Standard	Supports up to **2 VMs** and 1 Hyper-V host. Lacks some advanced features like Shielded VMs, Storage Replica (limited to 1 volume up to 2TB).
Essentials	Still limited to **25 users/50 devices**. Reduced features, no Hyper-V role.
Hyper-V Server 2019 *(free, headless)*	Core-only edition focused **solely on virtualization** (no GUI, no roles other than Hyper-V).

Windows Server 2022 Editions

Edition	**Description**
Datacenter	Full-featured: **unlimited VMs**, **Shielded VMs**, **Software-defined Networking**, **Storage Spaces Direct**, **Hotpatching**, **SMB over QUIC**.
Standard	Includes core roles like AD, DNS, DHCP. Supports **2 VMs** only, limited Storage Replica (same as 2019).
Essentials	Still capped at **25 users / 50 devices**. Ideal for very small businesses; fewer admin tools.
Azure Datacenter: Azure Edition	For Azure Stack HCI and cloud environments. Includes **Hotpatching**, **SMB over QUIC**, and other Azure-only features.

Windows Server 2025 (Preview Stage - LTSC)

Edition	Expected Features
Datacenter	Focus on deep Azure hybrid integration, improved virtualization, enhanced GPU and container support, advanced security (like Secured-core).
Standard	Base roles only; still supports 2 VMs. Same kernel and feature base as Datacenter but feature-limited.
Azure Datacenter Edition	Specific to Azure customers. Enhanced **cloud-first features**, like **Automanage**, **Hotpatching**, and **containers-as-a-service**.
Essentials (Tentative)	May continue or be phased out. Microsoft recommends **Microsoft 365 Business Premium** + Azure AD for small businesses.

Edition Comparison Summary

Feature	Datacenter	Standard	Essentials
Virtualization Rights	Unlimited VMs	2 VMs	None
User/Device Limit	Unlimited	Unlimited	25 users / 50 devices
Storage Spaces Direct	✅	❌	❌
Shielded VMs	✅	❌	❌
Hotpatching (2022/2025)	✅ (Azure Ed)	❌	❌
Windows Admin Center	✅	✅	✅
Licensing Model	Core-based	Core-based	Server-based

Notes:

- Datacenter & Standard use core-based licensing (minimum 8 cores per processor, 16 cores per server).
- Essentials uses a flat server license, no CALs needed.
- Client Access Licenses (CALs) are required for Datacenter and Standard editions.

Windows Server Physical Requirements Comparison

Requirement	Windows Server 2016	Windows Server 2019	Windows Server 2022	Windows Server 2025 *(Preview)*
Processor (CPU)	1.4 GHz 64-bit, compatible with x64 architecture	Same as 2016	1.4 GHz 64-bit, x64 with compatible instruction set (SLAT for Hyper-V)	1.4 GHz or faster, x64-based, SLAT support
CPU Cores	Minimum: 1 core Recommended: 2+ cores	Same	Same	Same
RAM (Minimum)	512 MB (2 GB for Server with Desktop Experience)	Same	512 MB (2 GB for Desktop Experience)	2 GB minimum
RAM (Recommended)	4 GB+ (depending on roles)	4 GB+	4 GB+	8 GB+ (expected due to Azure/AI features)
Disk Space (Minimum)	32 GB	32 GB	32 GB (more if updates/roles installed)	64 GB (expected minimum)
Disk Space (Recommended)	40–60 GB	40–60 GB	60 GB+	100 GB+
Network Adapter	Ethernet with Gigabit throughput; PCI Express compliant	Same	Same + UEFI and Secure Boot for Secured-Core	Same, but NIC offloading/virtualization features recommended
Display Adapter	Super VGA (1024 x 768) or higher	Same	Same	Same
Firmware	BIOS or UEFI	BIOS or UEFI	UEFI 2.3.1c-based, Secure Boot capable	UEFI with TPM 2.0 mandatory (for secured-core features)
TPM	Optional	Optional	TPM 2.0 Recommended	TPM 2.0 Required for some features
Internet Access	Not required but recommended for updates	Same	Required for some features like WAC, Azure Arc	Required for hybrid/Azure integration

Notes:

- GUI (Desktop Experience) requires significantly more RAM and disk compared to Server Core.
- Windows Server 2022/2025 enable Secured-Core server features which require:
    - UEFI with Secure Boot
    - TPM 2.0
    - CPU virtualization extensions (like Intel VT-x or AMD-V)
- Some advanced features like Hyper-V, Shielded VMs, or Storage Spaces Direct require:
    - SLAT (Second Level Address Translation)
    - More memory and multiple NICs
    - High IOPS storage (SSD/NVMe recommended)

Best Practice Hardware for Production Use:

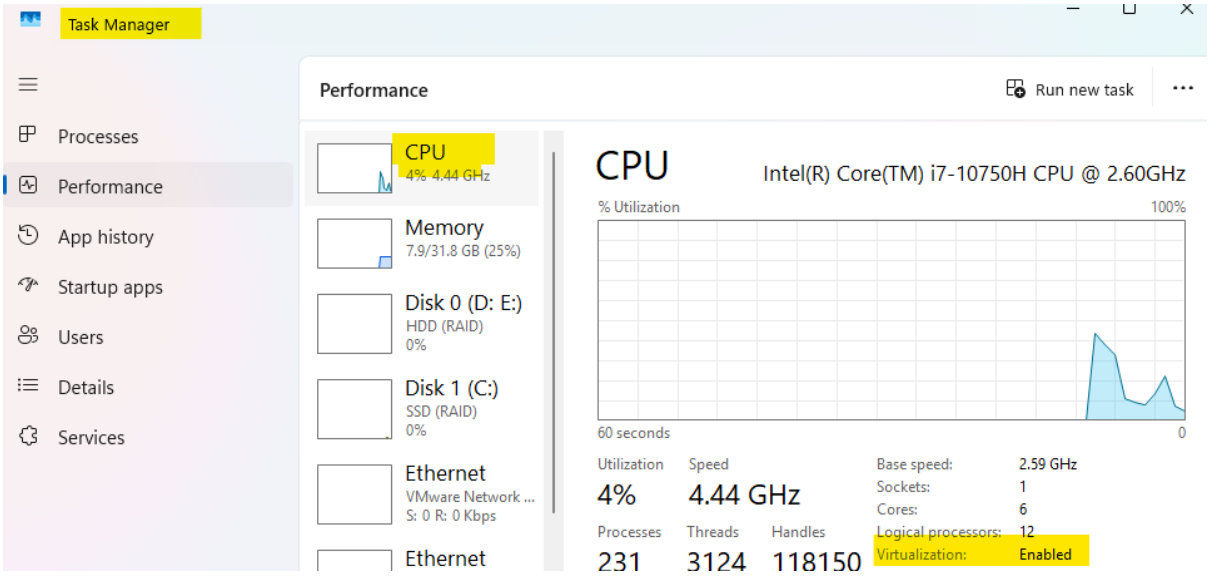
Component	Recommended
CPU	4+ core modern x64 processor
RAM	16–64 GB depending on roles
Disk	240 GB+ SSD or RAID array
NIC	Dual or quad Gigabit / 10GbE
TPM/UEFI	Required for newer features and security

Creating Windows Server Operating System (OS)

Pre-requisites

- ✓ A hypervisor tool – VMWare workstation, Microsoft Hyper-V, Oracle Virtual Box
- ✓ ISO file – appropriate ISO file for the server installation of Win server 2016 (or any other).
- ✓ Internet connectivity – Yes
- ✓ Guest OS (OS where you are going to install VM) requirement:
  - Minimum RAM: 4GB
  - Minimum HDD: 100 GB
  - CPU: 1.4GHz
- ✓ Knowledge on:
  - Computer hardware (link to study, watch video here)
  - Operating system (client and server) – (watch video for details)
  - Computer Networking – IPv4 & IPv6. (Networking, IP & subnetting)
- ✓ Virtualization (Intel VT/AMD-V) must be enabled

To validate, go to Task Manager:



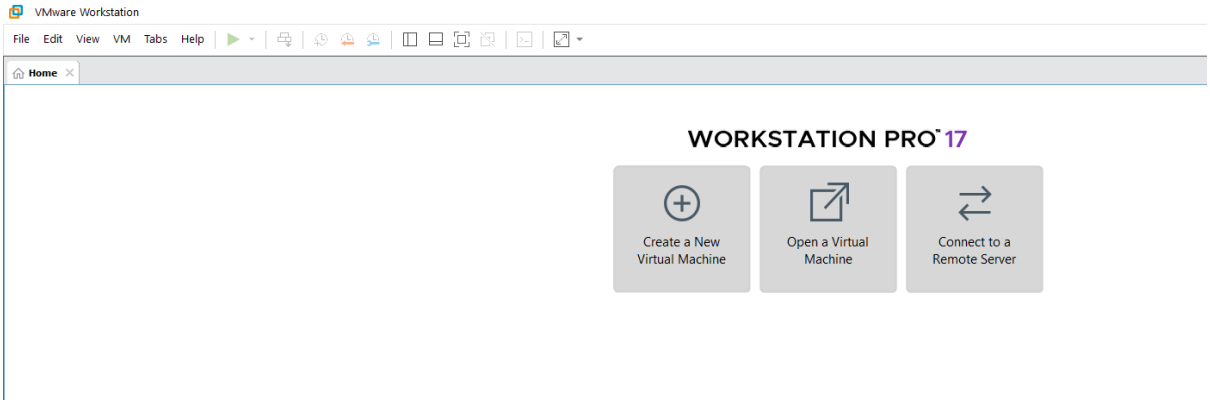
Resources

- Product Resources | Windows Server technical documentation
- Community | Microsoft Tech Community: Windows Server
- Getting Started Guides | Get started with Windows Server
- Learning Path | Windows Server deployment, configuration, and administration

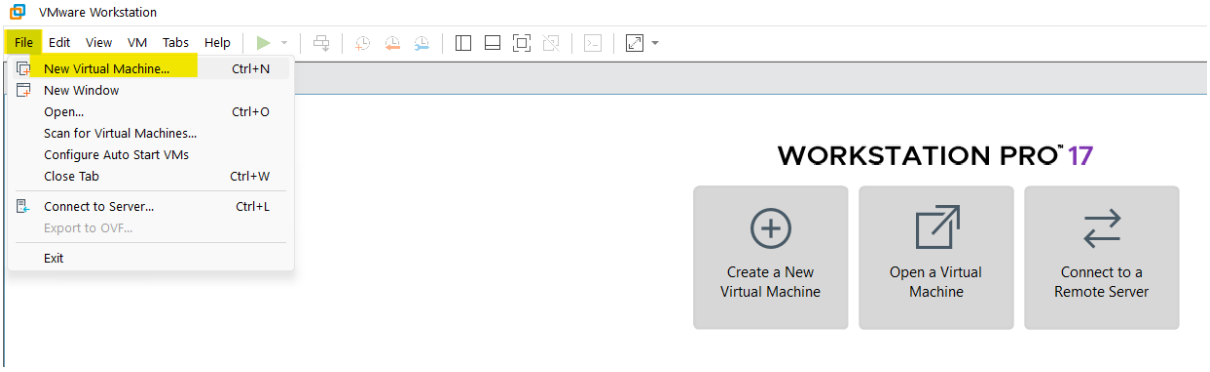
Note – You must know the basics before you proceed further.

To create a new windows server virtual machine using VMWare Workstation 17 or above

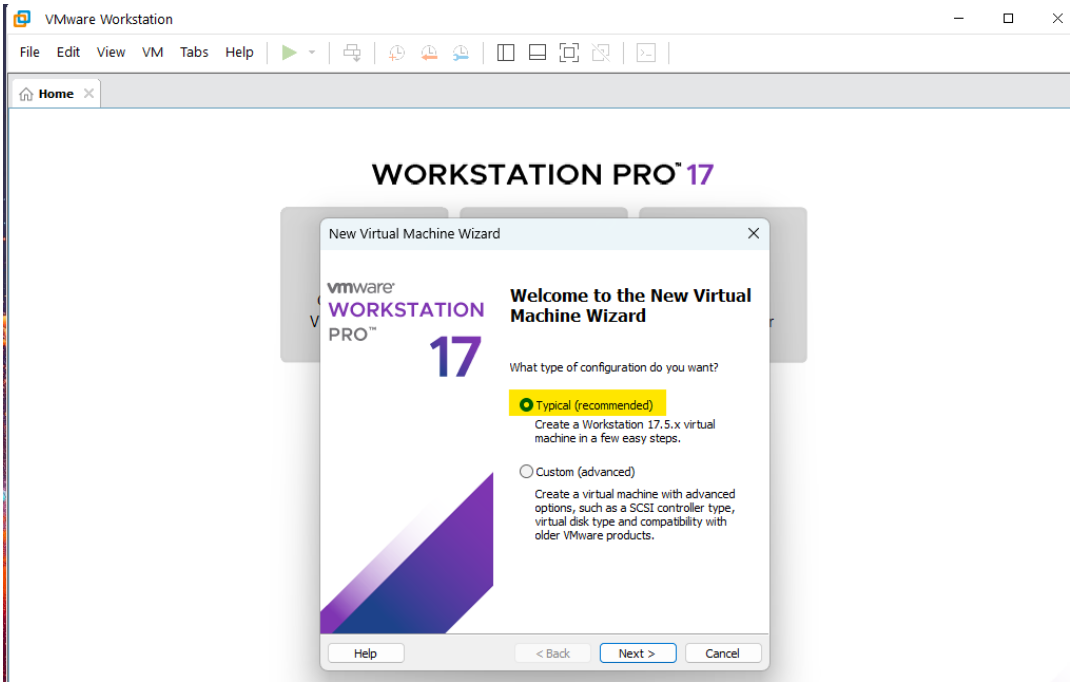
Open VMWare Workstation



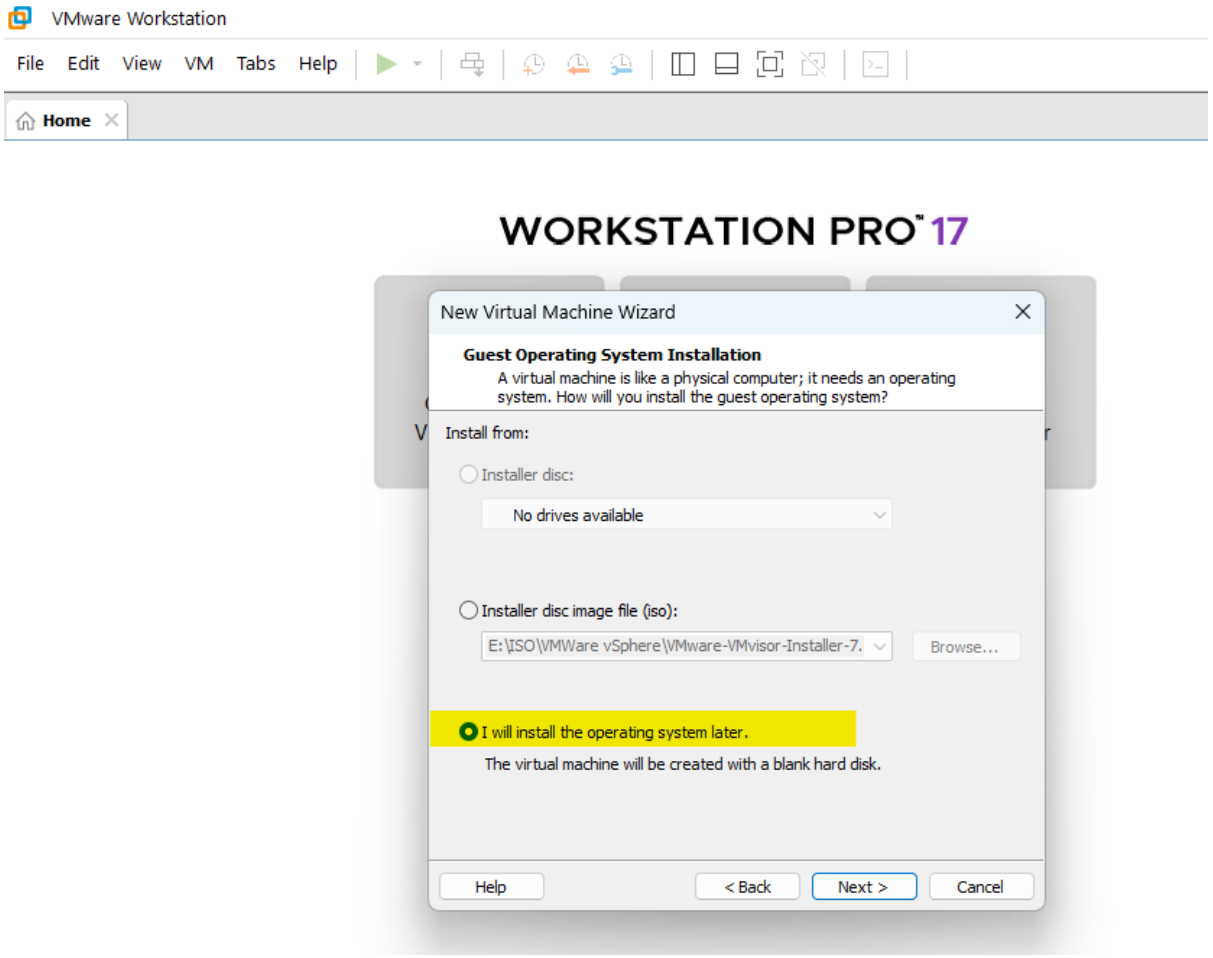
Go to File → New Virtual Machine…



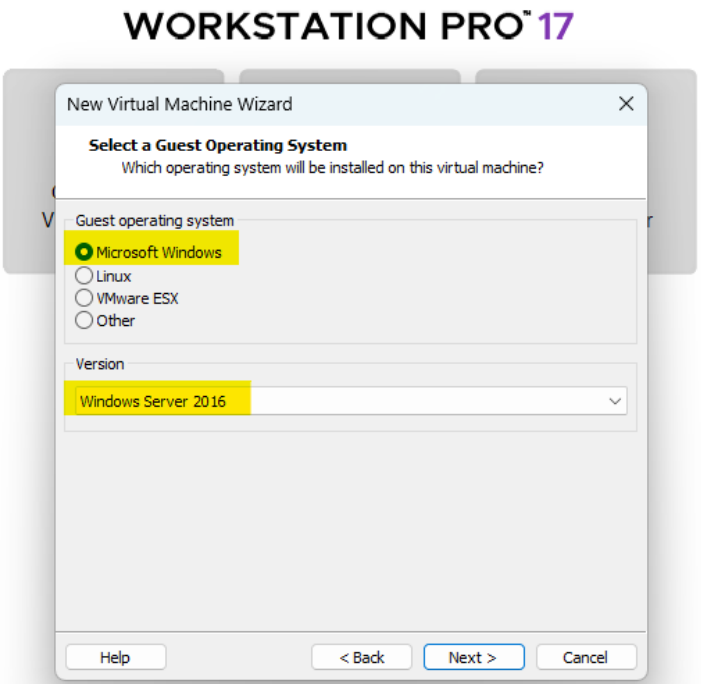
In the welcome wizard, select “typical”



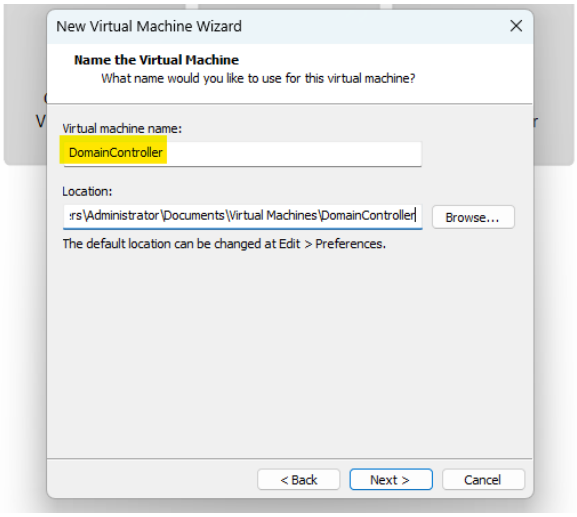
In the “Guest Operating System Installation” wizard, select “I will install the OS later:



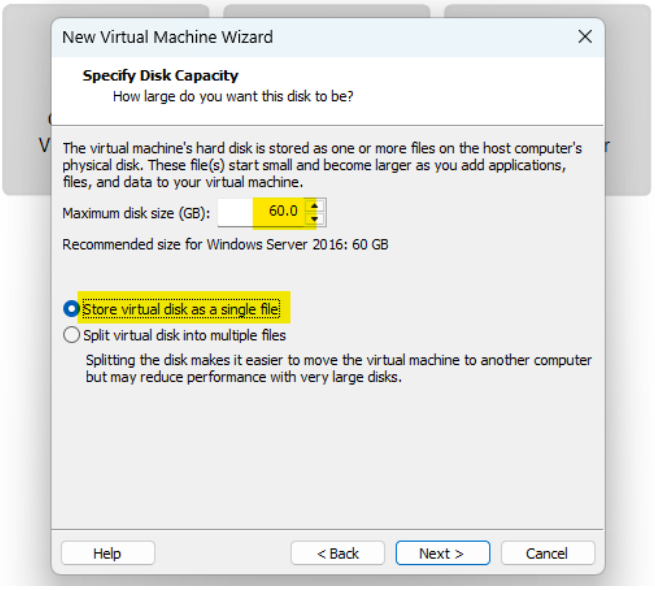
Under the Guest OS, select the appropriate operating system. In our case it’s Windows Server 2016



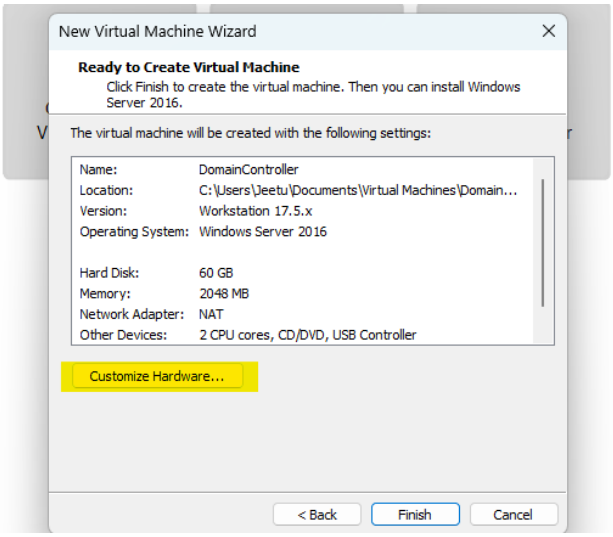
Under “Name the Virtual Machine” wizard, write the VM name (this can be changed later also)



Under “Specify Disk Capacity”, provide disk size for WinSVR2016

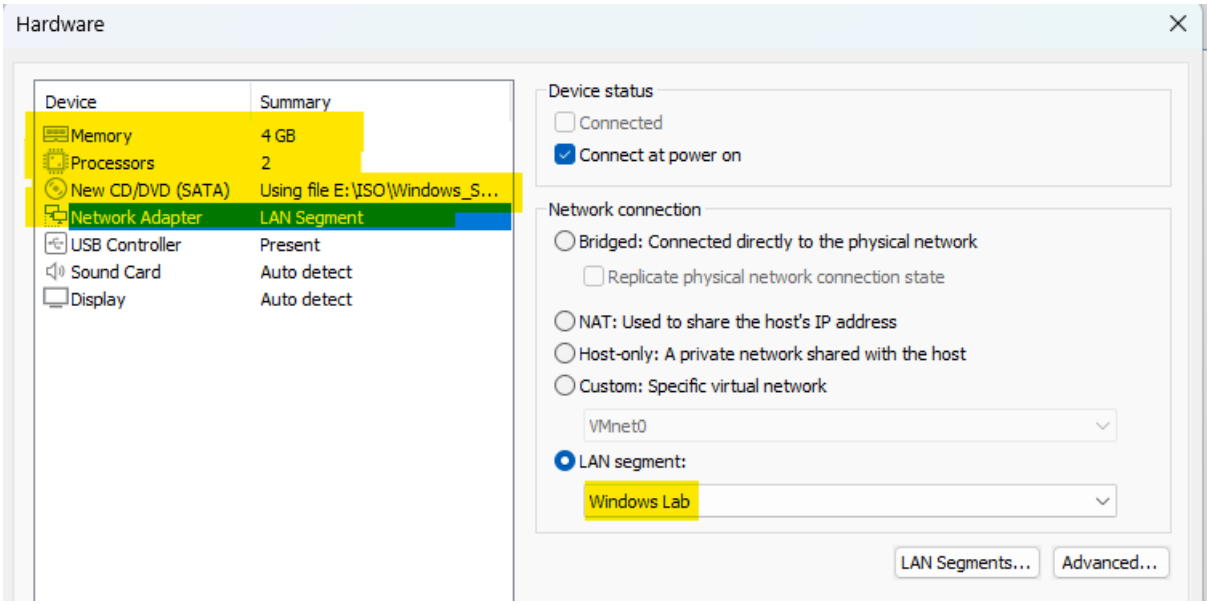


Before you finish, select “Customize Hardware…”



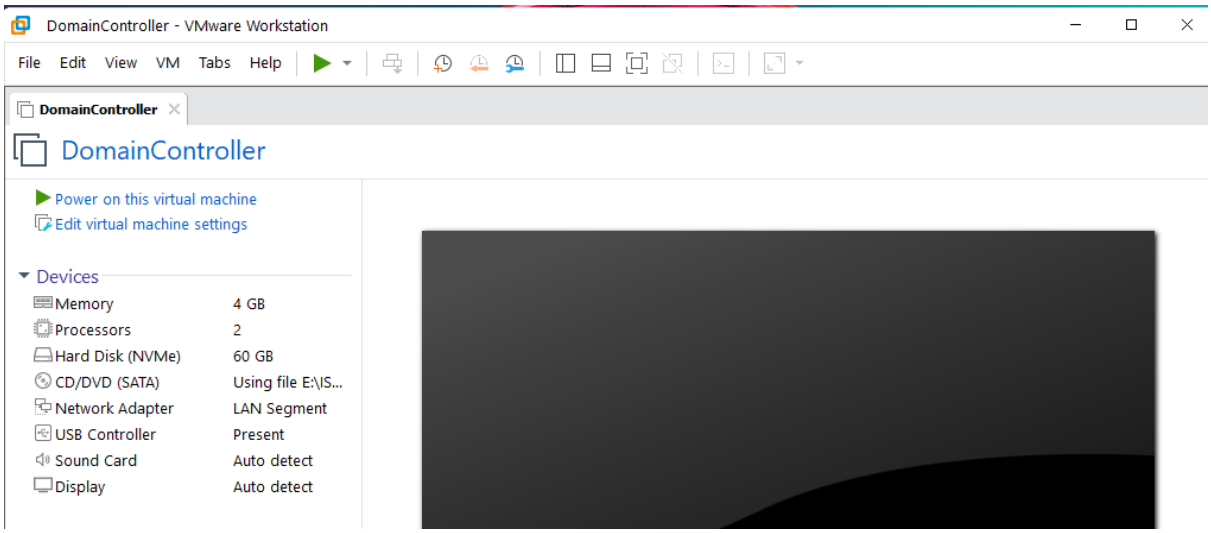
Configure the hardware based on the needs:

- RAM: 4GB
- Processors:
  - Number of processors: 1
  - Number of cores per processors: 2
- New CD/DVD (SATA)
  - Use ISO image file: <select the Window server 2016 ISO file>, by clicking on browse.
- Network Adapter
  - LAN Segment → LAN Segments… → Add → Provide a name “Windows Lab” → Ok
  - LAN Segment → drop down → select “Windows Lab” → close



In the “Ready to create virtual machine” wizard → Finish

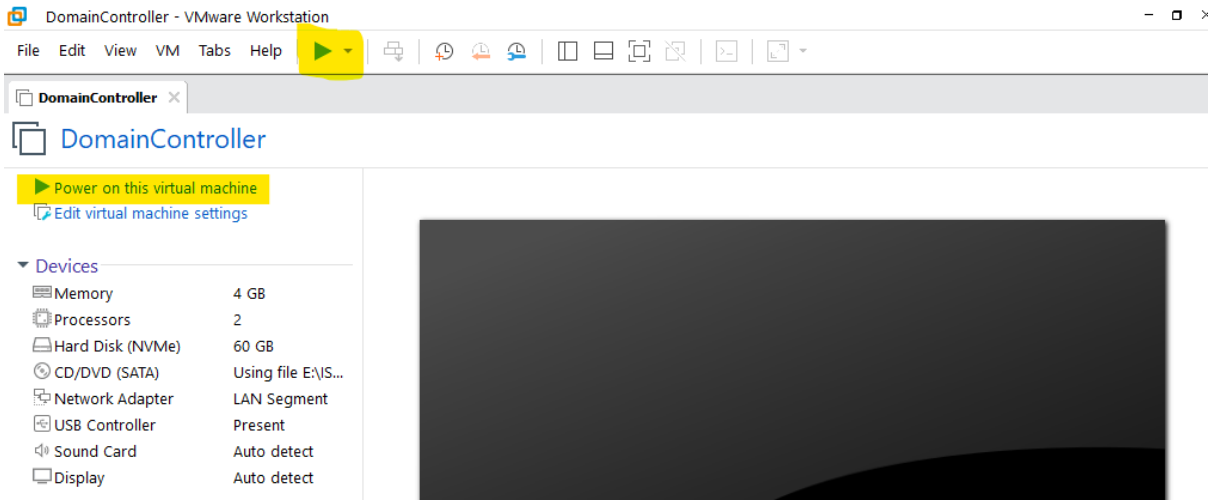
Verify:



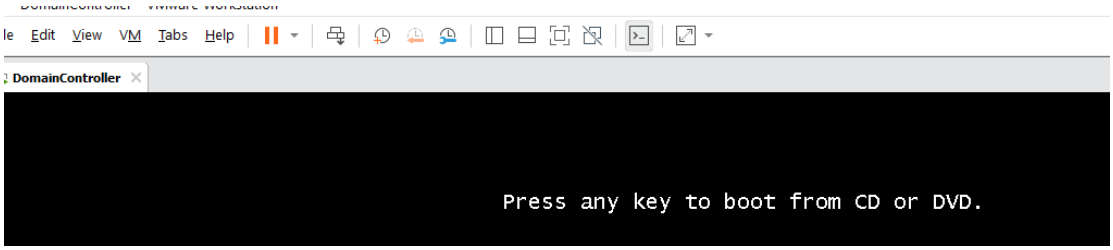
Question – How many VMs can be created (not running) within VMWare Workstation?

Installing a windows server 2016

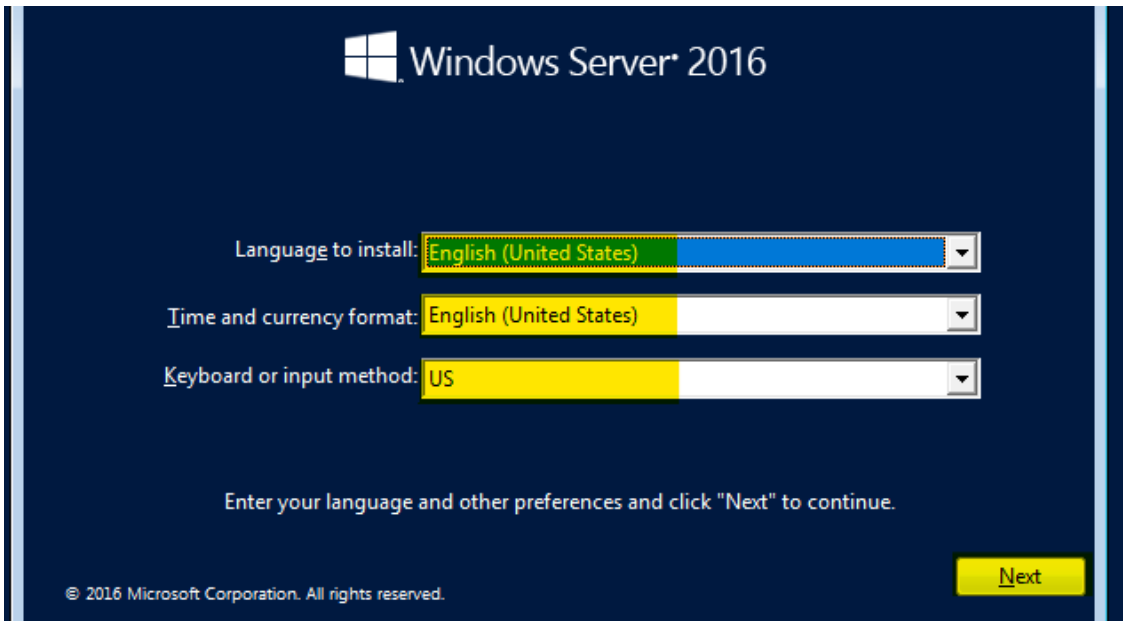
To Power On the VM, use either of following:



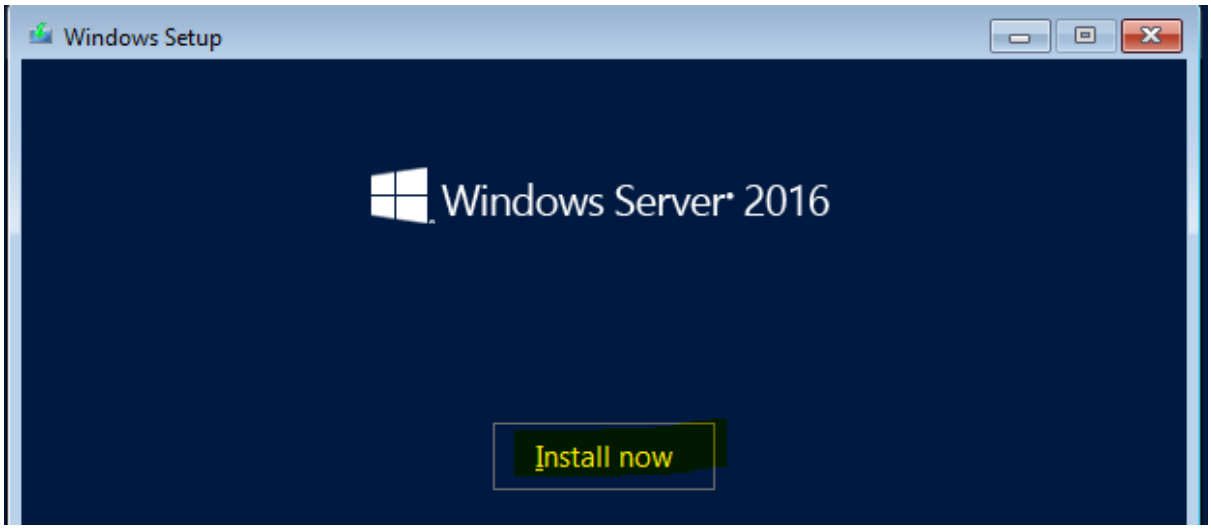
Once VM is powered on, click inside the VM and wait until it prompts “Press any key to boot from CD or DVD.”



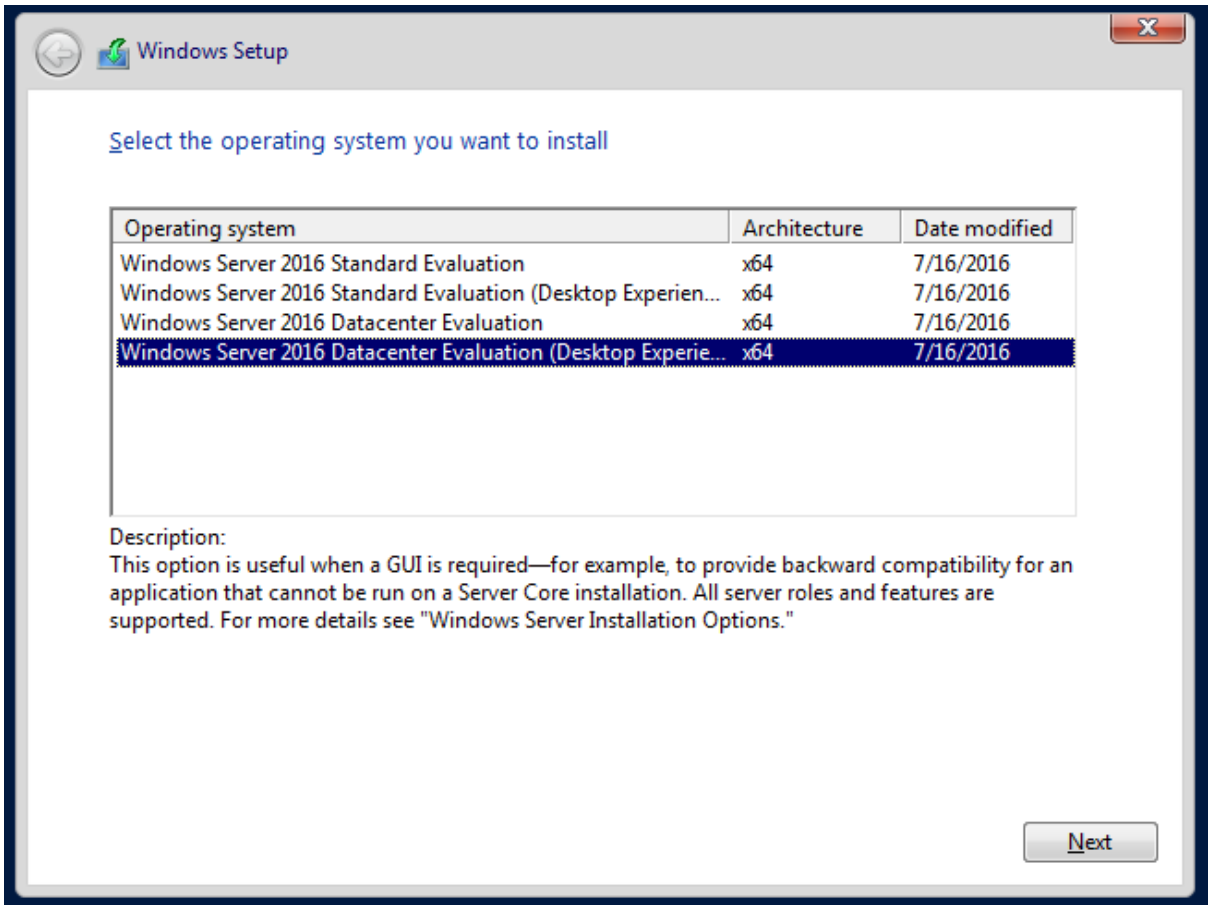
Once you get this screen, press “space button” on your keyboard and wait the fill the following:



Click the button “Install Now”

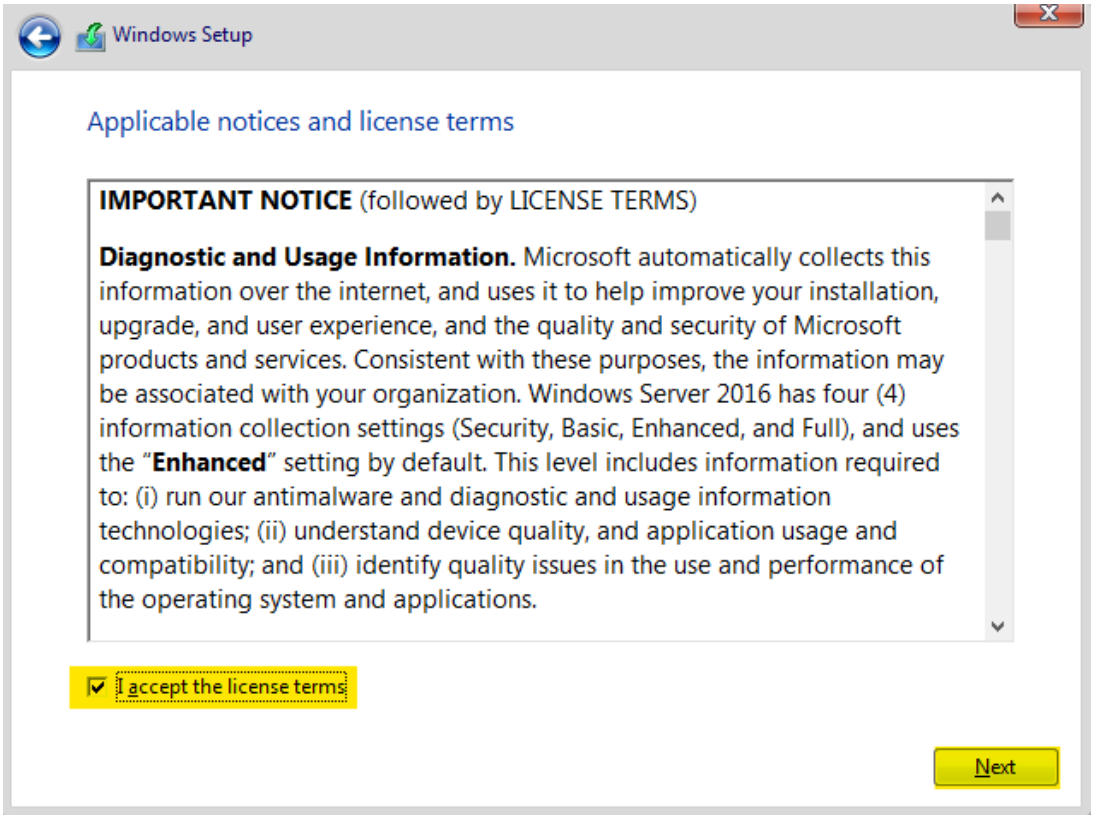


To install the Windows Server – GUI (select Desktop experience)

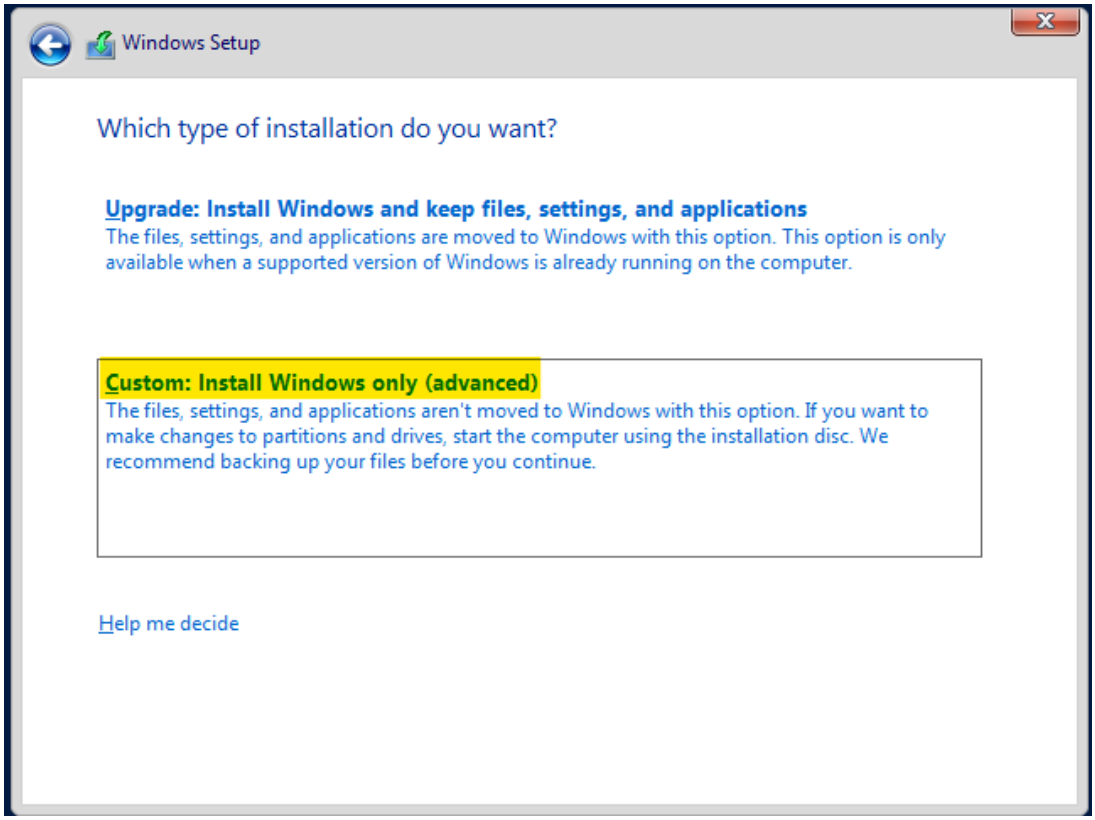


- Here’s the comparison of various Windows Server.
- To install server core (or CLI) operating system, select “Windows Server 2016 Standard or Datacenter Evaluation (not Desktop Experience).

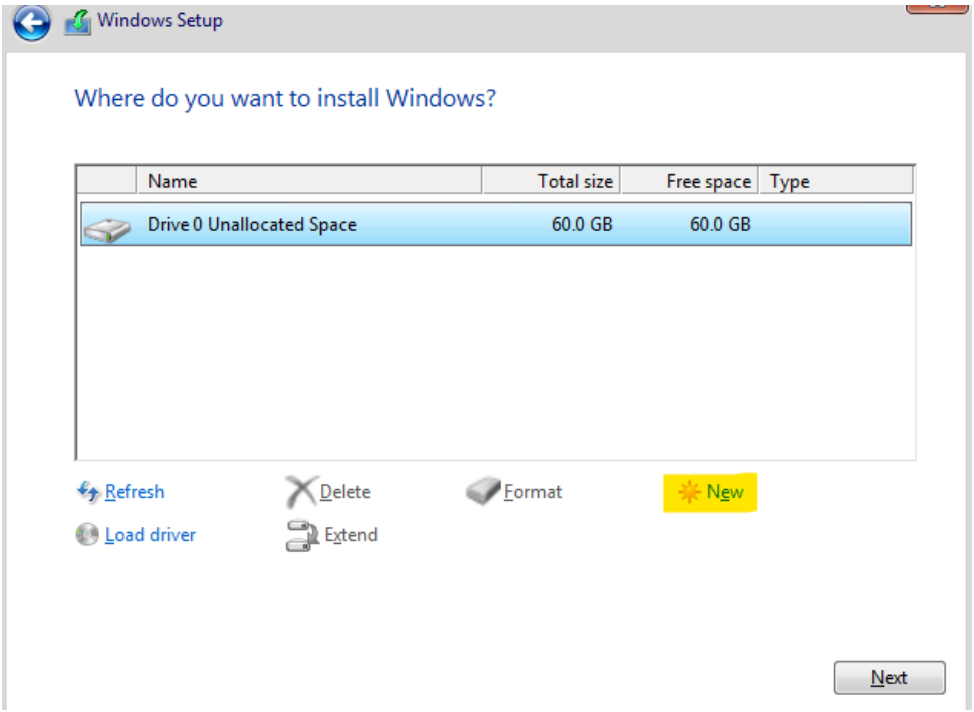
Accept the license agreement.



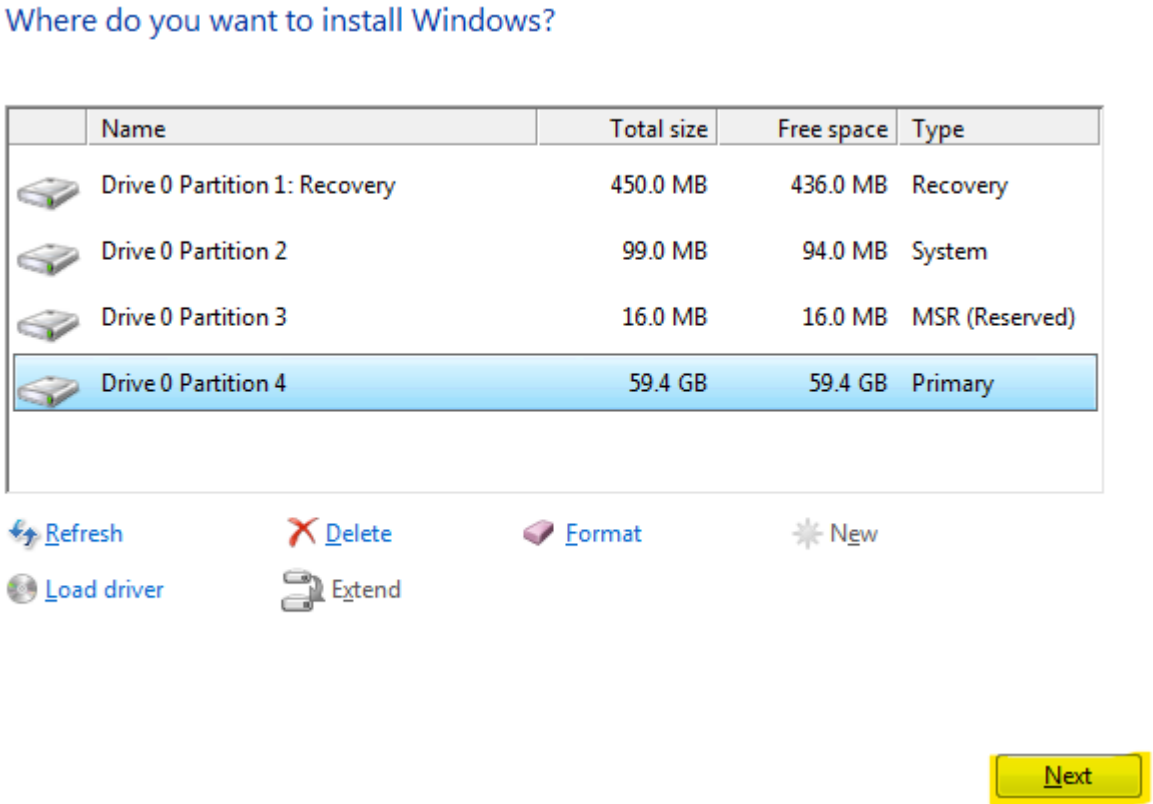
Select "Custom: Install Windows only" for fresh installation. Else, you can select "Upgrade", if you want to upgrade existing operating system.



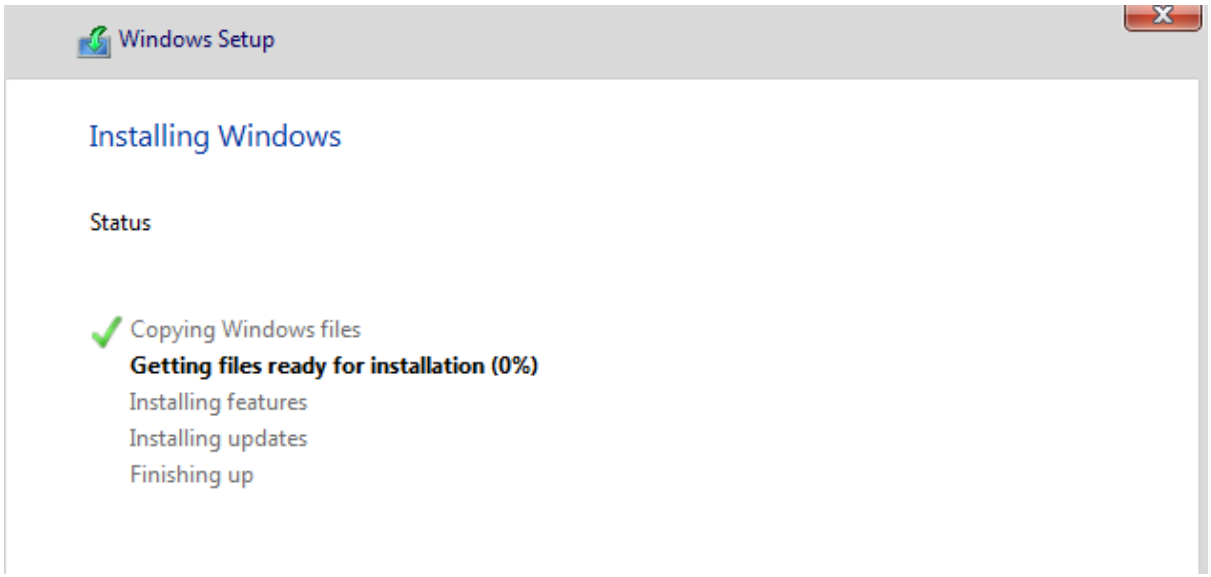
To create required partitions, click “New” → Apply → Ok.

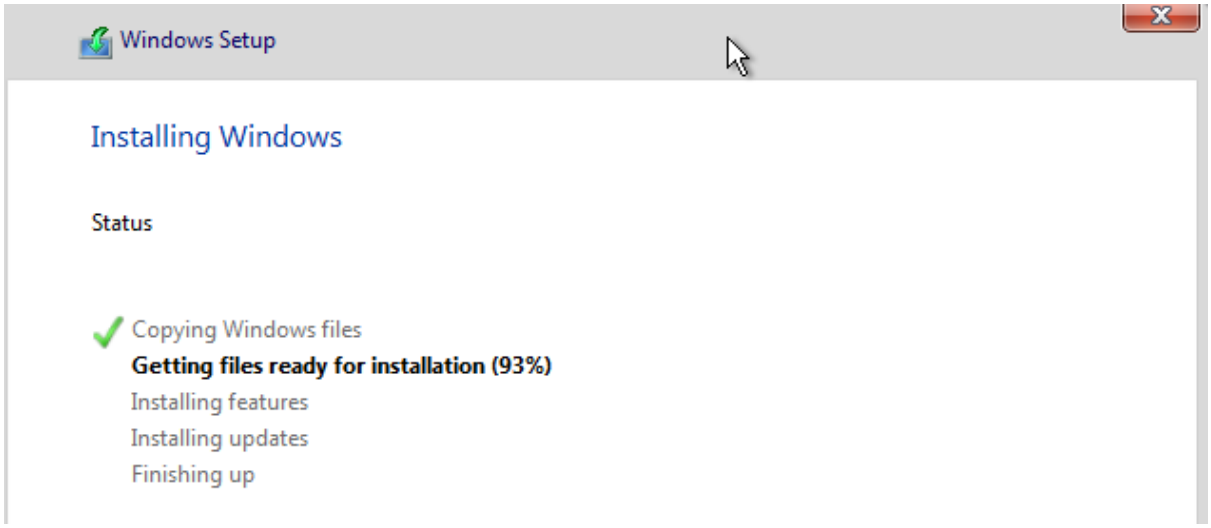


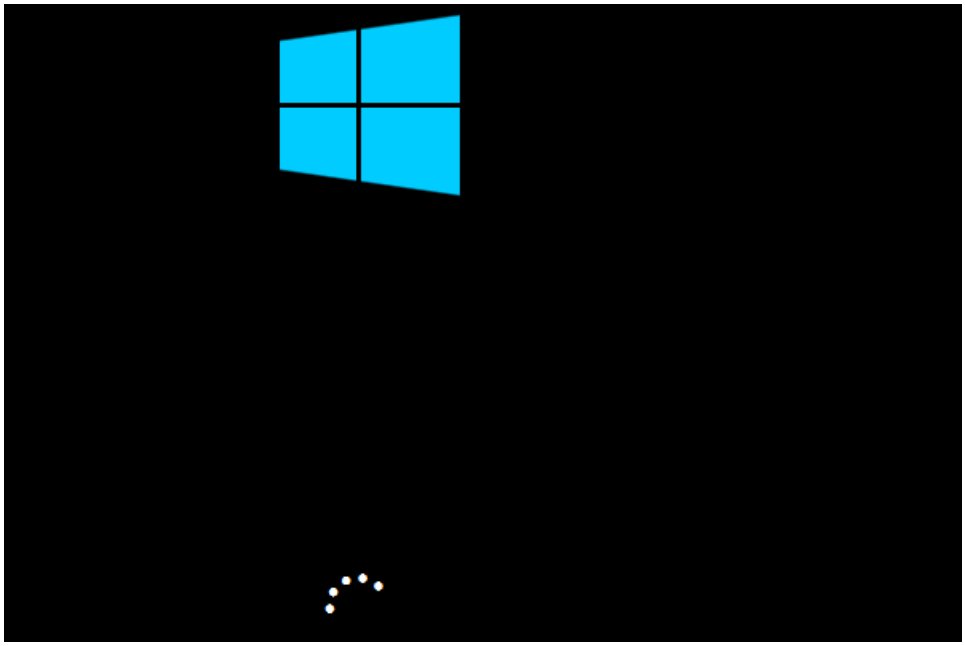
After creating partitions, click on “Next”



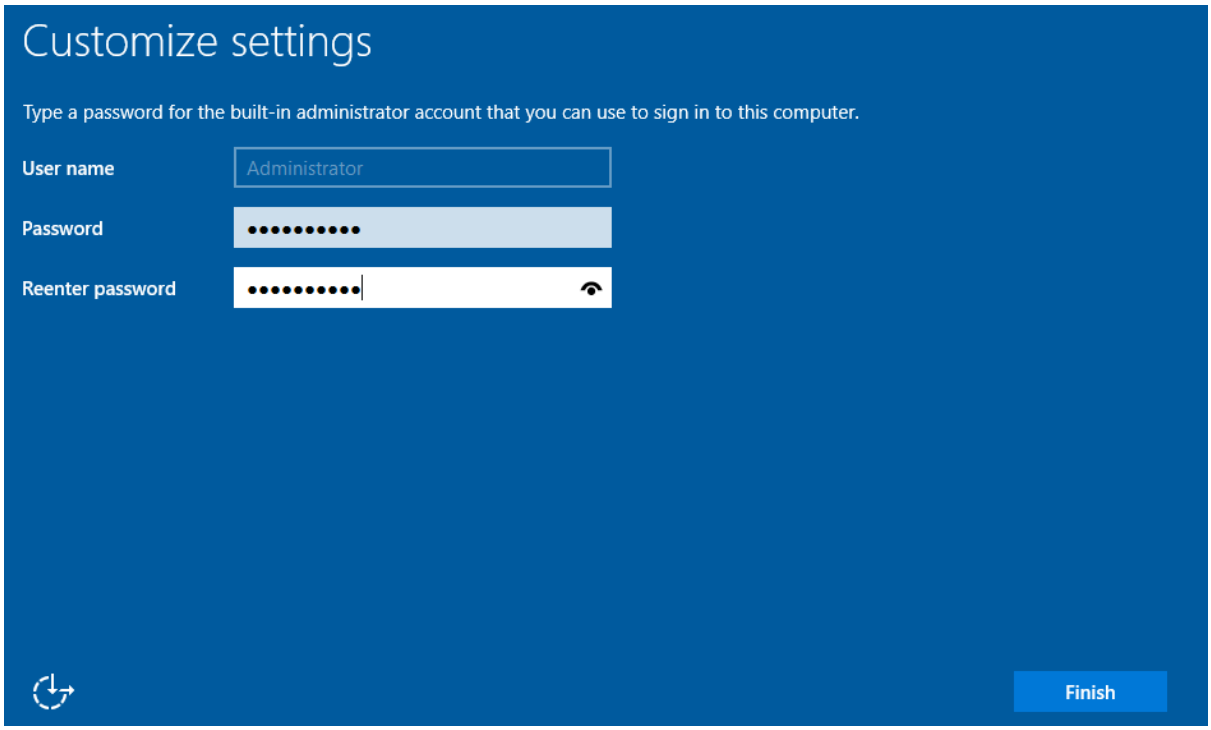
Wait until the installation is completed, and then reboot (else it will auto-reboot)



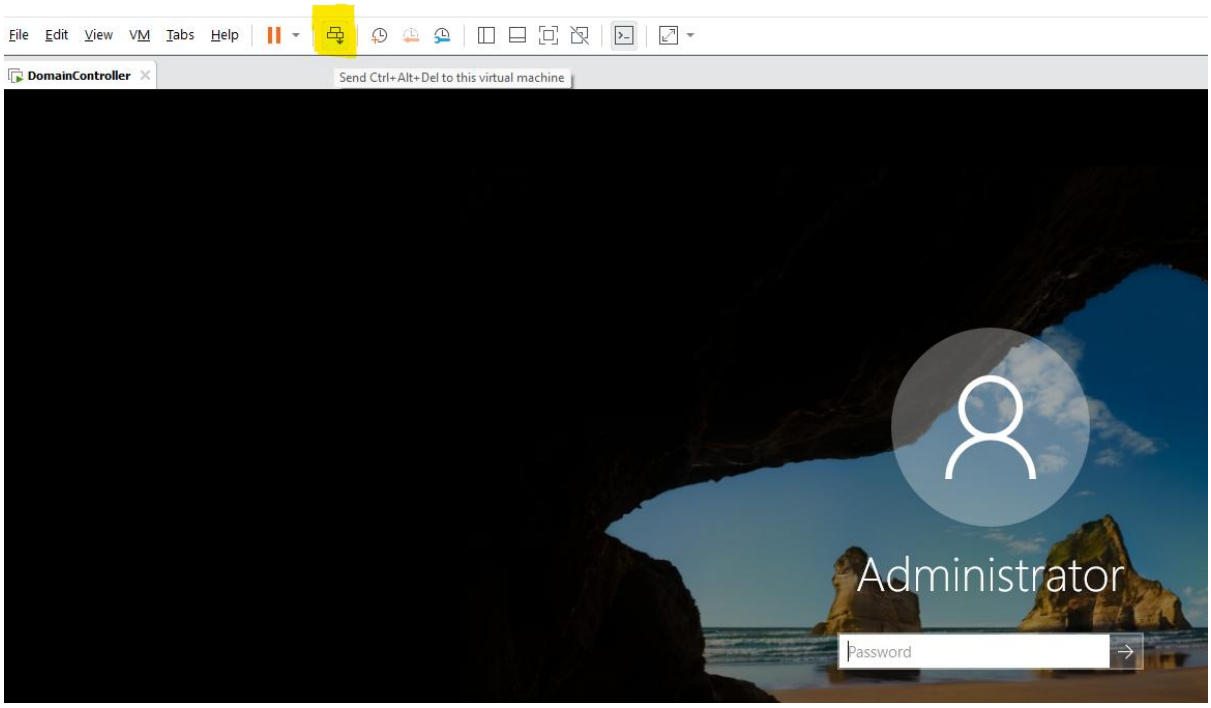




Set the local “Administrator” password



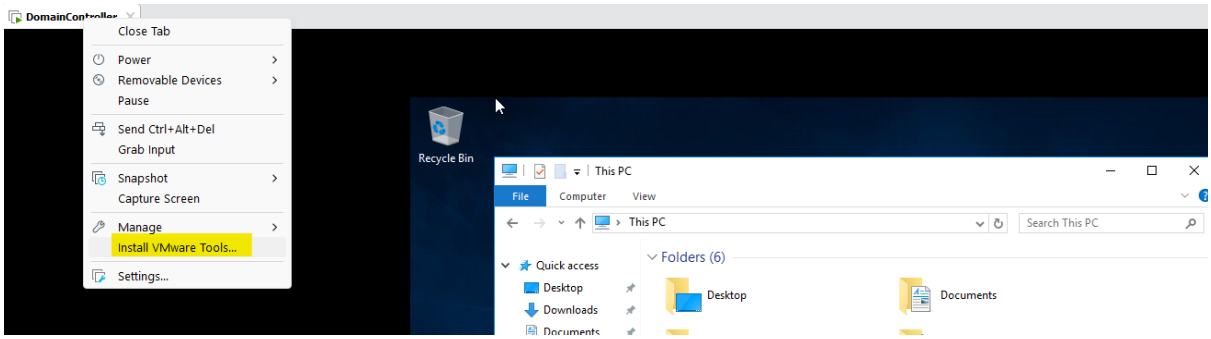
Press “Ctrl+Alt+Del” button to unlock screen and type password.



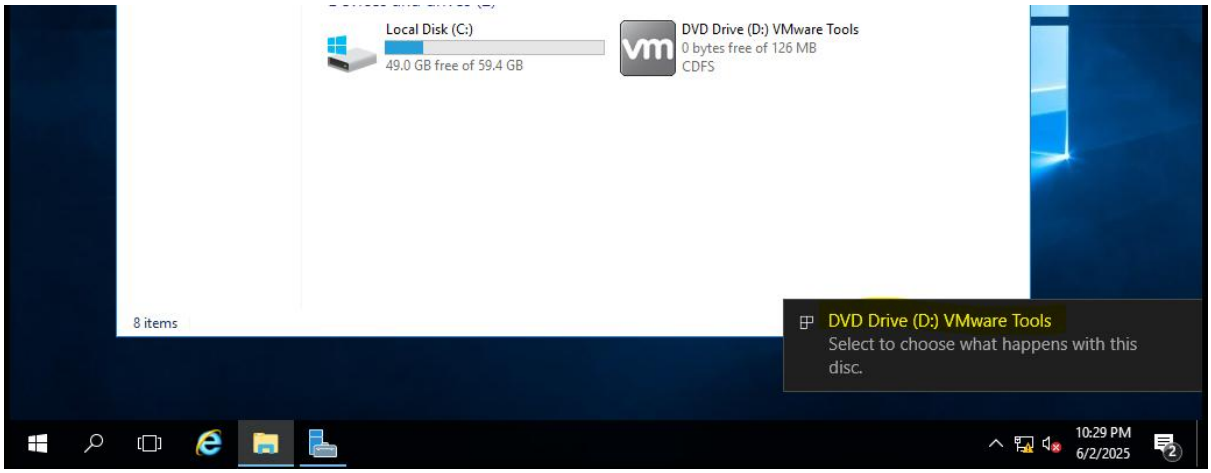
Installing VMWare Tools on DC

Once logged-in, install the VMWare tools so that you can work on complete screen.

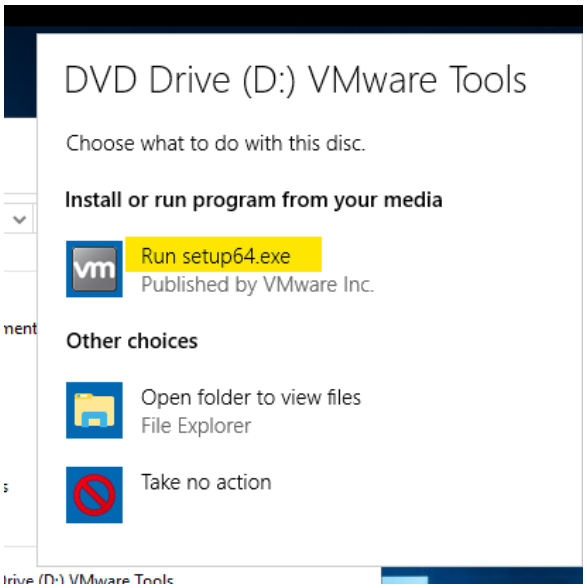
To install VMWare tools, right click on the VM name on the top virtual machine tab.



Click left bottom tab:

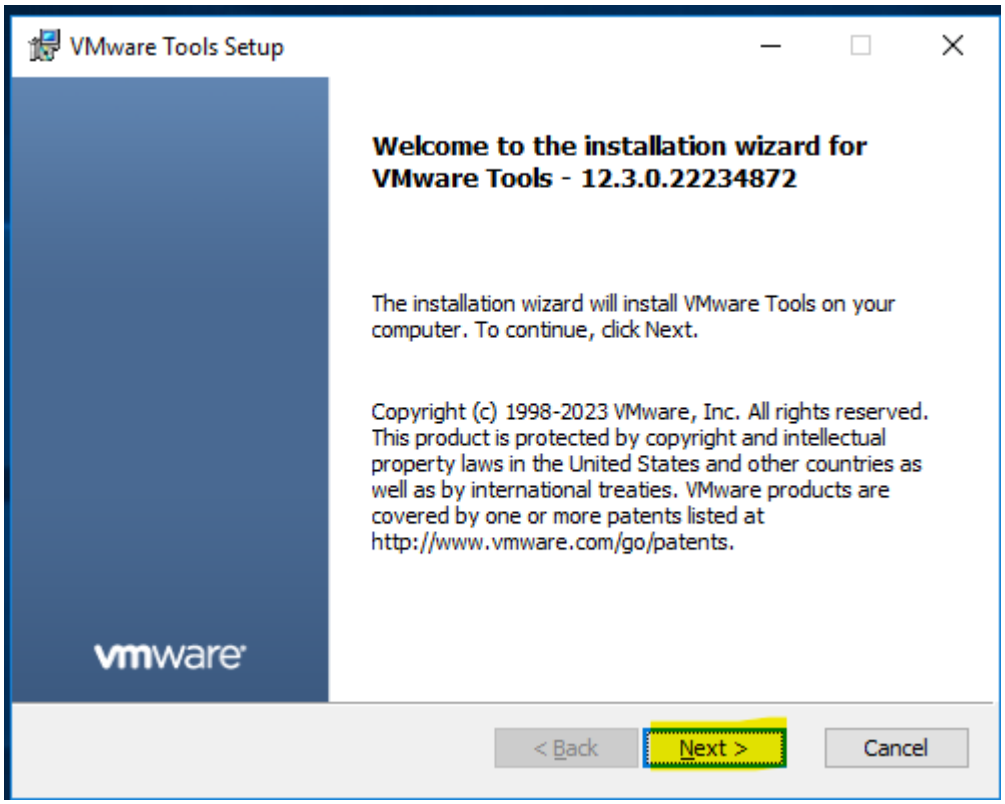


Click on “Run setip64.exe” from the options listed

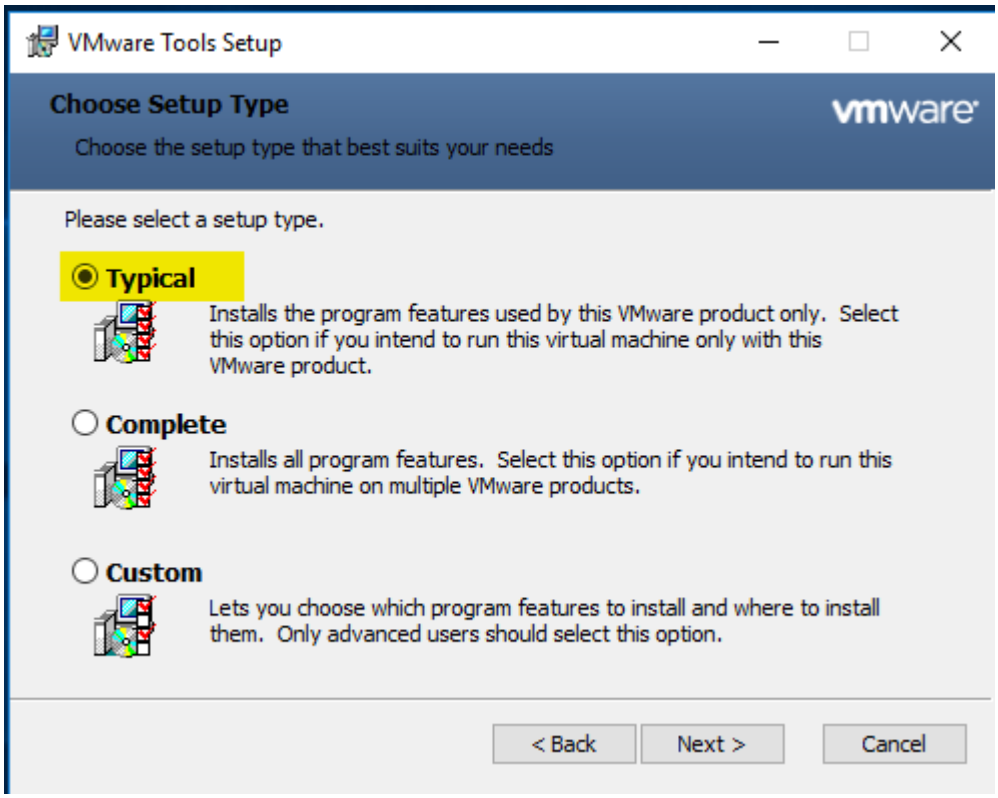


Note – if these options aren’t present, just double click on the D:\ drive, under This PC.

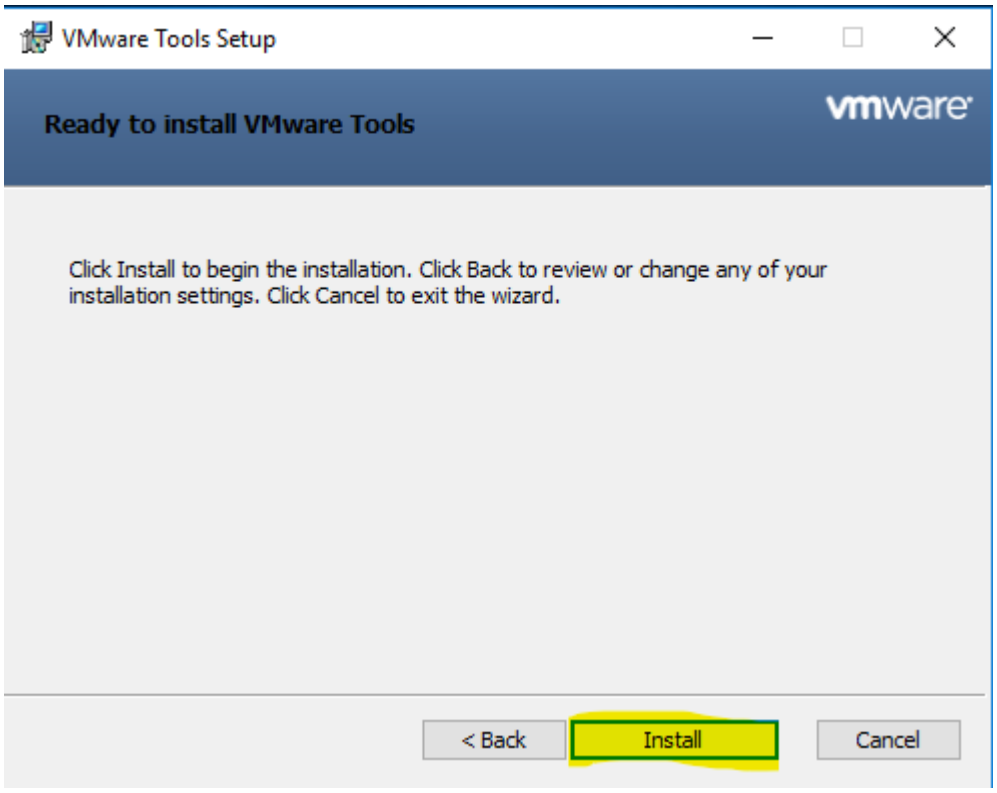
On welcome wizard, click Next



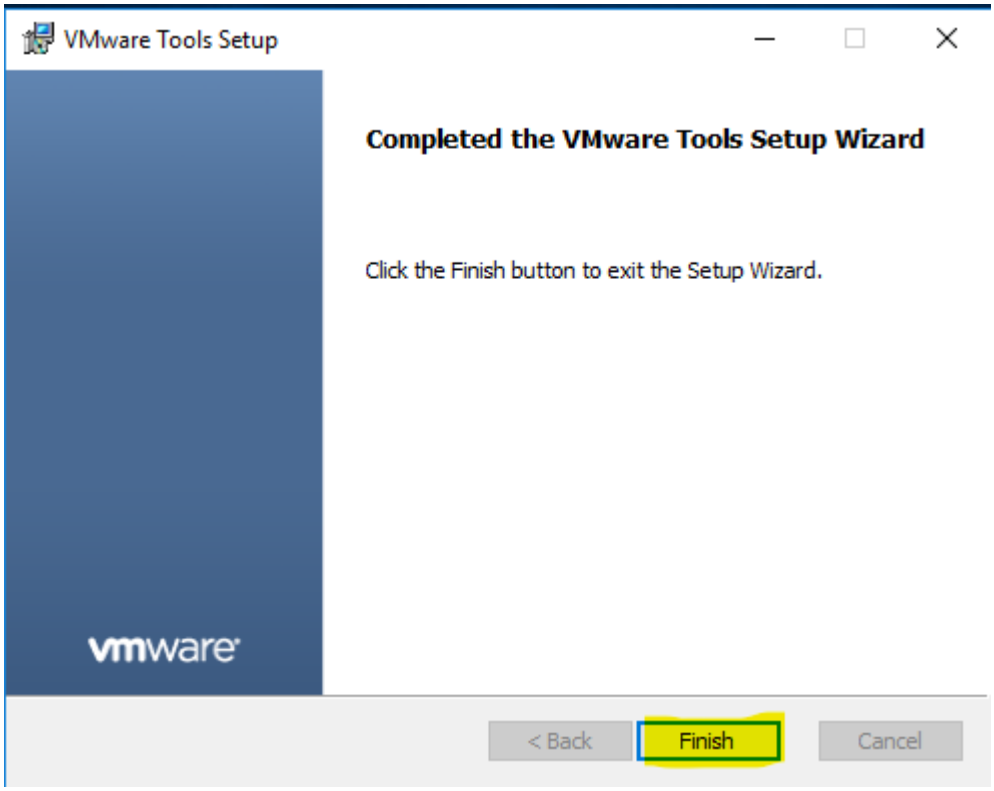
Under choose setup type, select typical.



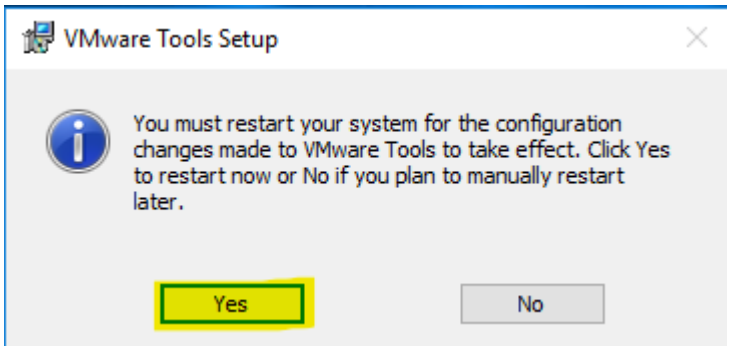
Select “Install”



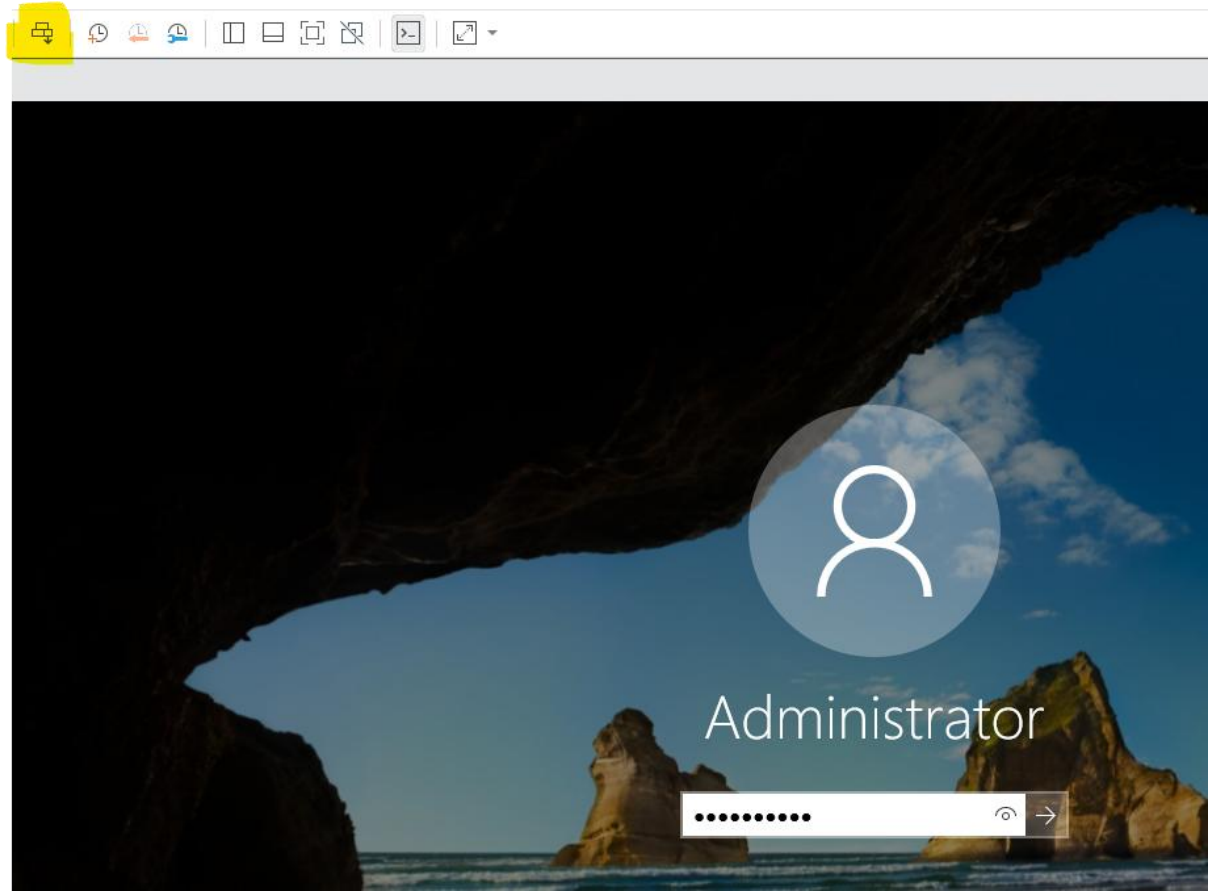
Click on Finish,



And reboot the VM.

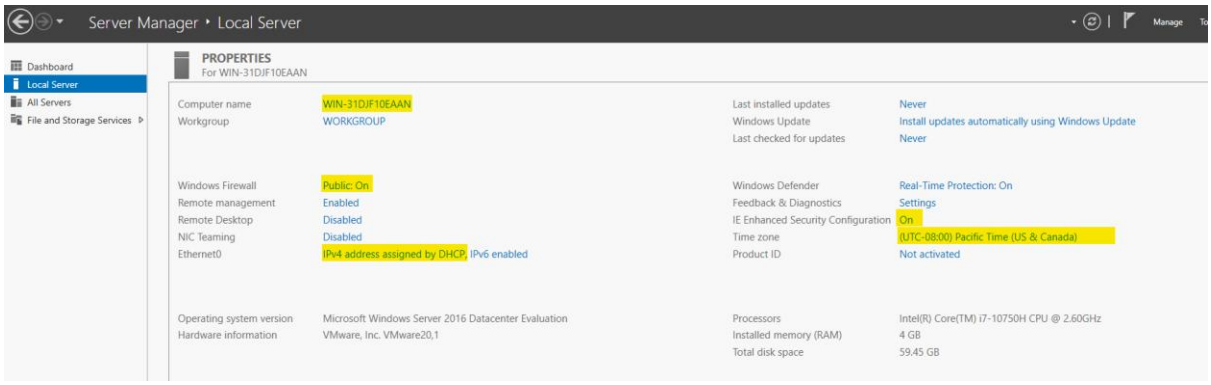


After reboot, press “Ctrl+Alt+Del” from VMWare workstation to unlock and type password



Post Installation configuration on DC

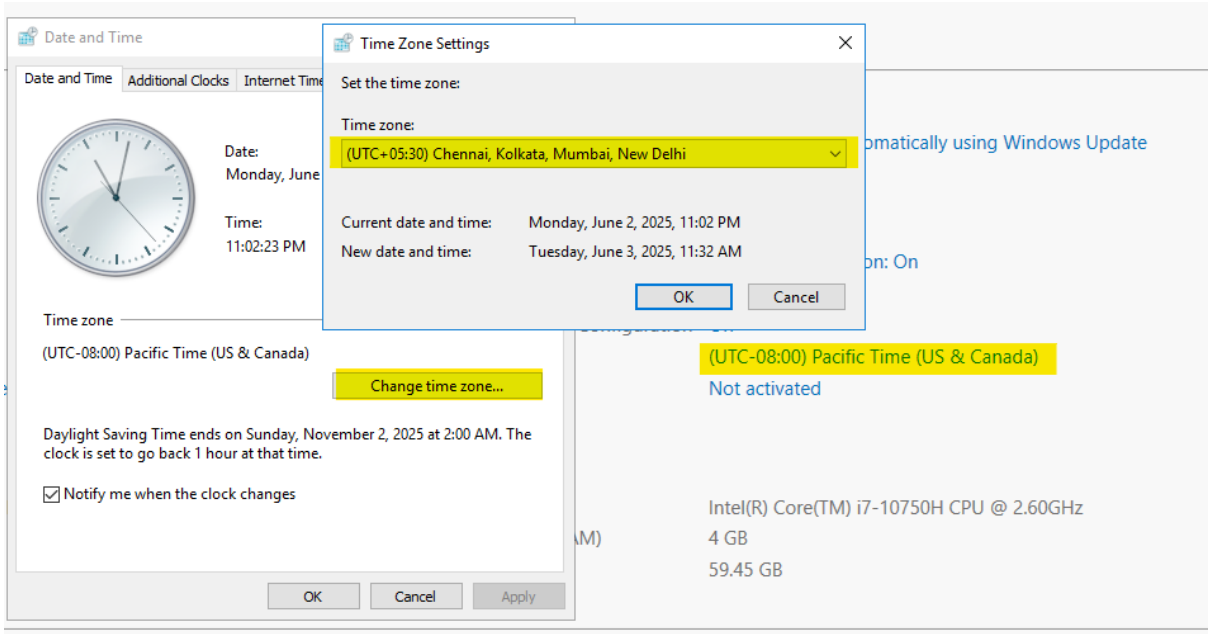
On the server manager dashboard page, click on “Local Server” and perform post-installation configuration



Under post-installation configuration, perform the following

- Change the computer name (at last, because it will reboot the system)
- Disable “firewall”
- Change the IP address:
    - IP Address: 192.168.10.10
    - Subnet Mask: 255.255.255.0
    - Default Gateway: 192.168.10.10
    - DNS: 192.168.10.10
- Turn “IE Enhanced security configuration”: OFF
- Time zone: (+05:30)

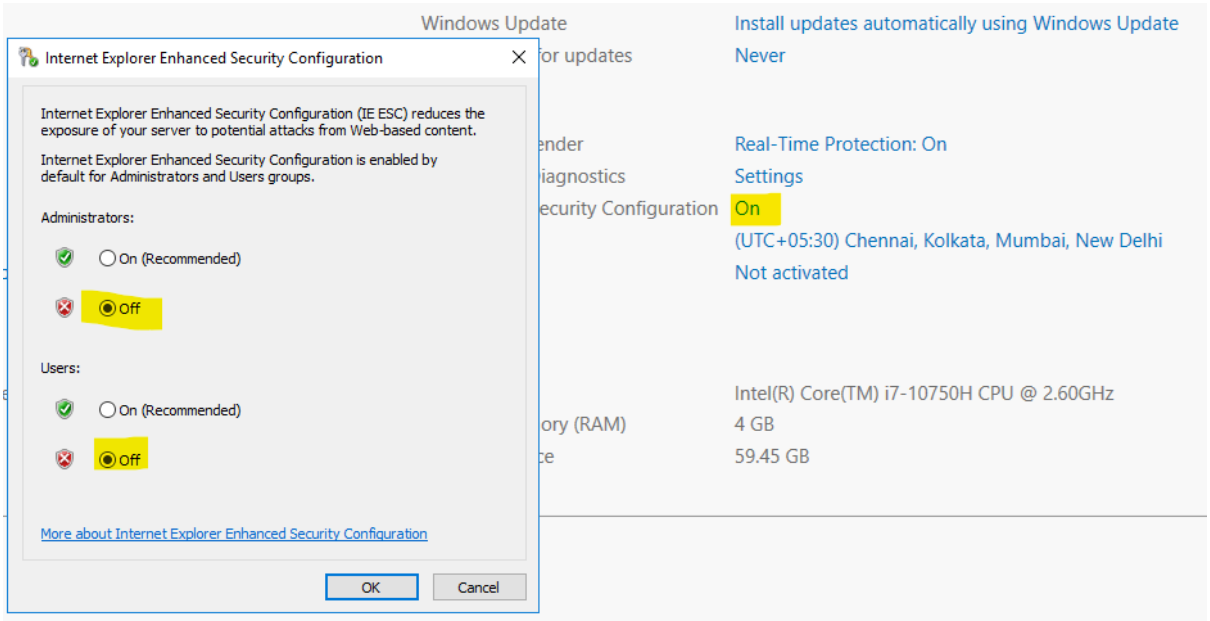
To change the data & Time zone:



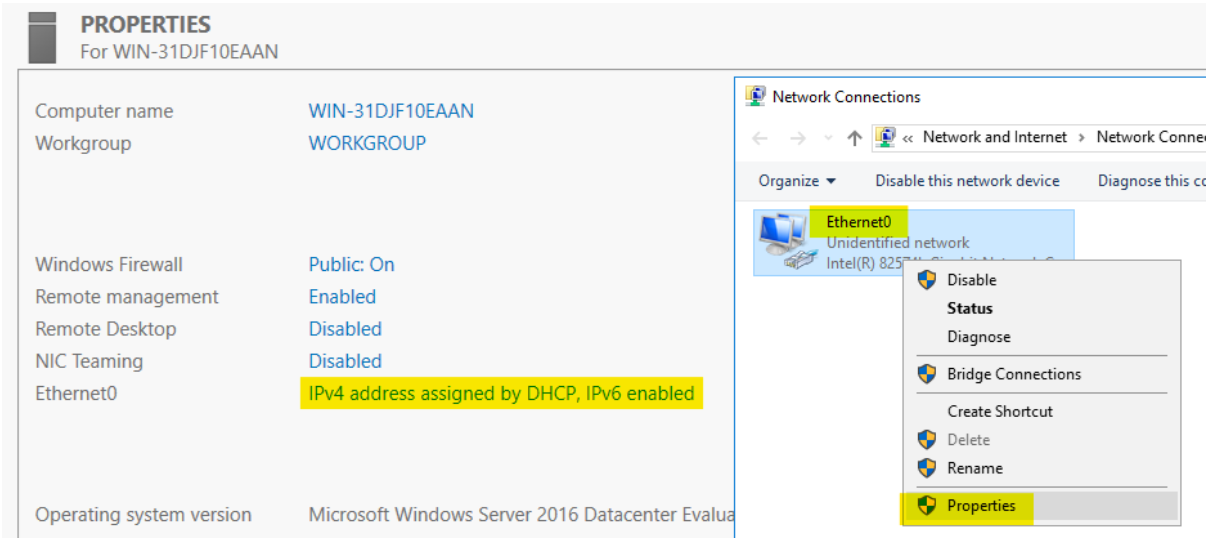
1. Click (UTC -08:00) Pacific time (US & Canada)
2. Click “Change Time zone…”
3. Select the time zone according to your location.

And refresh (right-top corner) after every change on this server manager.

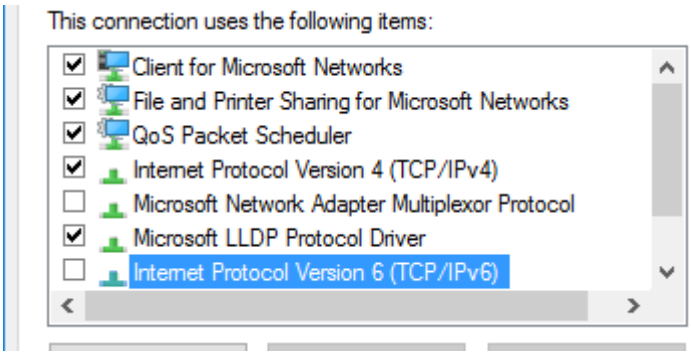
Turn off "IE Enhanced security configuration" to OFF (in case you want to work with web browser)



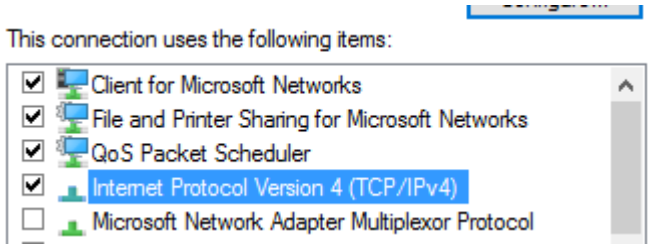
To change IP address, Click on the "Ethernet0" and right-click → properties



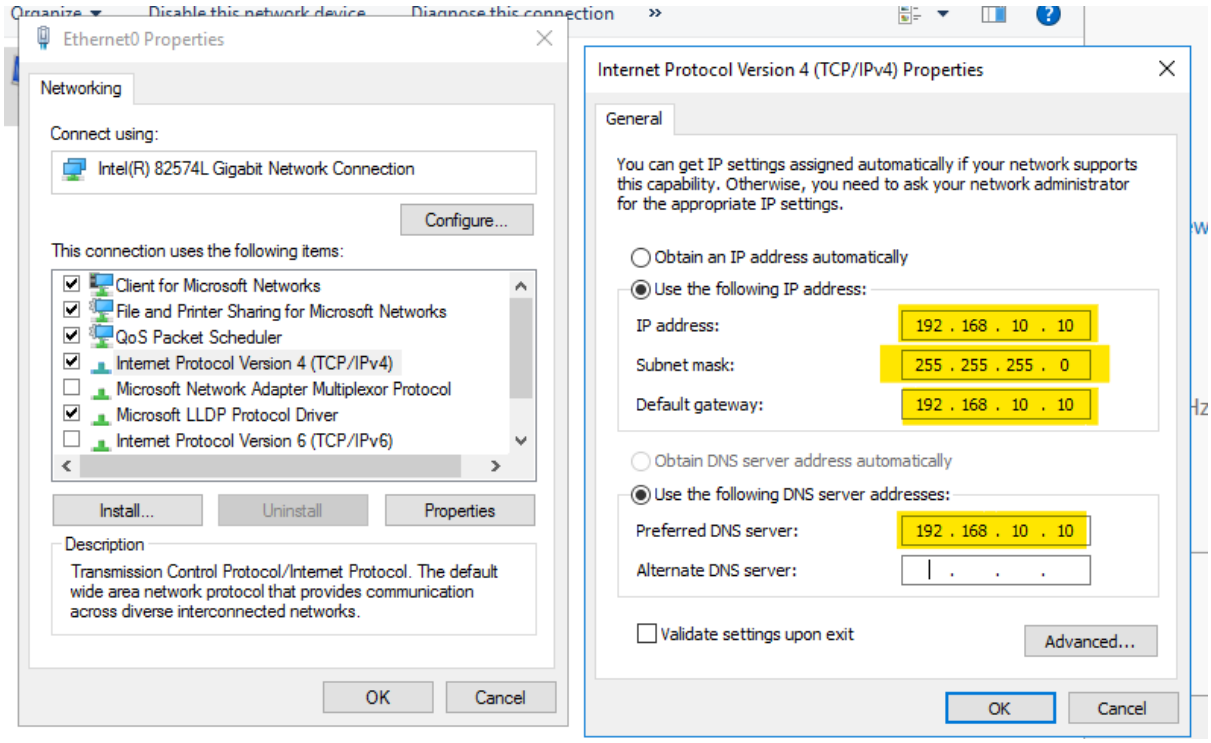
Uncheck, Internet Protocol Version 6 (TCP/IPv6):



Double click on “Internet Protocol Version 4”

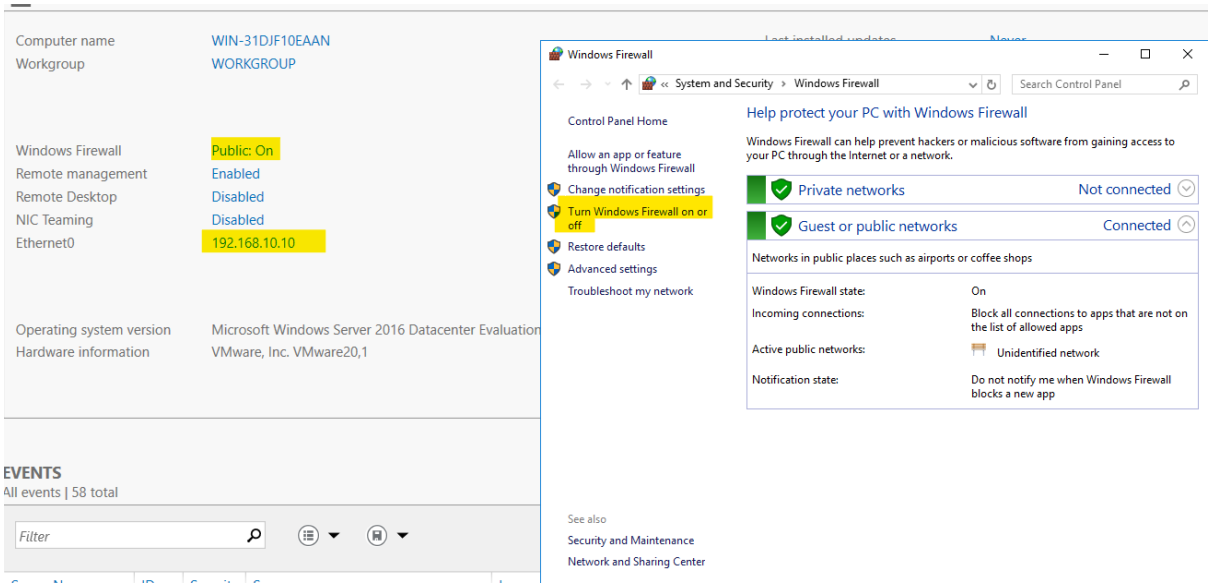


Fill the values accordingly:

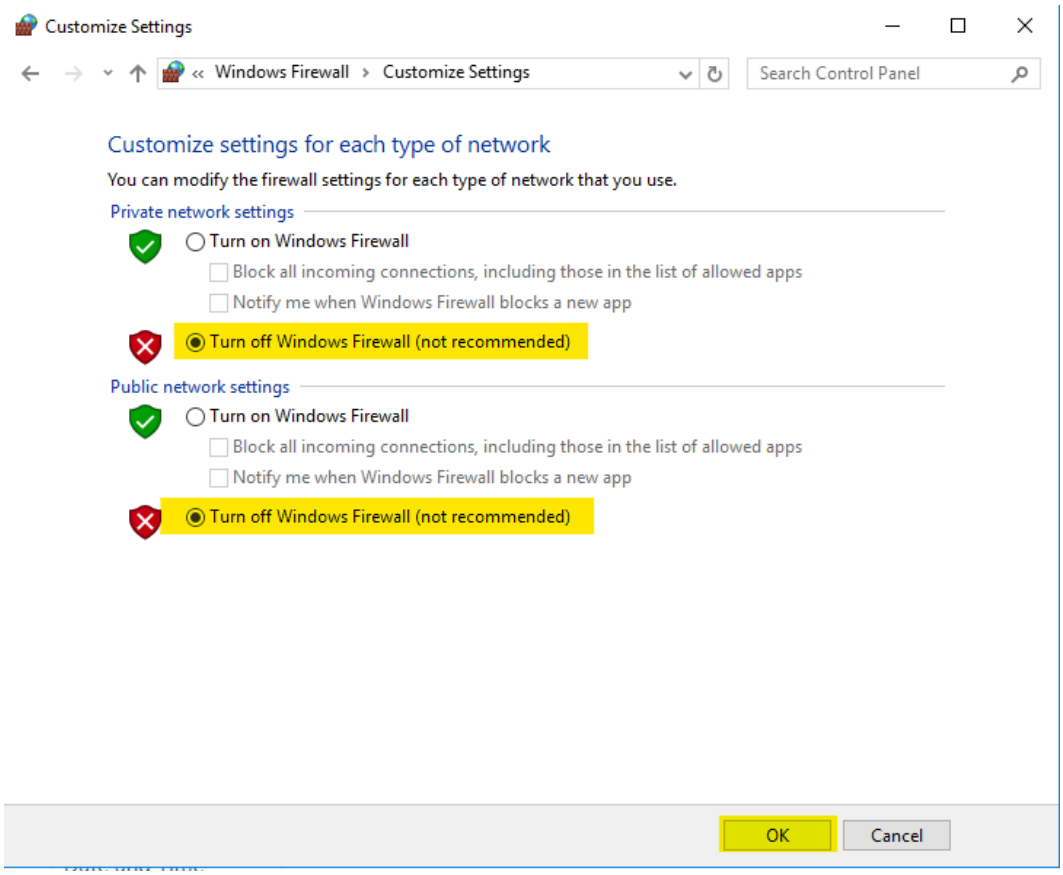


Click Ok → OK & then refresh

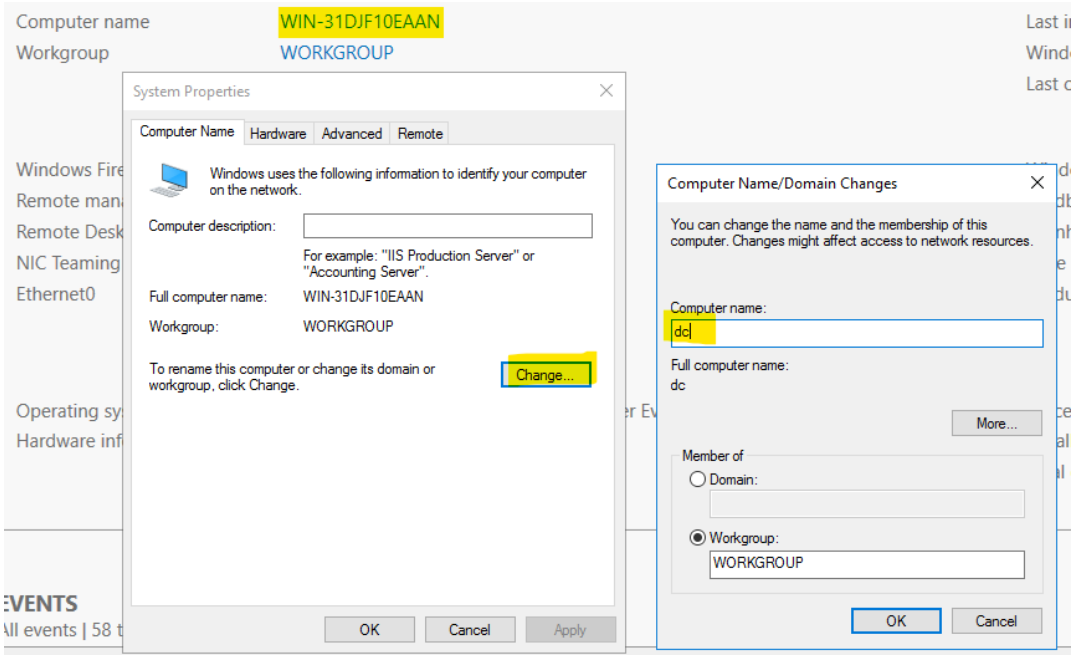
Click on Firewall → click on “Tuen Windows Firewall on or off”



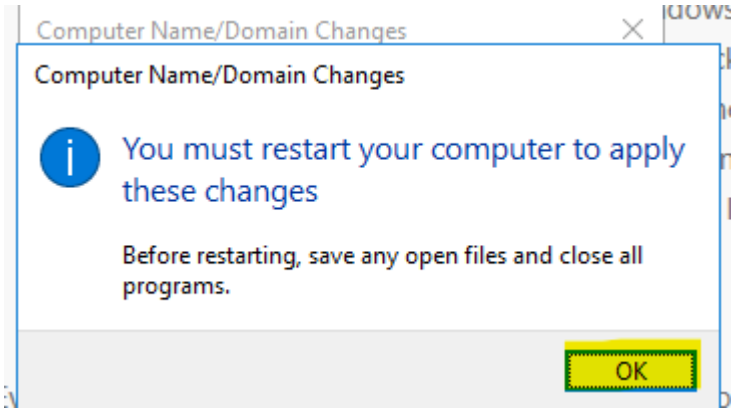
Tuen off firewall & then OK



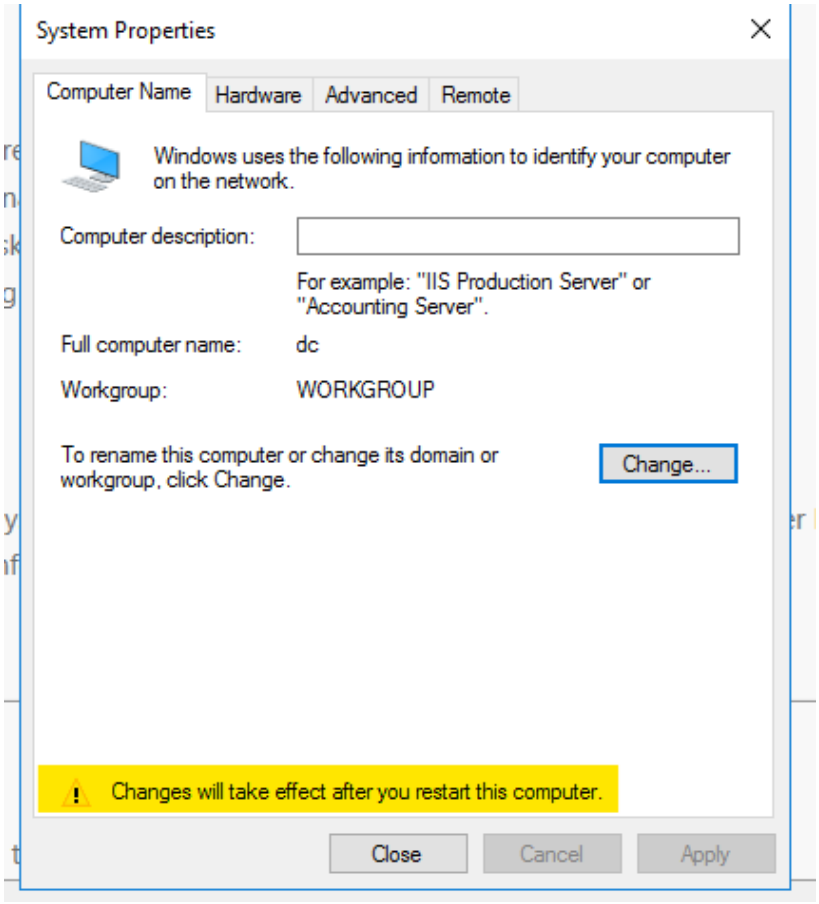
To change computer name:



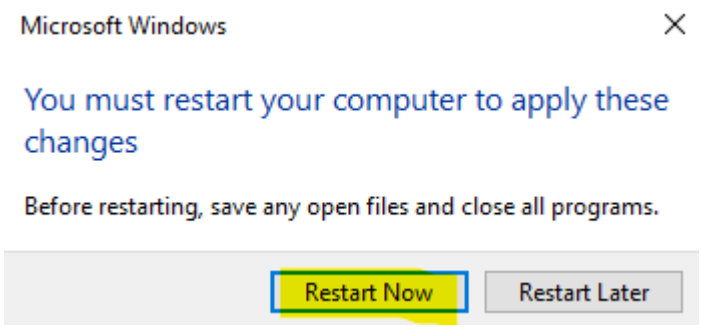
Click ok



& restart:

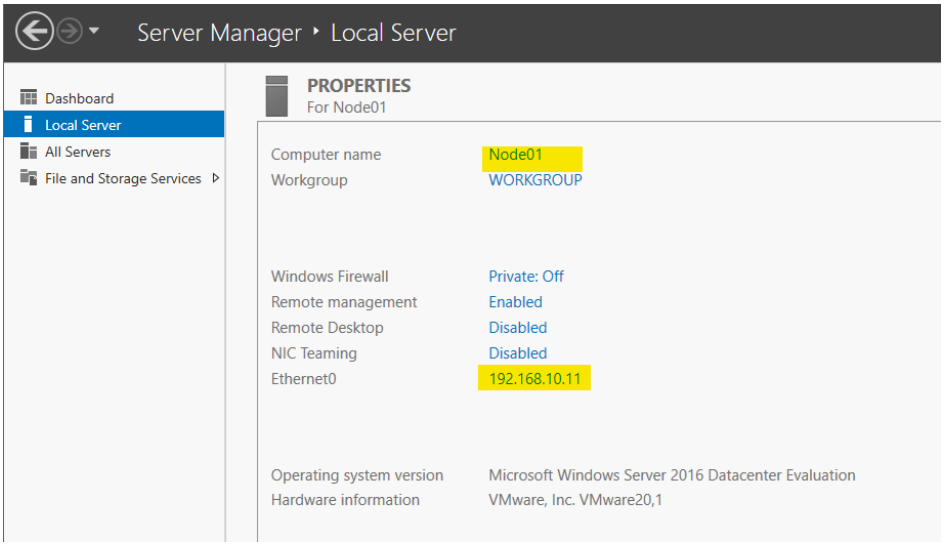


Click on “restart now”

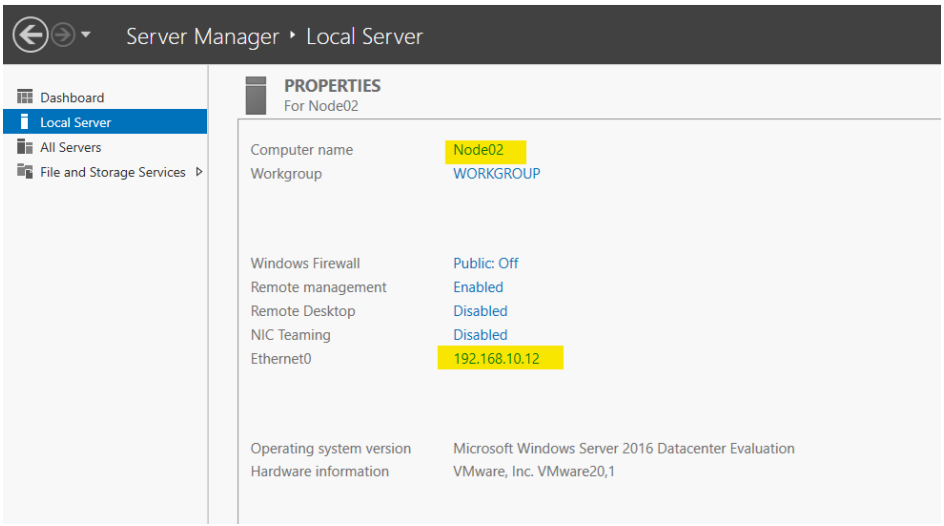


Similarly, create 2 more virtual machines

1. Node01
    a. IP address: 192.168.10.11
    b. Subnet Mask: 255.255.255.0
    c. Default gateway: 192.168.10.10
    d. DNS: 192.168.10.10



2. Node02
    a. IP address: 192.168.10.12
    b. Subnet Mask: 255.255.255.0
    c. Default gateway: 192.168.10.10
    d. DNS: 192.168.10.10



Note – ping Node01 & Node02 to DC machine

What is Windows Active Directory (AD)?

Active Directory (AD) is a directory service developed by Microsoft for Windows domain networks. It is used to manage and organize network resources such as users, computers, groups, and services in a centralized, secure, and scalable way.

AD provides a structured data store for information about objects in a network and enables administrators to manage permissions and access to network resources.

Core Components of Active Directory

1. Domain

- A logical group of network objects (users, computers, devices).
- Domains define a security boundary.
- Each domain stores its data in a **Domain Controller (DC)**.

2. Domain Controller (DC)

- A server running Windows Server with Active Directory Domain Services (AD DS) installed.
- Hosts a writable copy of the AD database.
- Authenticates and authorizes users and computers.

3. Forest

- The top-level container in an AD network.
- One or more domains grouped together sharing a common schema, configuration, and global catalog.
- Represents the security boundary for the entire organization.

4. Tree

- A hierarchical collection of domains within a forest.
- Domains in a tree share a contiguous namespace.

5. Organizational Units (OUs)

- Containers within domains used to organize objects into logical administrative groups.
- Facilitate delegation of administration and application of Group Policies.

6. Global Catalog

- A distributed data repository containing a partial replica of every object in the forest.
- Enables users to find objects across all domains.

7. Schema

- Defines the types of objects and attributes stored in AD.
- Controls the structure and rules for objects in the directory.

Key Features of Active Directory

1. Centralized Management

- Allows admins to manage users, computers, groups, and policies from a single console.

2. Authentication and Authorization

- Provides user logon authentication (Kerberos, NTLM).
- Controls access to resources via permissions and Group Policies.

3. Replication

- Data is replicated between DCs to ensure consistency and fault tolerance.

4. Group Policy

- Centralized management tool to enforce security settings and configure computers/users in the domain.

5. Trust Relationships

- Establishes trust between domains and forests to allow resource sharing.

6. Scalability

- Supports millions of objects and multiple domains in complex hierarchical structures.

Active Directory Logical Structure

Level	Description
Forest	Collection of one or more domain trees
Tree	Collection of one or more domains sharing namespace
Domain	Core administrative unit
Organizational Unit (OU)	Subdivision within domains for management
Objects	Users, computers, groups, printers, etc.

Active Directory Physical Structure

- **Sites:** Represent the physical structure, usually mapped to network locations or subnets.
- **Domain Controllers:** Servers hosting AD database replicas.
- **Replication topology:** Defines how data replicates between DCs/sites.

Common Active Directory Services

1. Active Directory Domain Services (AD DS)

- Core service for directory management, authentication, and authorization.

2. Active Directory Certificate Services (AD CS)

- Provides Public Key Infrastructure (PKI) for issuing and managing digital certificates.

3. Active Directory Federation Services (AD FS)

- Enables single sign-on (SSO) and federated identity management across organizational boundaries.

4. Active Directory Lightweight Directory Services (AD LDS)

- Lightweight directory service for applications requiring directory-enabled services without a full domain.

Tools to Manage Active Directory

- Active Directory Users and Computers (ADUC)
- Active Directory Sites and Services
- Group Policy Management Console (GPMC)
- Active Directory Administrative Center (ADAC)
- PowerShell (Active Directory module)
- Repadmin and DCDiag (for troubleshooting replication and DC health)

Summary of Benefits

Benefit	**Description**
Centralized control	Manage users and resources from one place
Scalability	Supports large organizations
Security	Kerberos authentication, group policies
Fault tolerance	Multi-master replication and multiple DCs
Delegation	Granular admin delegation via OUs
Integration	Works with Microsoft services and many apps

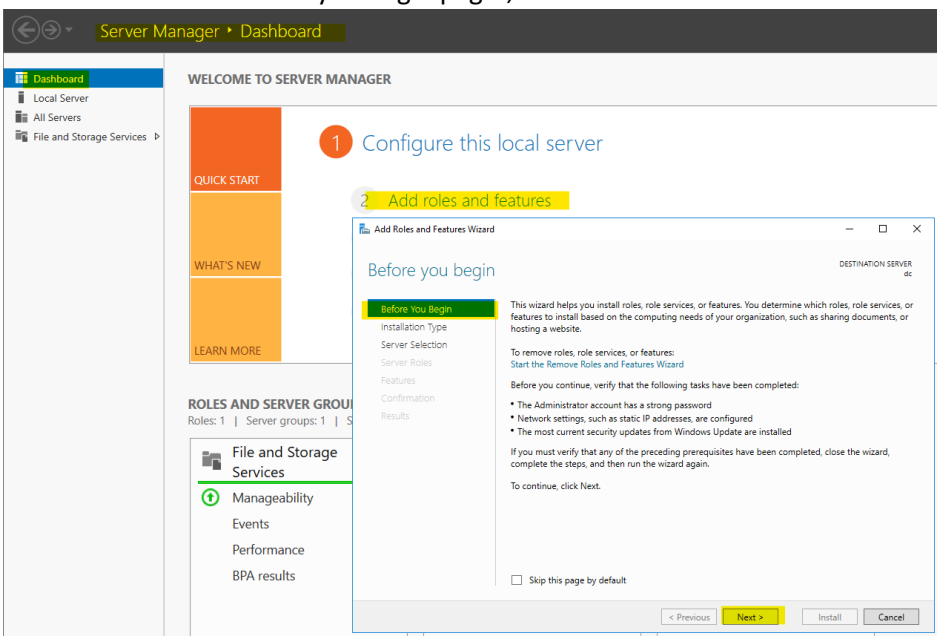
Creating a domain controller (DC) on DC machine

Installing ADDS (Active Directory Domain Services) on Domain Controller, using:

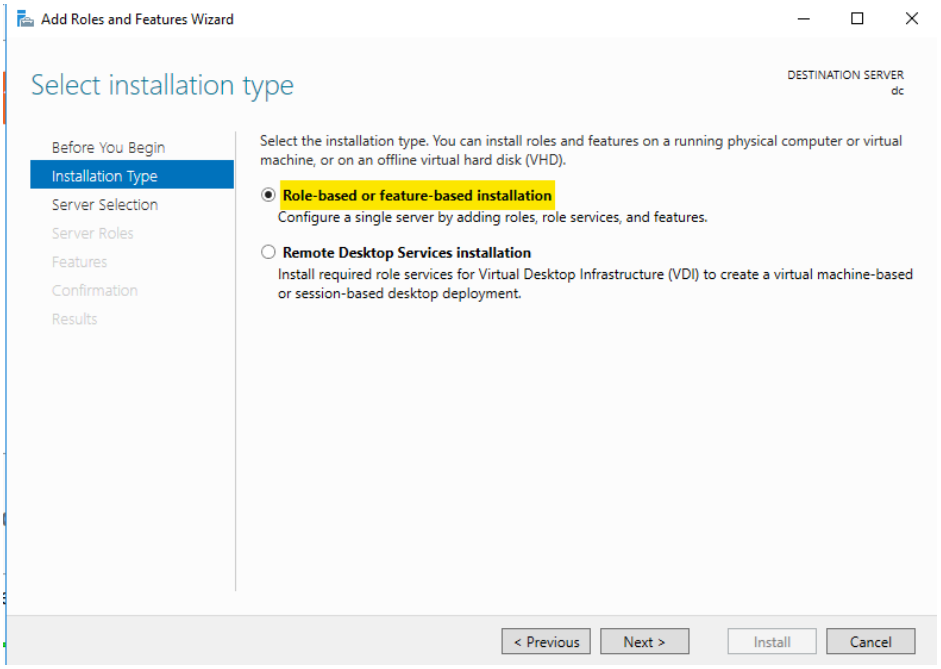
1. PowerShell cmdlet

```
Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools -Restart
```

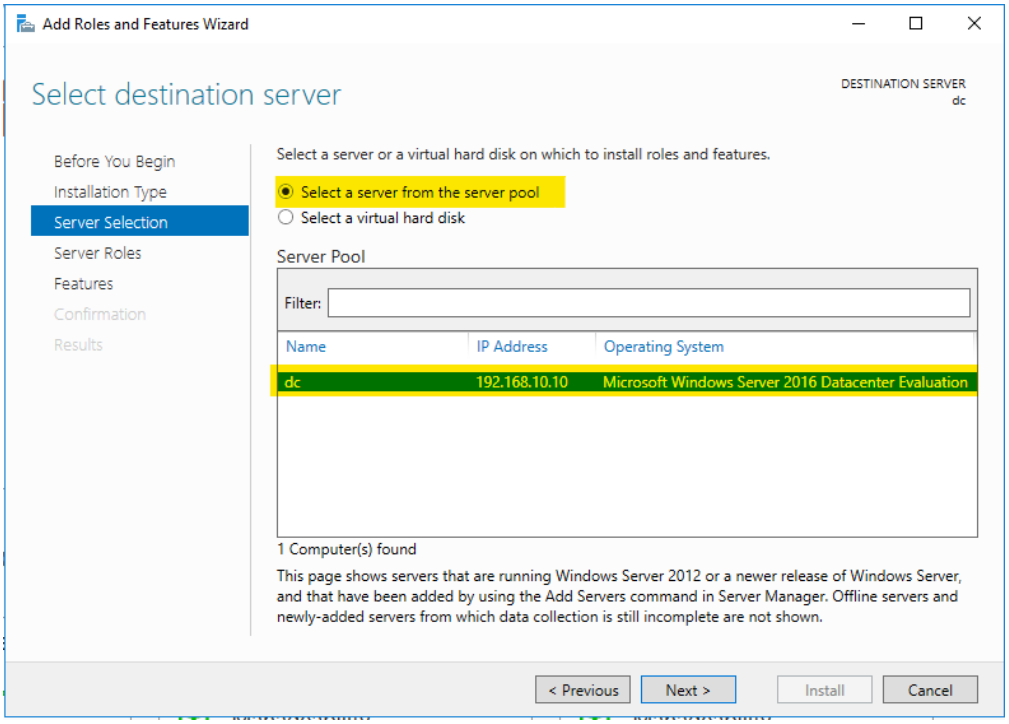
2. Server Manager dashboard page
   - Click on “Next” in “Before you begin page”,



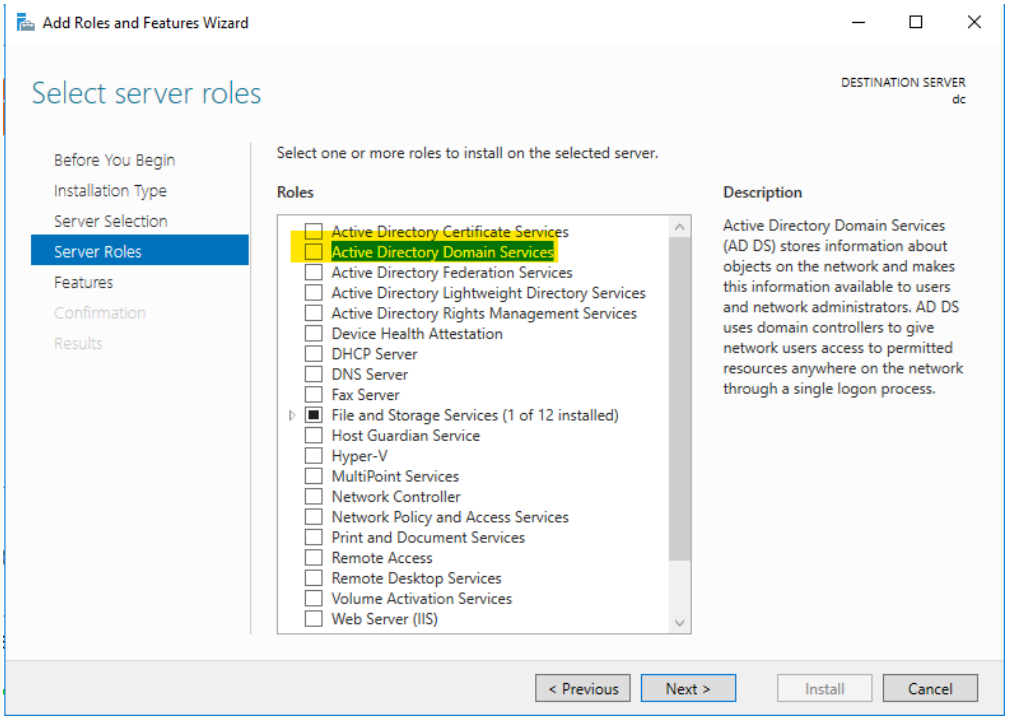
   - Select the installation type as “Role-base or Feature-based installation” & then click Next.



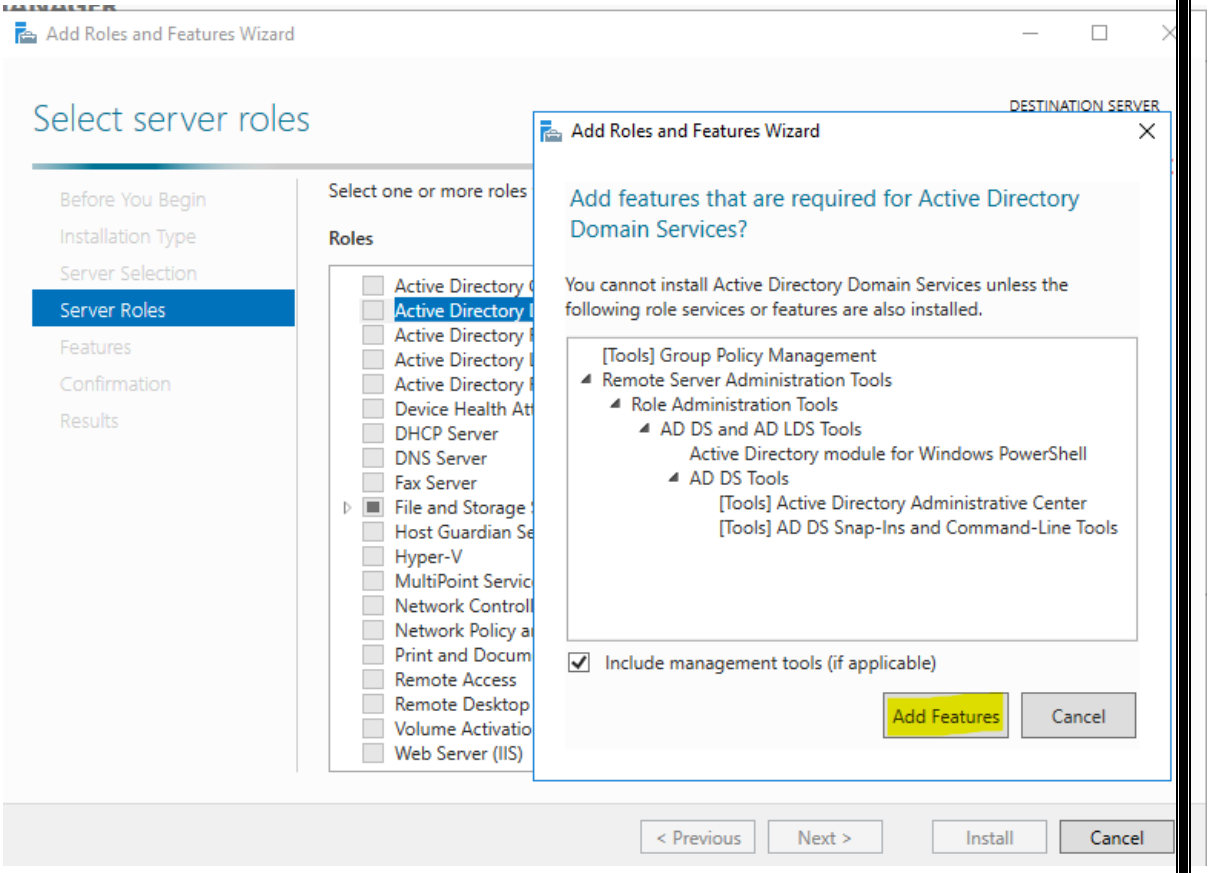
- Select a server from the server pool & verify the IP address.



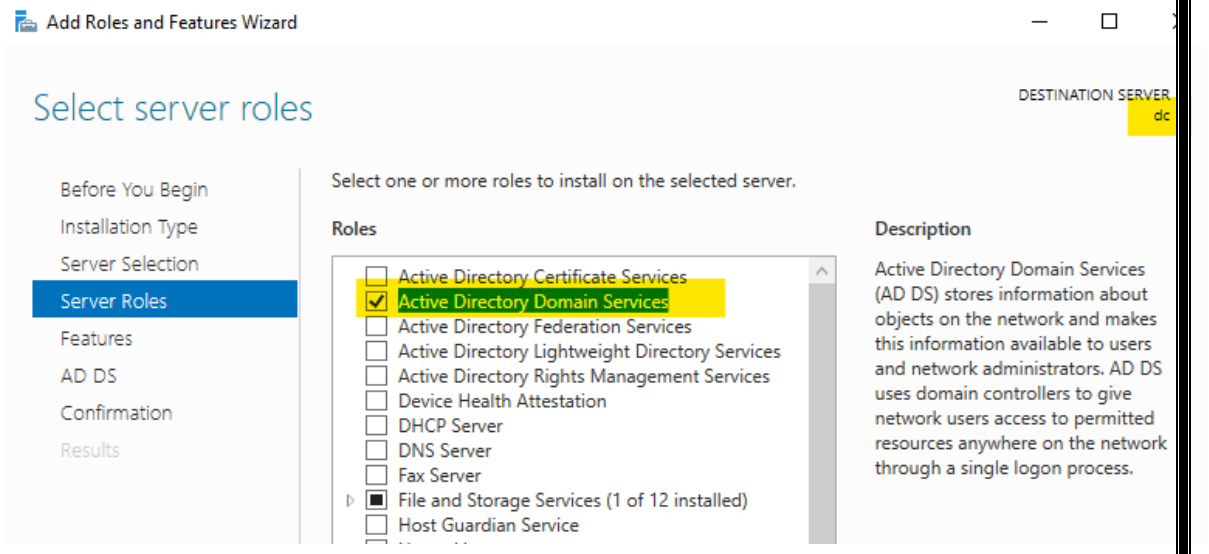
- Select appropriate role from the list:



- Click on “Add features”

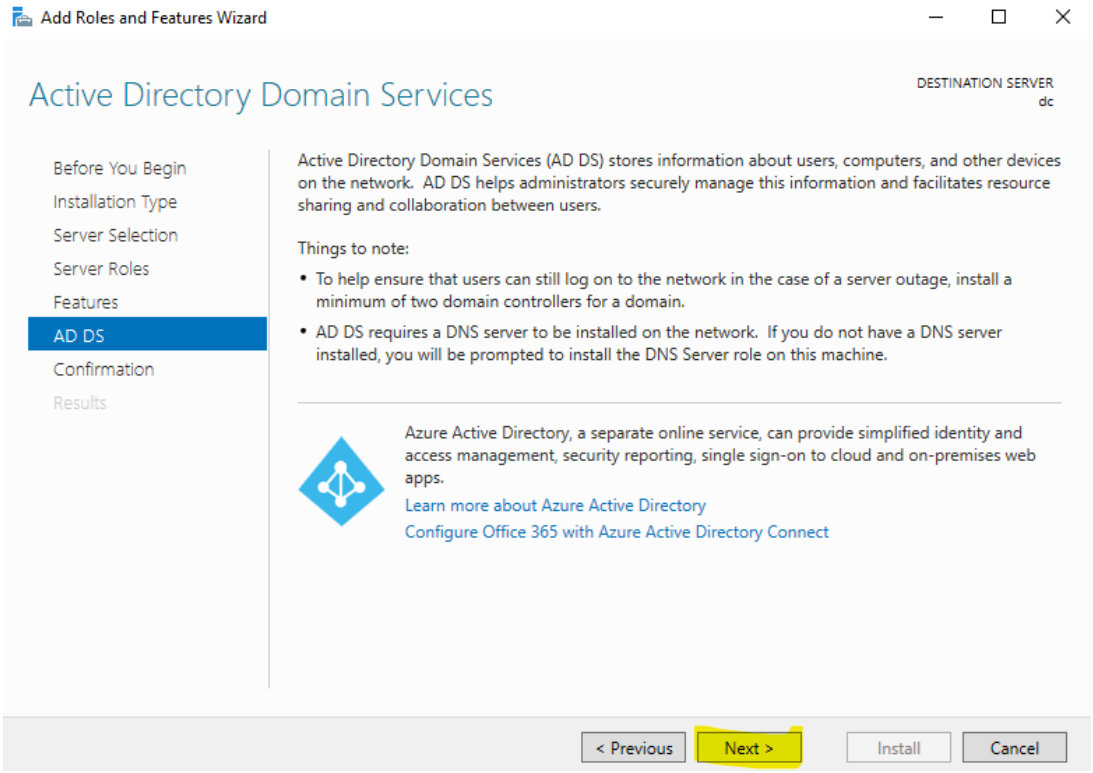


- Verify:

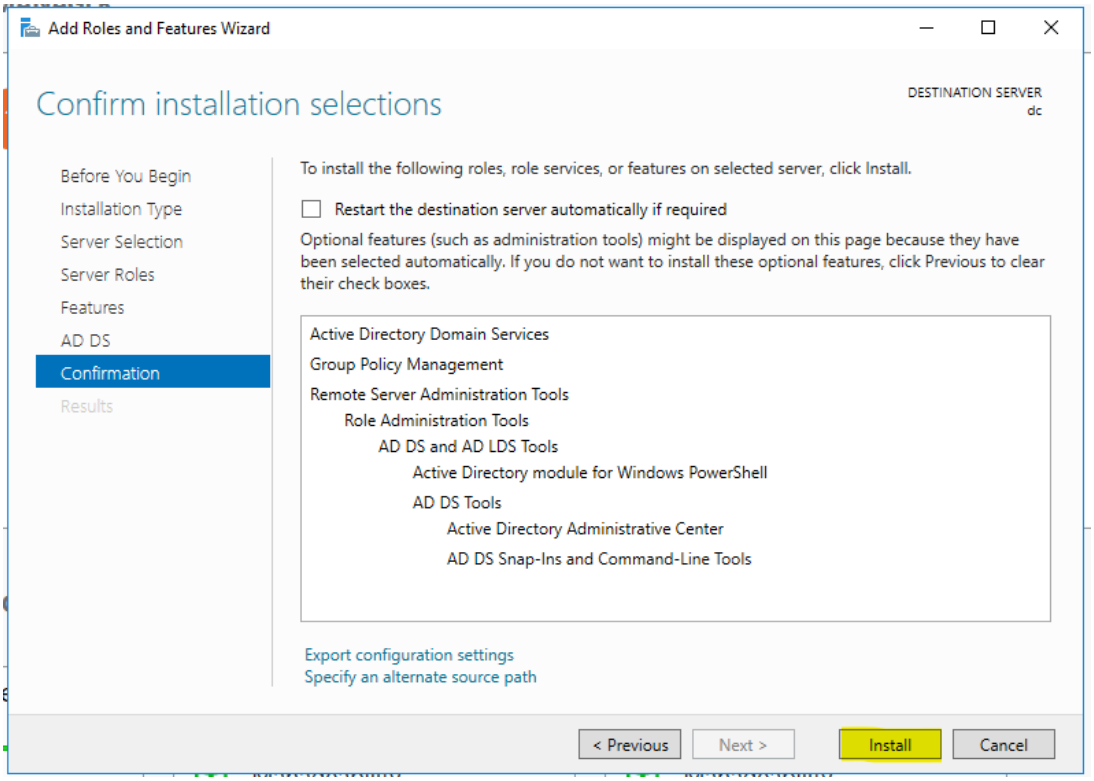


- Click on Next
- Nothing to select on “features” page, then click on Next.

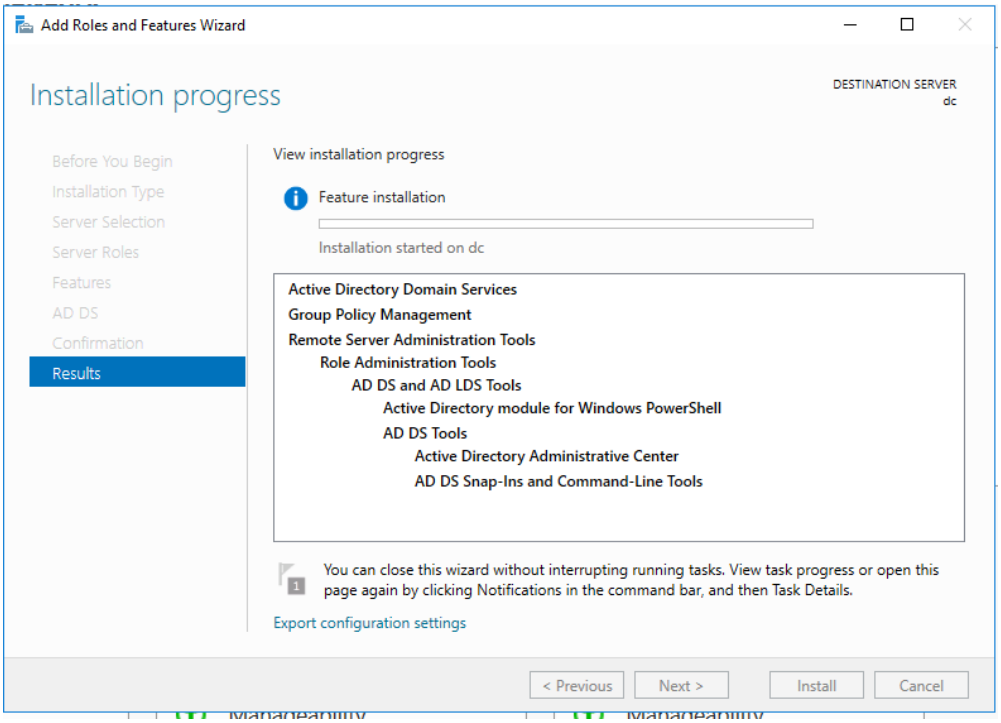
- Nothing to select on Active Directory Domain Services Page, click Next.



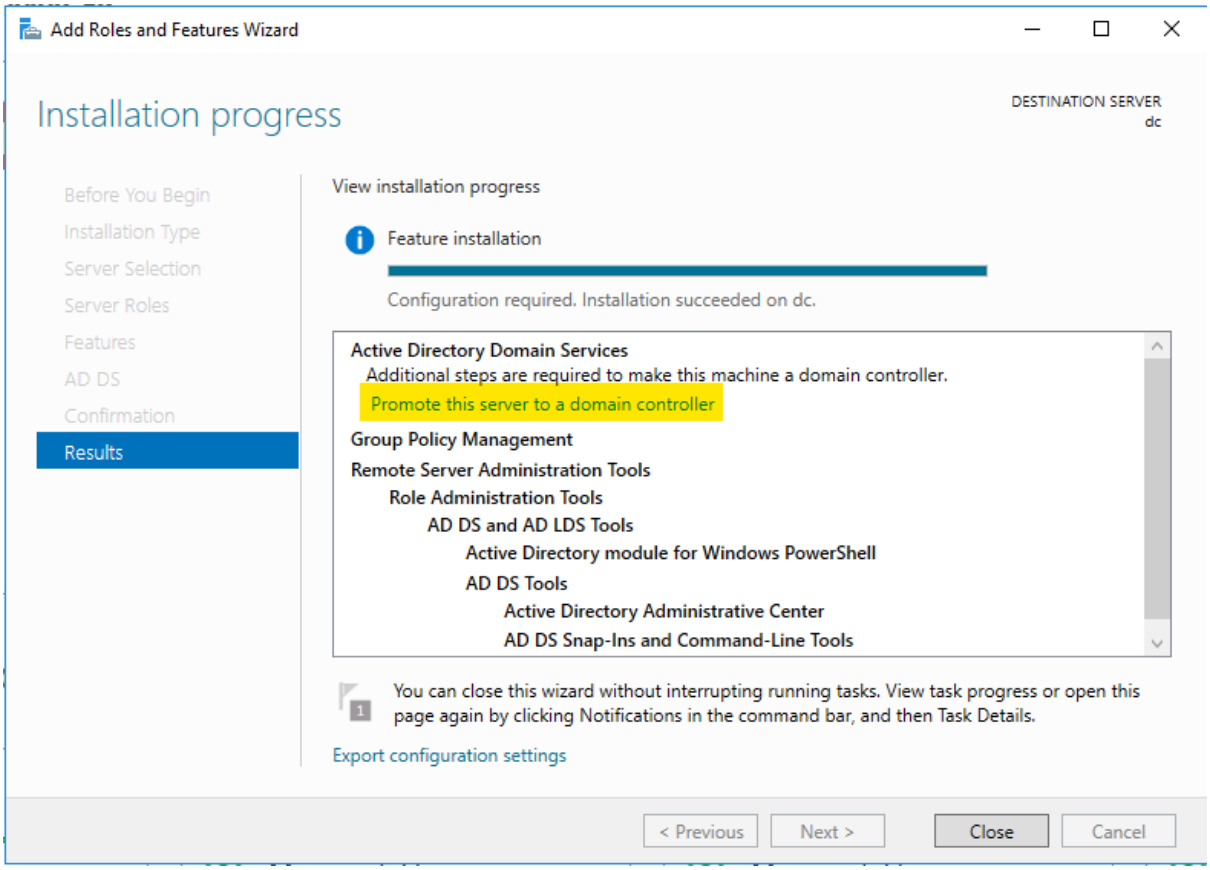
- During the installation of ADDS role, reboot/restart isn't needed so leave it untick and click on "Install" button.



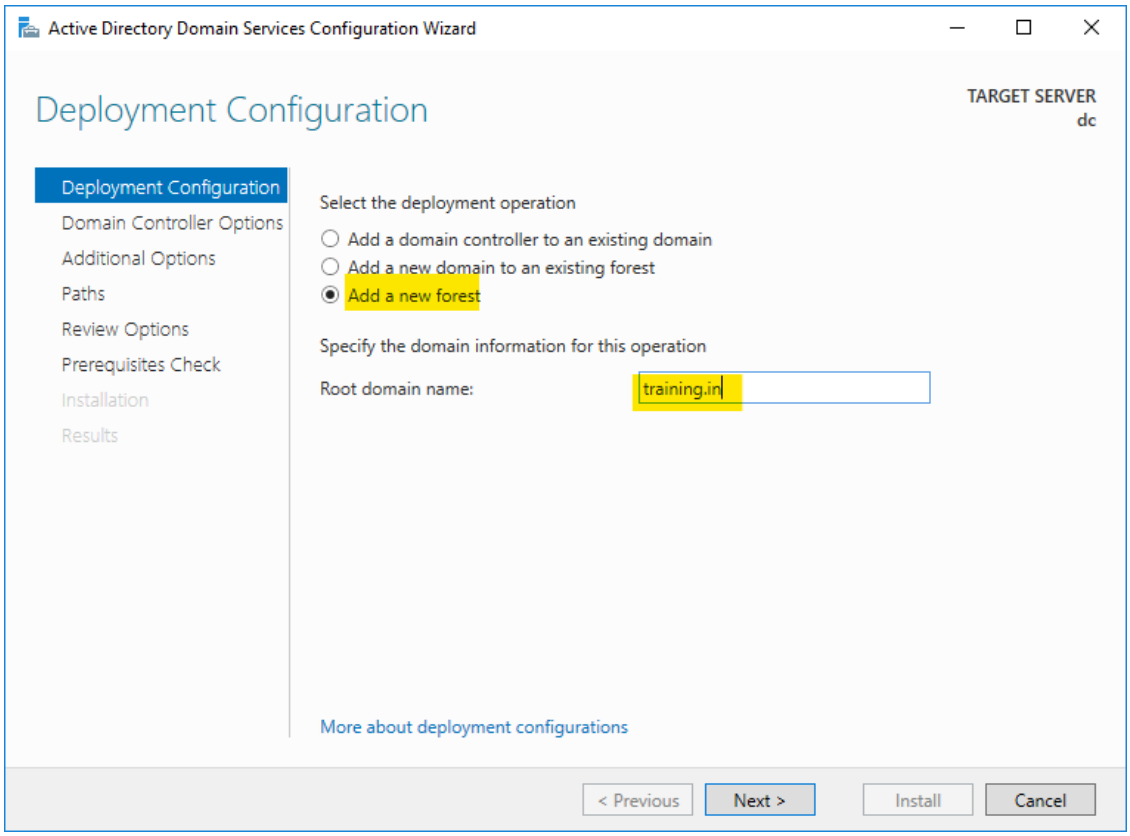
- Wait until role installation is over.



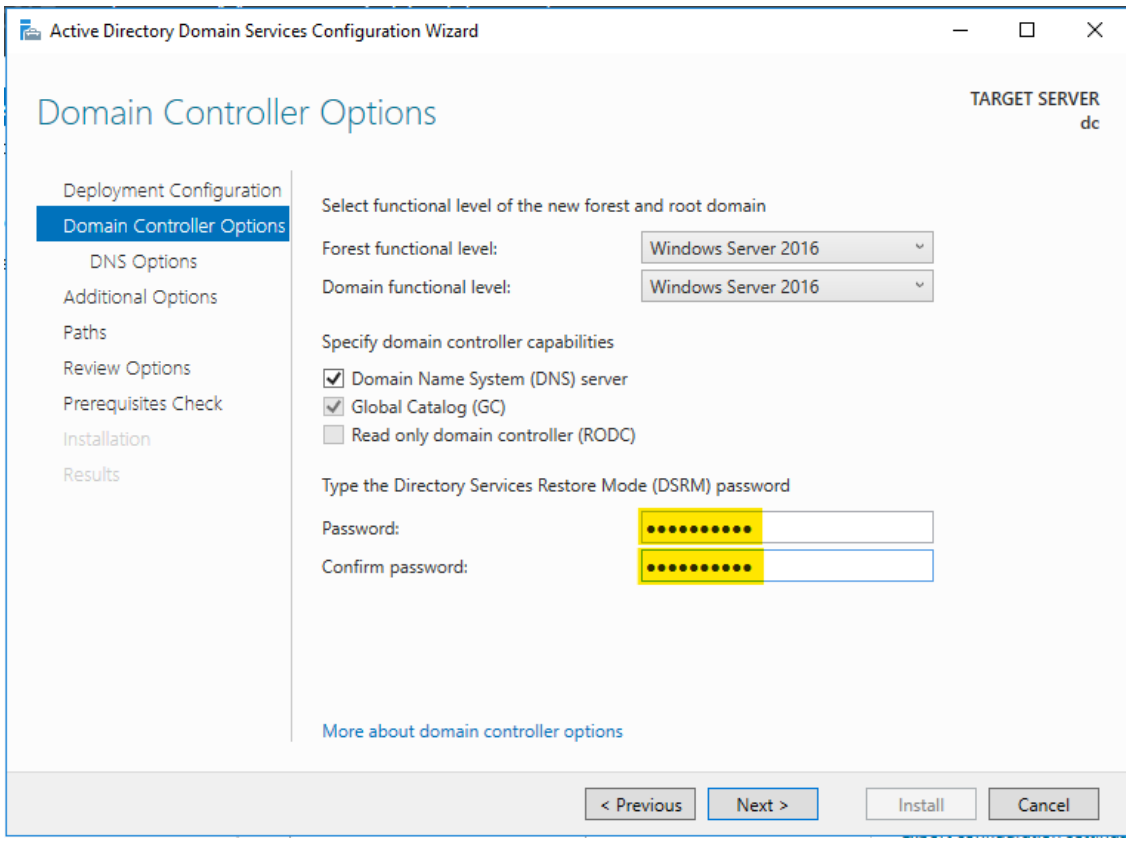
Promote this machine to domain controller.



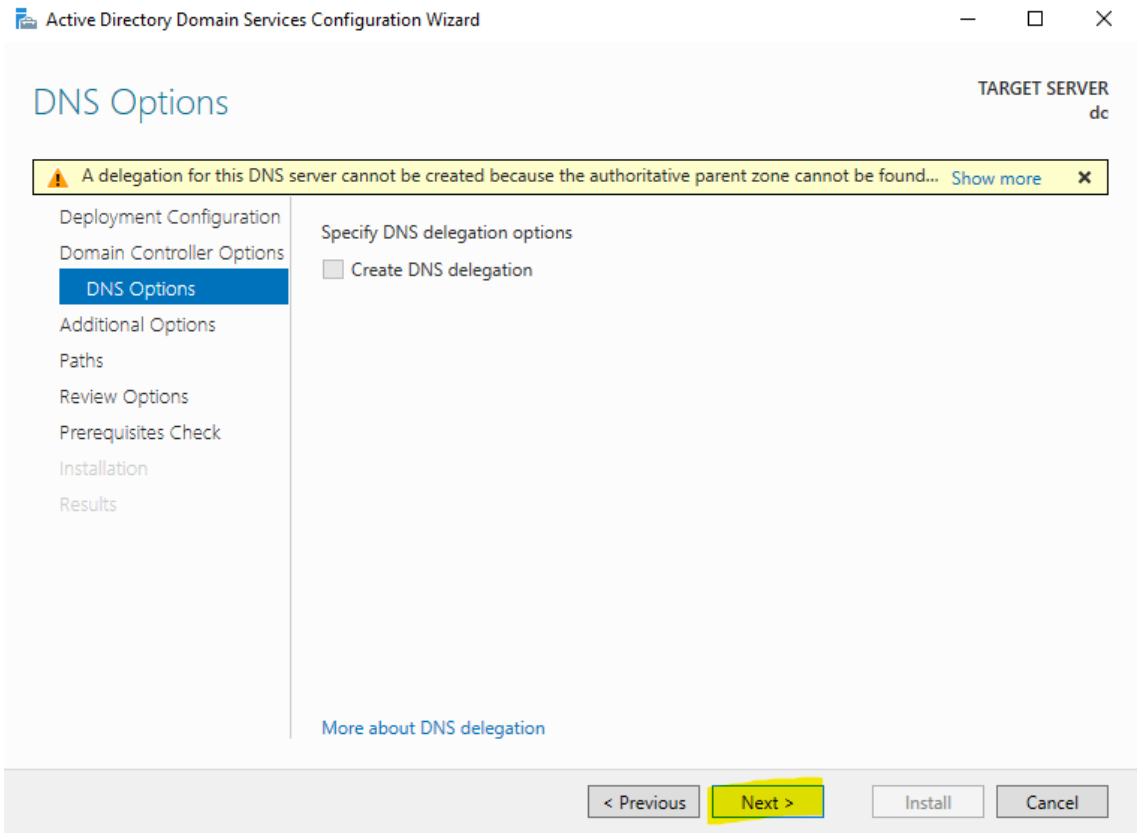
Under deployment configuration, select “Add a new forest” and type a domain/forest name.



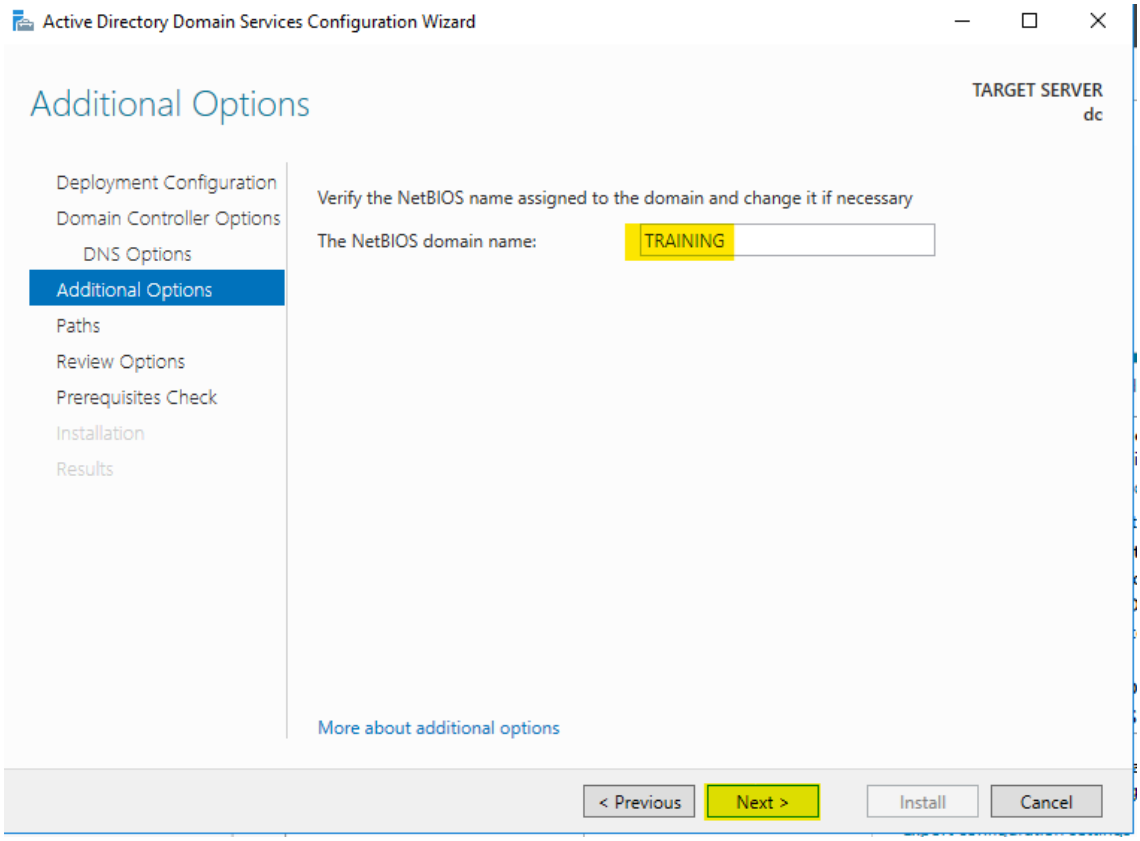
Type DSRM password (click here to know more about DSRM),



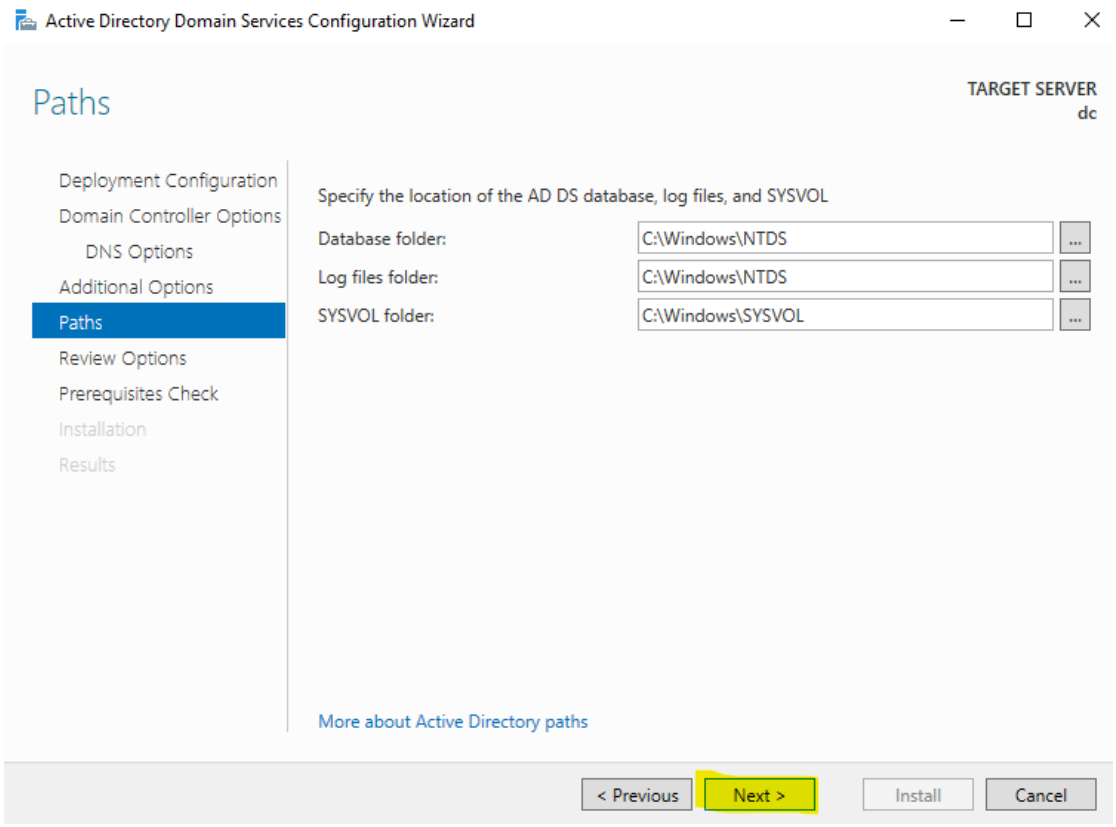
Under DNS Option, warning is expected as there are no additional DNS servers present.



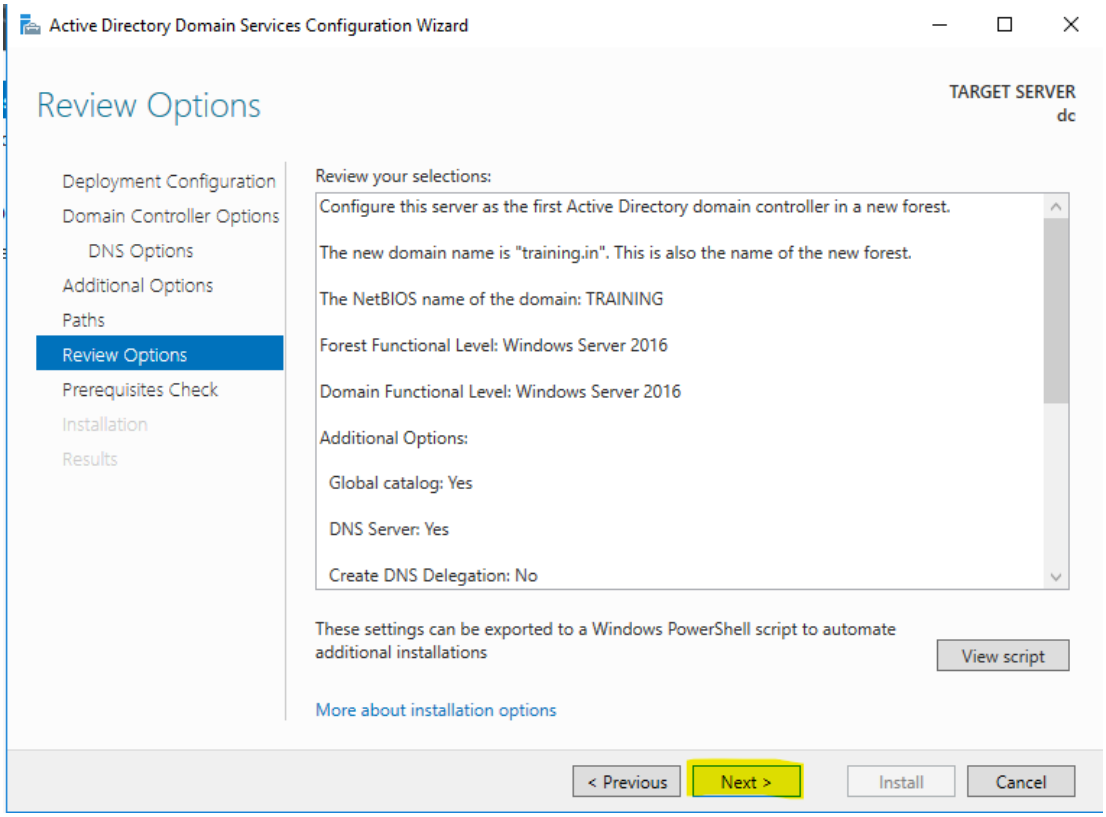
Verify NetBIOS name and click next



Leave default path as it is, and click on Next:

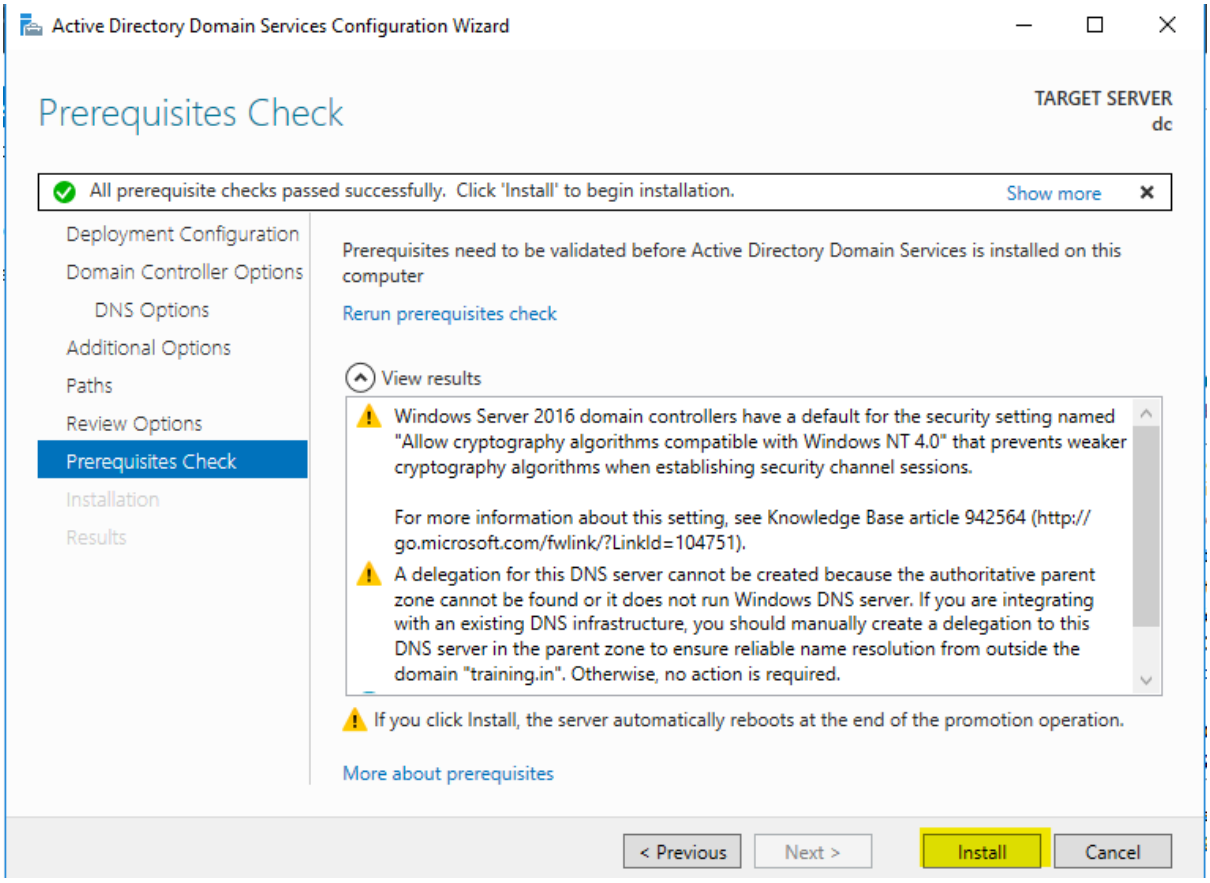


Verify the details and click on Next.



Powershell script to achieve the same.
Import-Module ADDSDeployment Install-ADDSForest ` -CreateDnsDelegation:$false ` -DatabasePath "C:\Windows\NTDS" ` -DomainMode "WinThreshold" ` -DomainName "training.in" ` -DomainNetbiosName "TRAINING" ` -ForestMode "WinThreshold" ` -InstallDns:$true ` -LogPath "C:\Windows\NTDS" ` -NoRebootOnCompletion:$false ` -SysvolPath "C:\Windows\SYSVOL" ` -Force:$true

After verifying, click on “Install”.

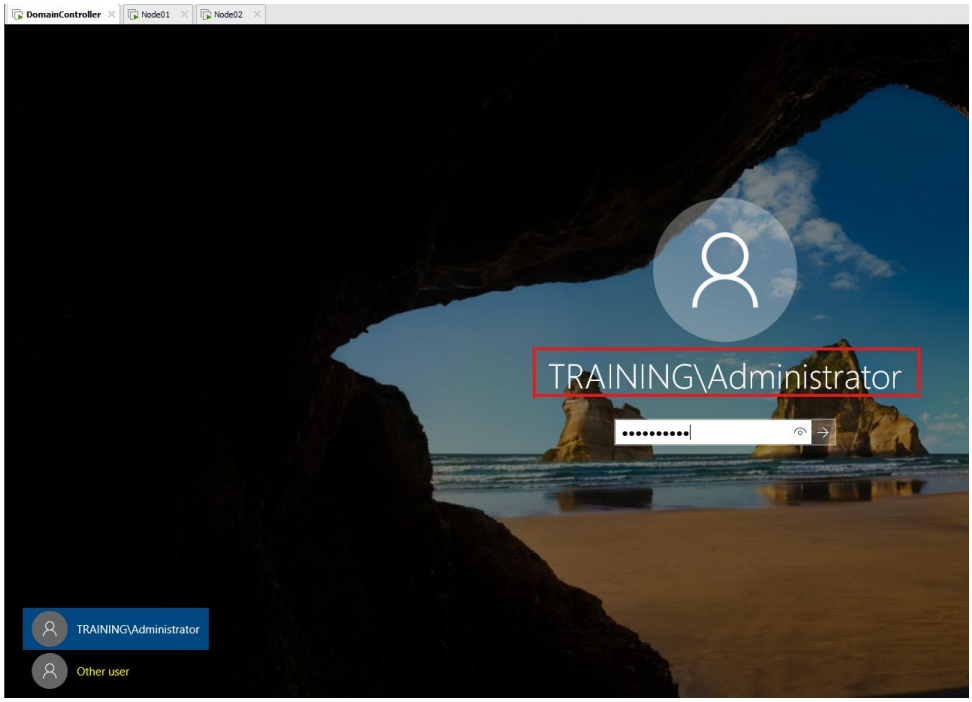


After successful installation, a reboot is expected. Once rebooted, login with domain administrator.

Domain administrator login

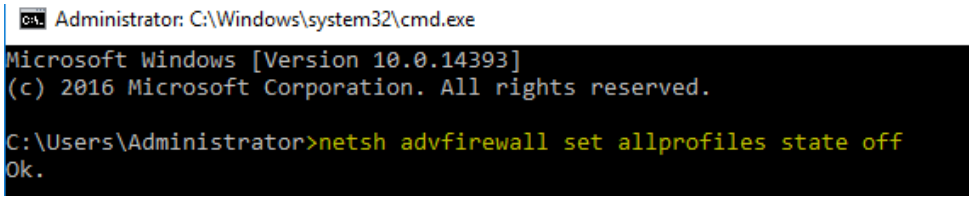
- Domain\Administrator → Training\Administrator
  OR
- Administrator@domain → Administrator@training.in

Login with domain administrator.



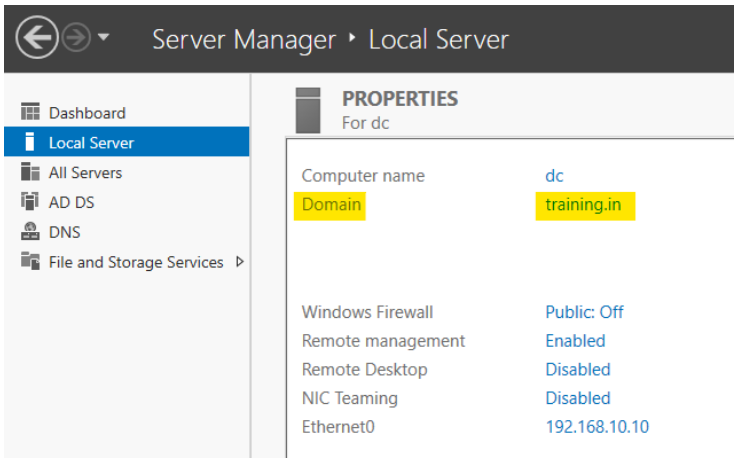
Note – if you see only Administrator, then click on "Other User" on left bottom corner and then login with domain\administrator.

Run the following command to disable domain firewall:



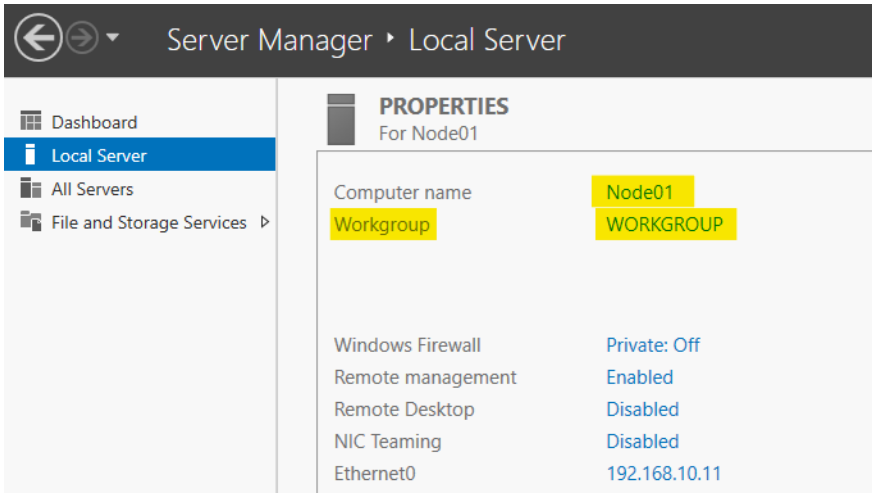
Cmd: netsh advfirewall set allprofiles state off

To find if the machine is a domain controller, go to server manager dashboard page →Local Server

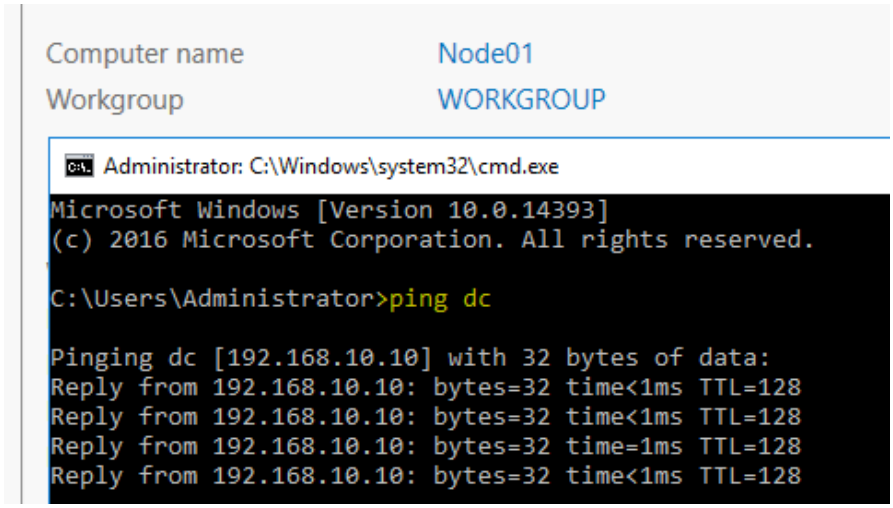


Domain joining Node01 to the domain controller (using the GUI)

Before domain joining



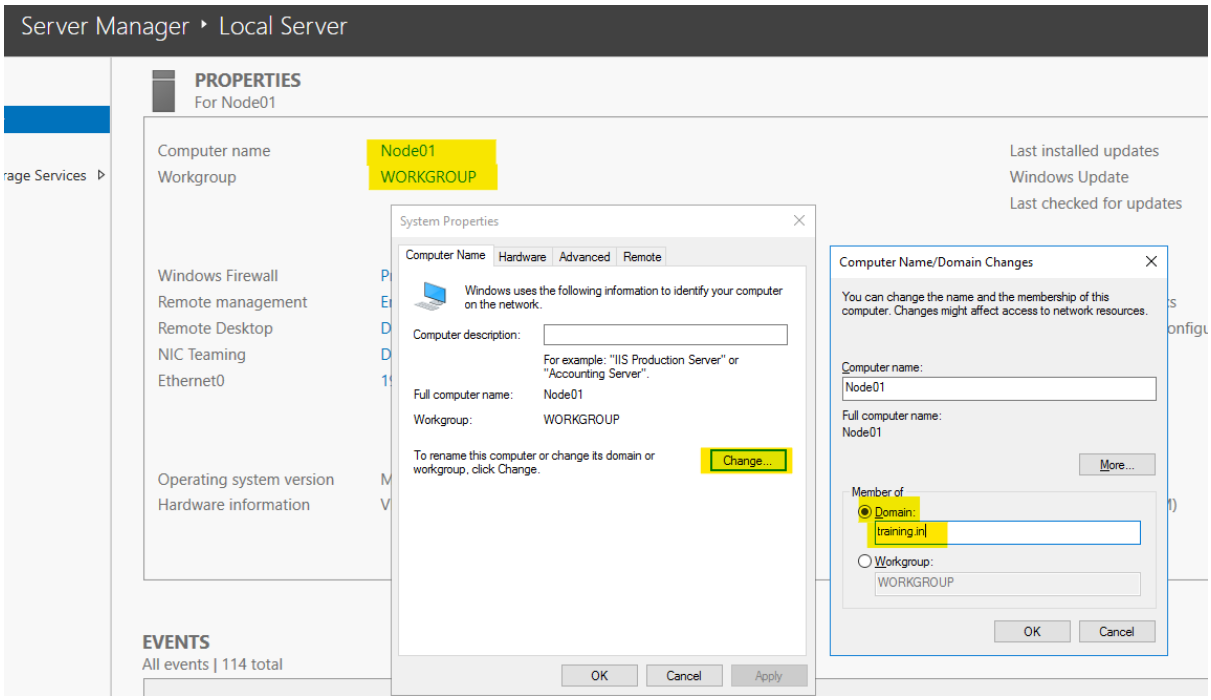
Ping the DC machine from Node01 using name:



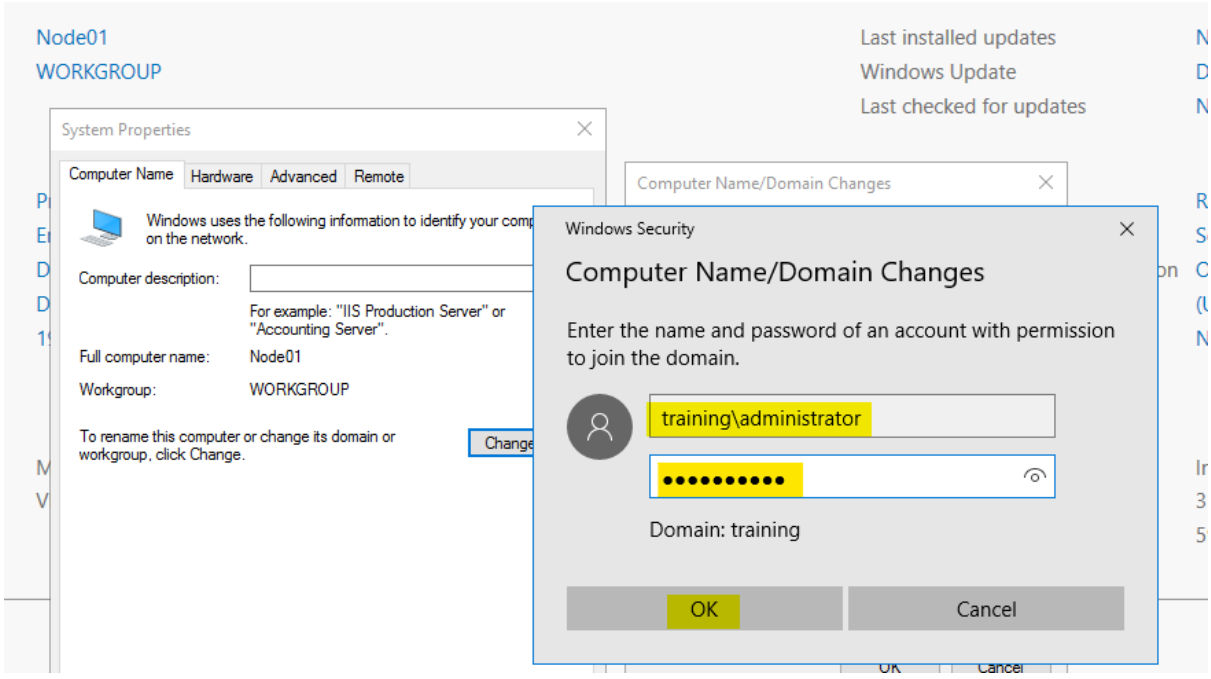
Note – if this fails, check the following:

- ✓ *Both DC and Node01 are in same Lan Segment (Windows Labs)*
- ✓ *On Node01, DNS is configured as DC IP address (192.168.10.10)*
- ✓ *DC machine is powered on (not power off state or suspended)*

After successful ping, go to Node01→ Dashboard page → Local server →click on workgroup → click on “Change” button → select “Member of”



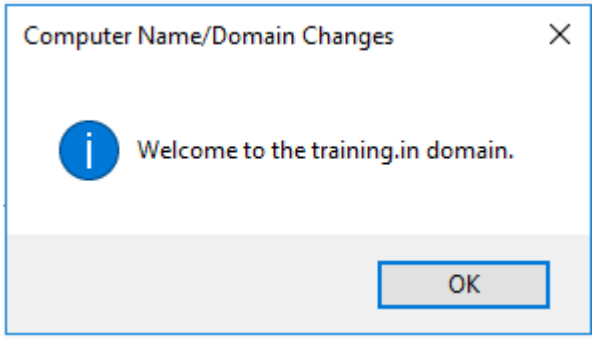
After clicking on “OK”, type domain administrator credentials username and password:

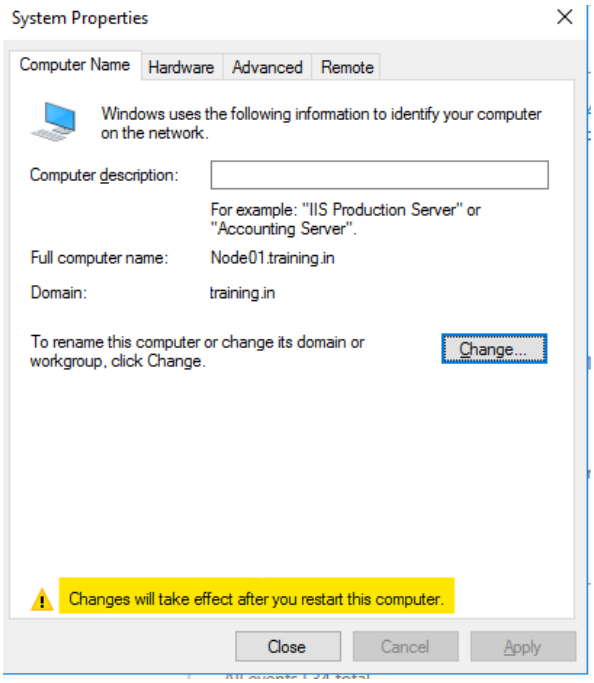


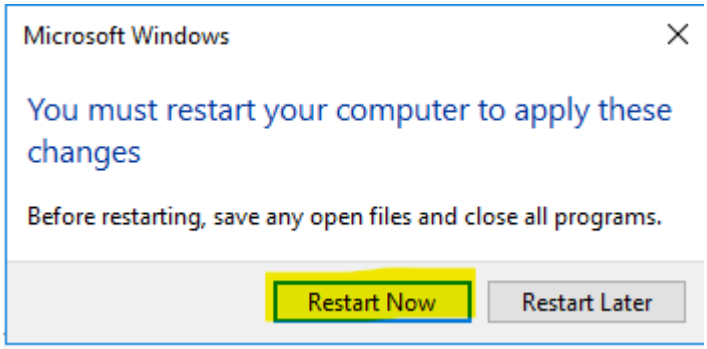
During this stage, if you get error related to “AD domain controller cannot be contact”. This is due to DNS IP address related issue. Please check

- ✓ Proper DNS is present in Node01
- ✓ DC is pingable.

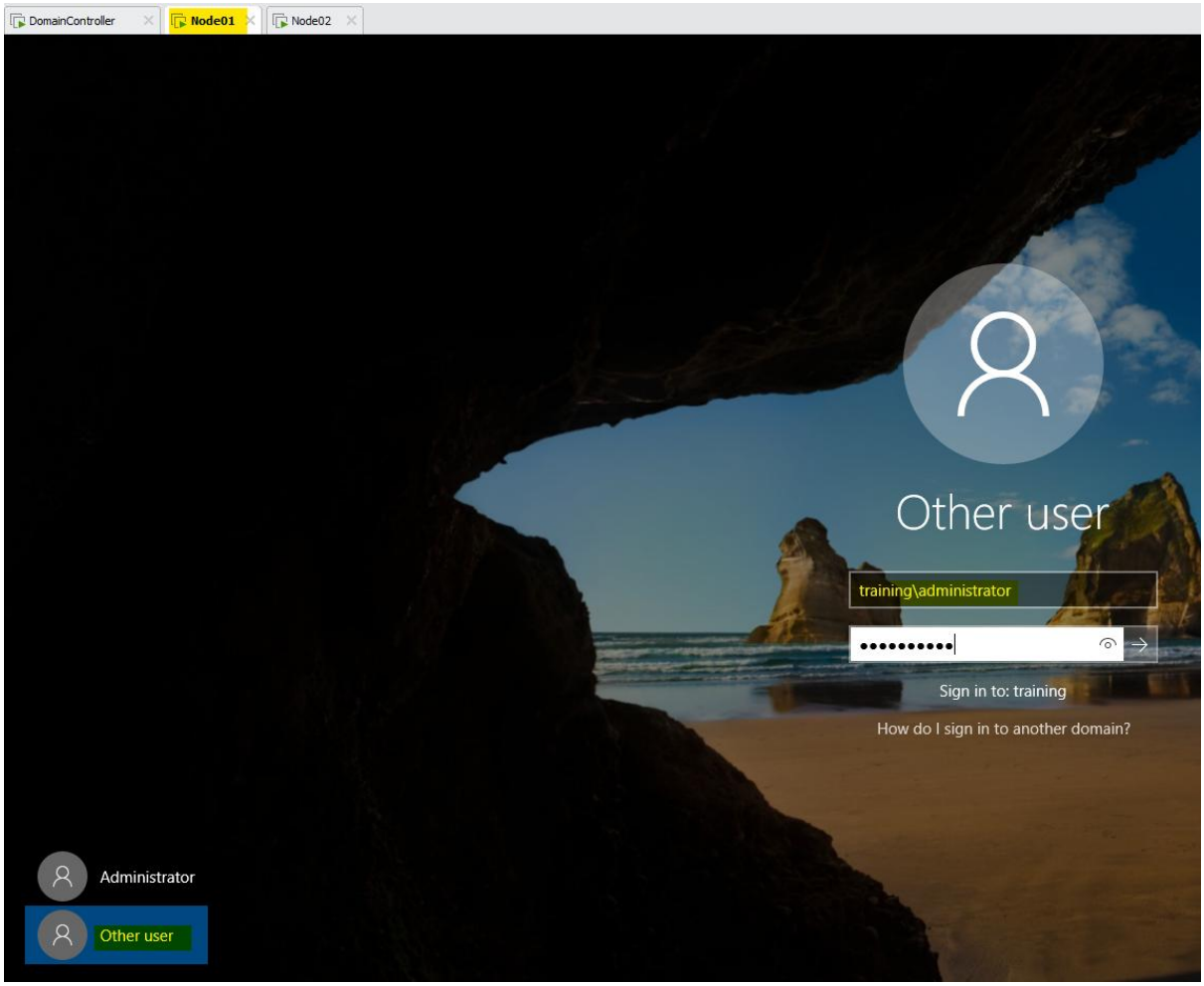
Click OK, once you get this prompt & restart this computer.



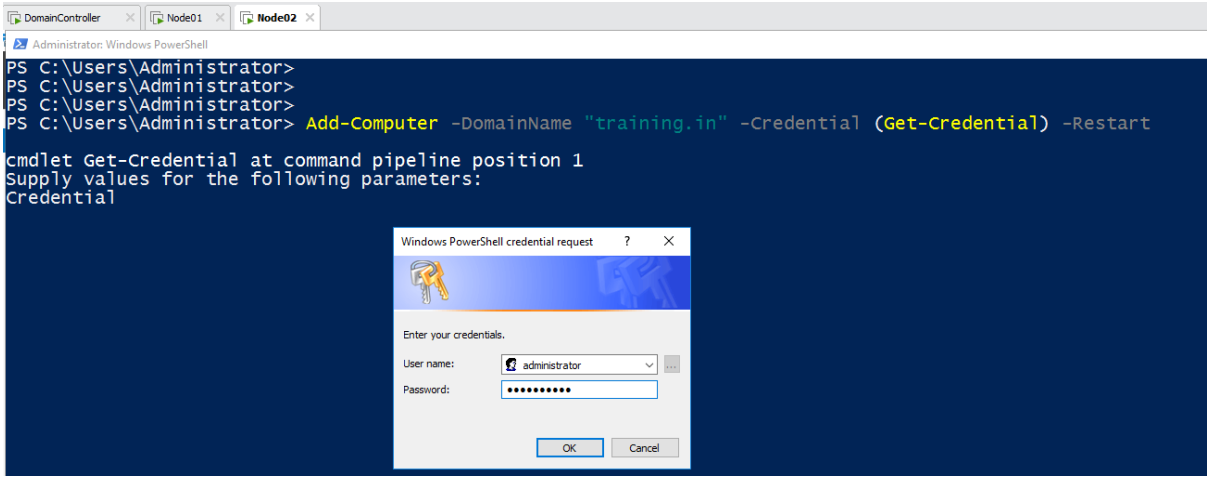




After joining the Node01 to domain, login as domain administrator:



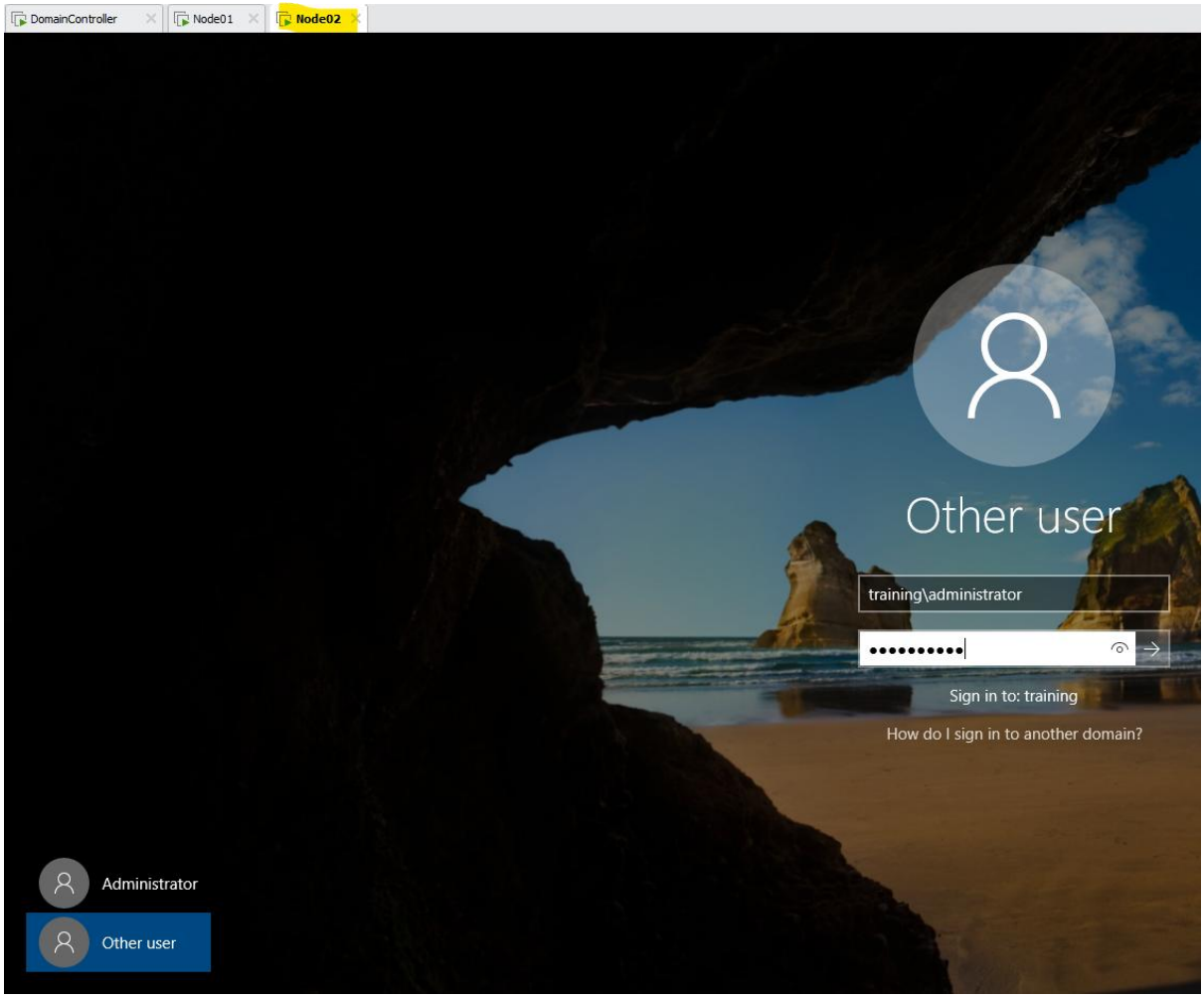
Domain joining Node02 to the domain controller via PowerShell:



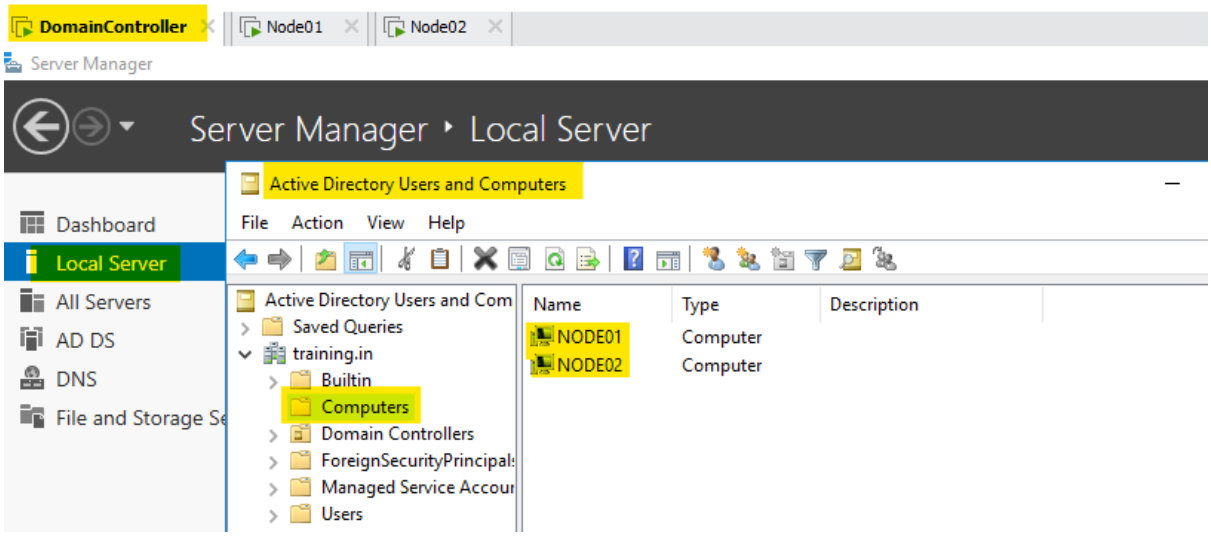
Cmd: **Add-Computer -DomainName "training.in" -Credential (Get-Credential) -Restart**

Note – If everything is OK, then the Node02 will restart automatically.

After restart, login as domain administrator:



Verify if the Node01 and Node02 is domain joined or not. Go to DC → Dashboard page → Tools → Active directory Users and Computers → 'Computers' OU.



Ping DC from Node01

```
Node01
PS C:\Users\administrator.TRAINING> ping dc

Pinging dc.training.in [192.168.10.10] with 32 bytes of data:
Reply from 192.168.10.10: bytes=32 time<1ms TTL=128
Reply from 192.168.10.10: bytes=32 time=1ms TTL=128
Reply from 192.168.10.10: bytes=32 time=1ms TTL=128
Reply from 192.168.10.10: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
PS C:\Users\administrator.TRAINING>
```

Ping DC from Node02

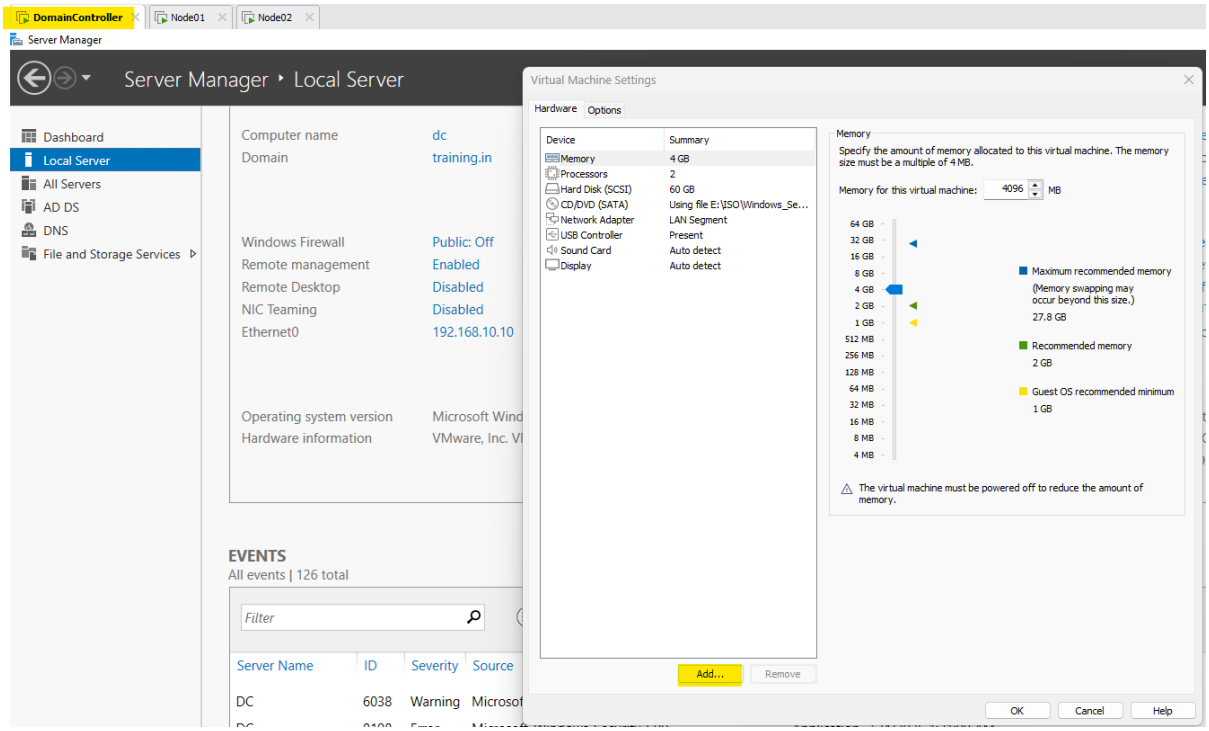
```
PS C:\Users\administrator.TRAINING> hostname
Node02
PS C:\Users\administrator.TRAINING> ping dc

Pinging dc.training.in [192.168.10.10] with 32 bytes of data:
Reply from 192.168.10.10: bytes=32 time<1ms TTL=128
Reply from 192.168.10.10: bytes=32 time<1ms TTL=128
Reply from 192.168.10.10: bytes=32 time<1ms TTL=128
Reply from 192.168.10.10: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
PS C:\Users\administrator.TRAINING>
```

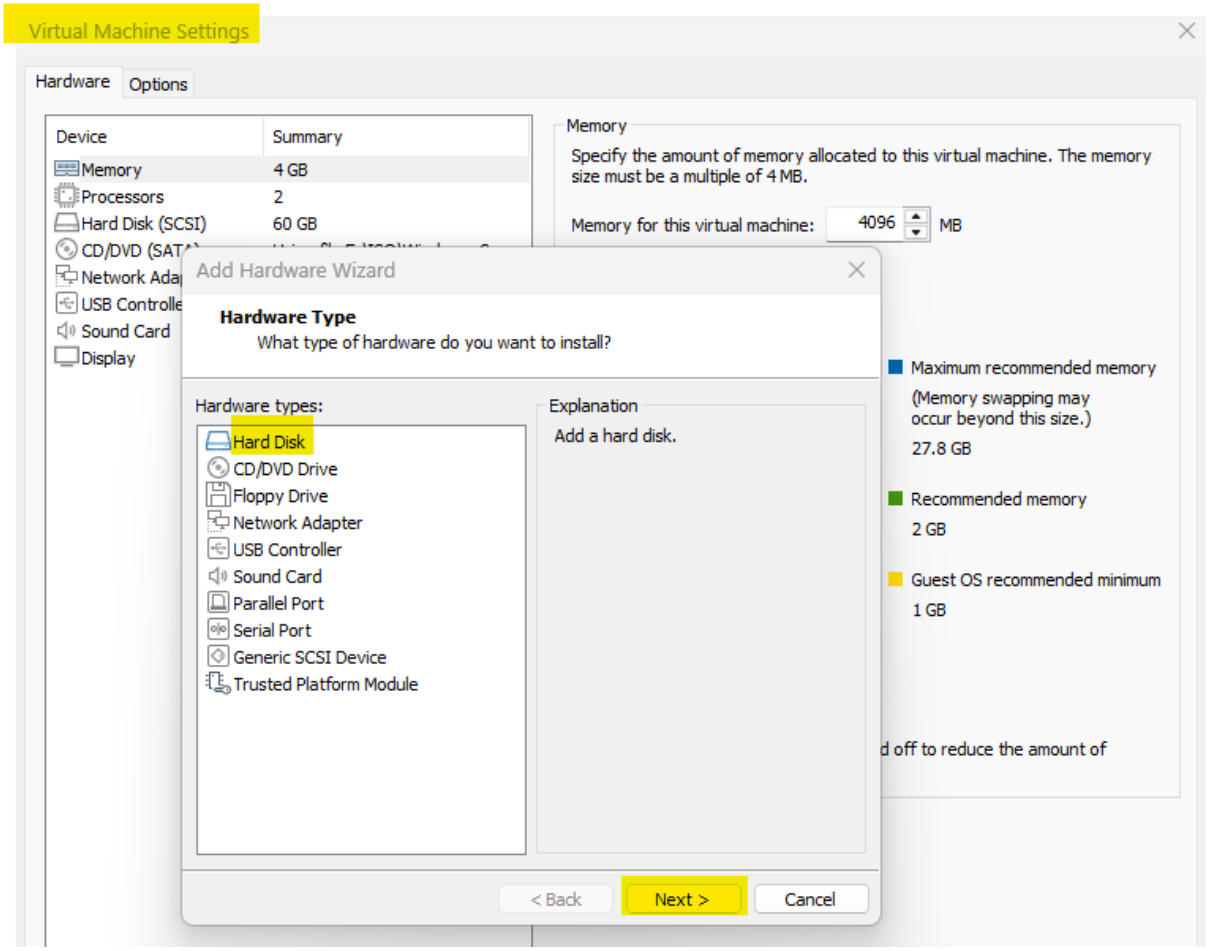
Ping Node 01 & 02 from DC:

```
PS C:\Users\Administrator> hostname
dc
PS C:\Users\Administrator> ping node01

Pinging node01.training.in [192.168.10.11] with 32 bytes of data:
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\Administrator> ping node02

Pinging node02.training.in [192.168.10.12] with 32 bytes of data:
Reply from 192.168.10.12: bytes=32 time<1ms TTL=128
Reply from 192.168.10.12: bytes=32 time<1ms TTL=128
Reply from 192.168.10.12: bytes=32 time=1ms TTL=128
Reply from 192.168.10.12: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.10.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
PS C:\Users\Administrator> _
```

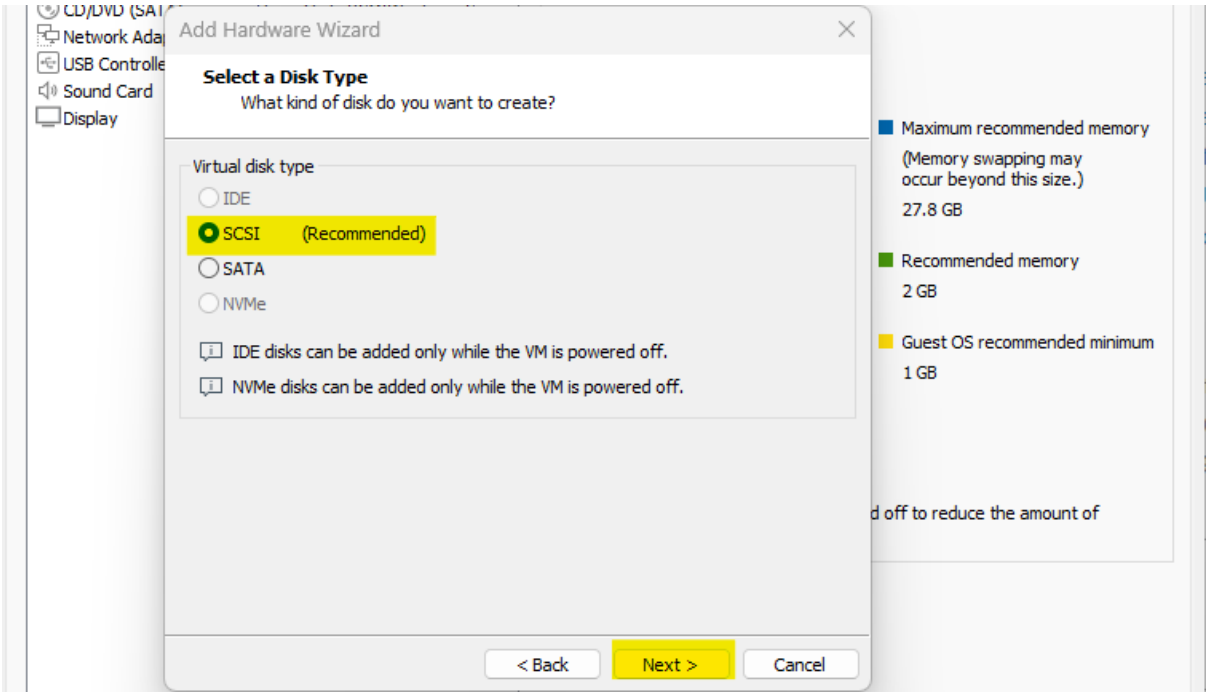
Adding a new disk on DC machine & creating an NTFS file system

To add a new disk to domain controller machine, go to virtual machine → Setting →Add

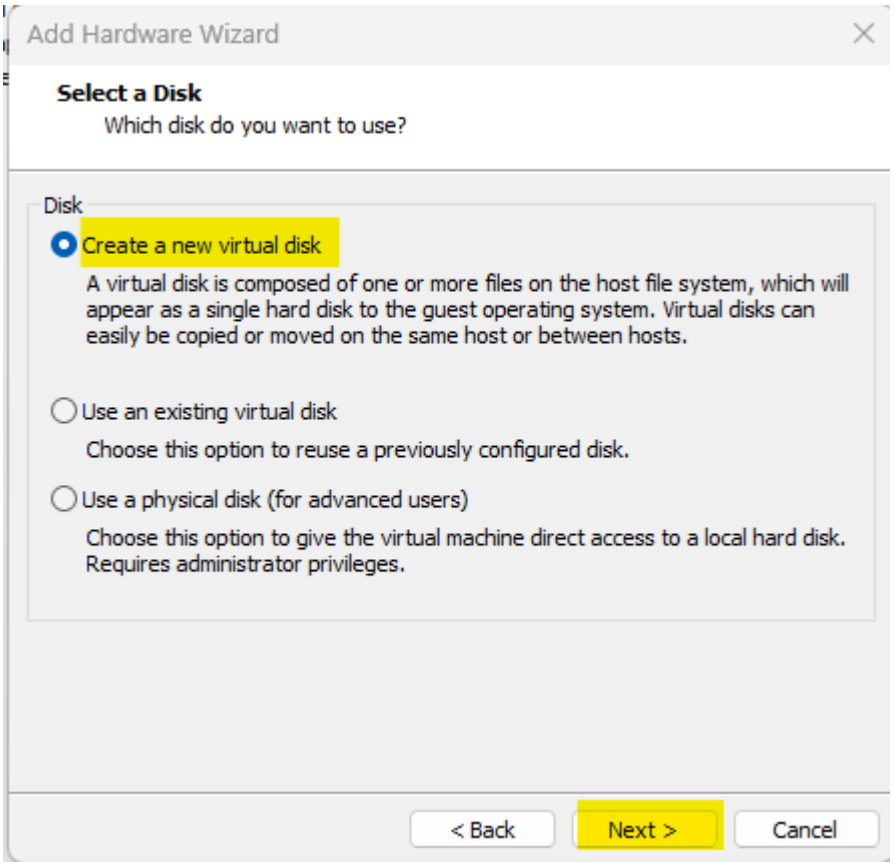




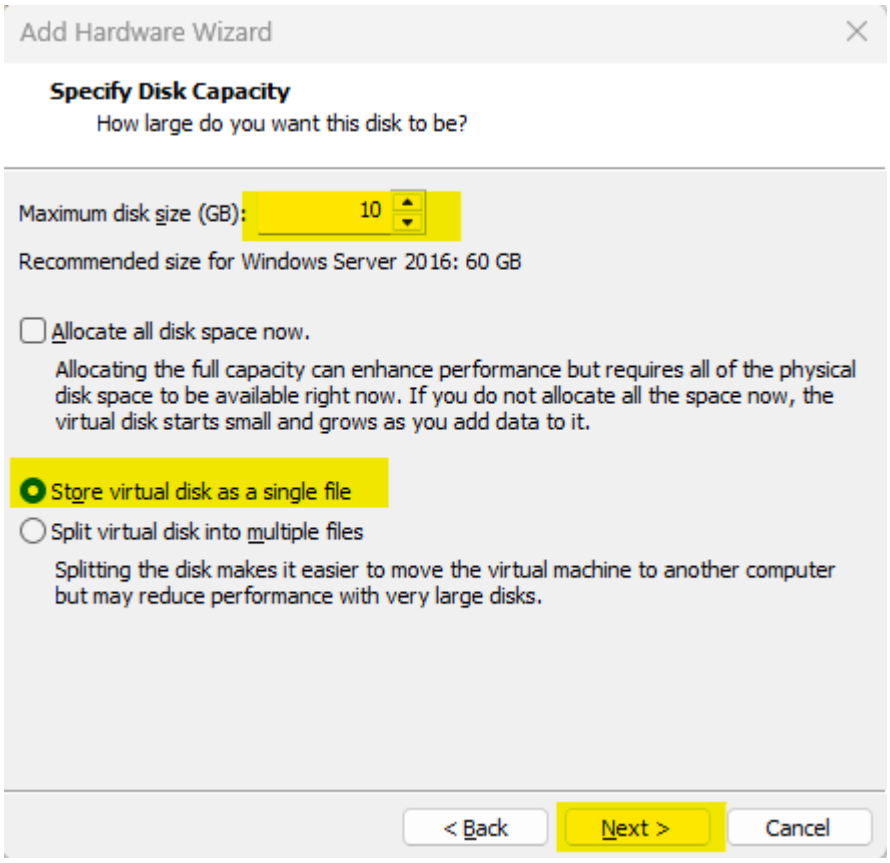
Select SCSI disk



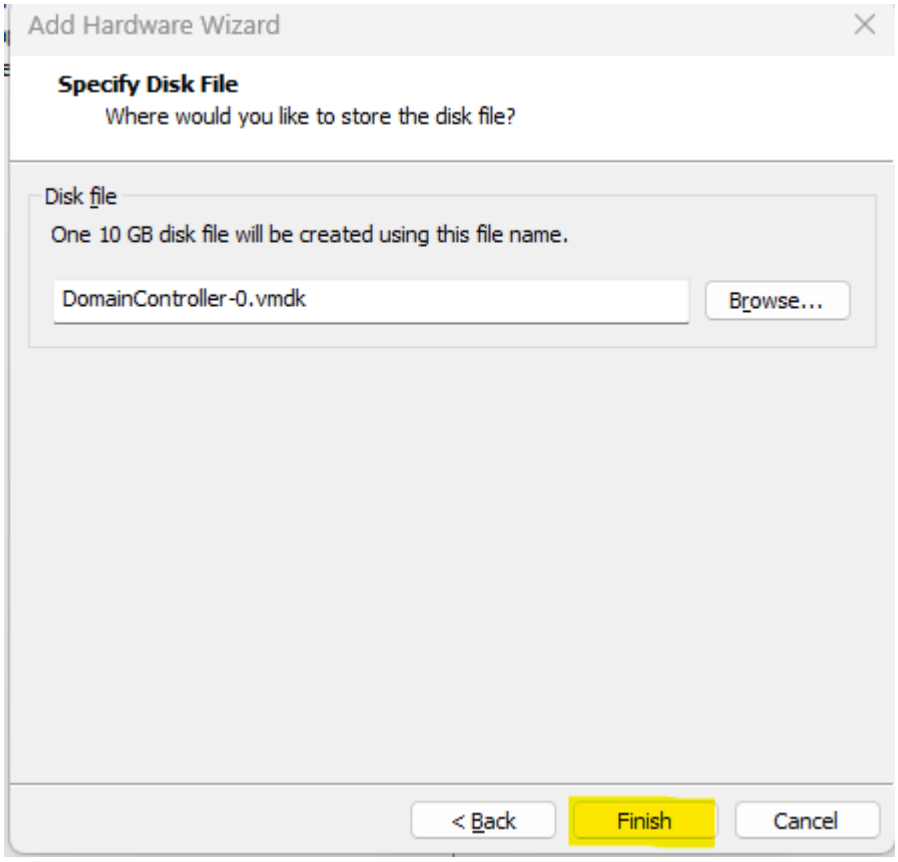
Create a new virtual disk



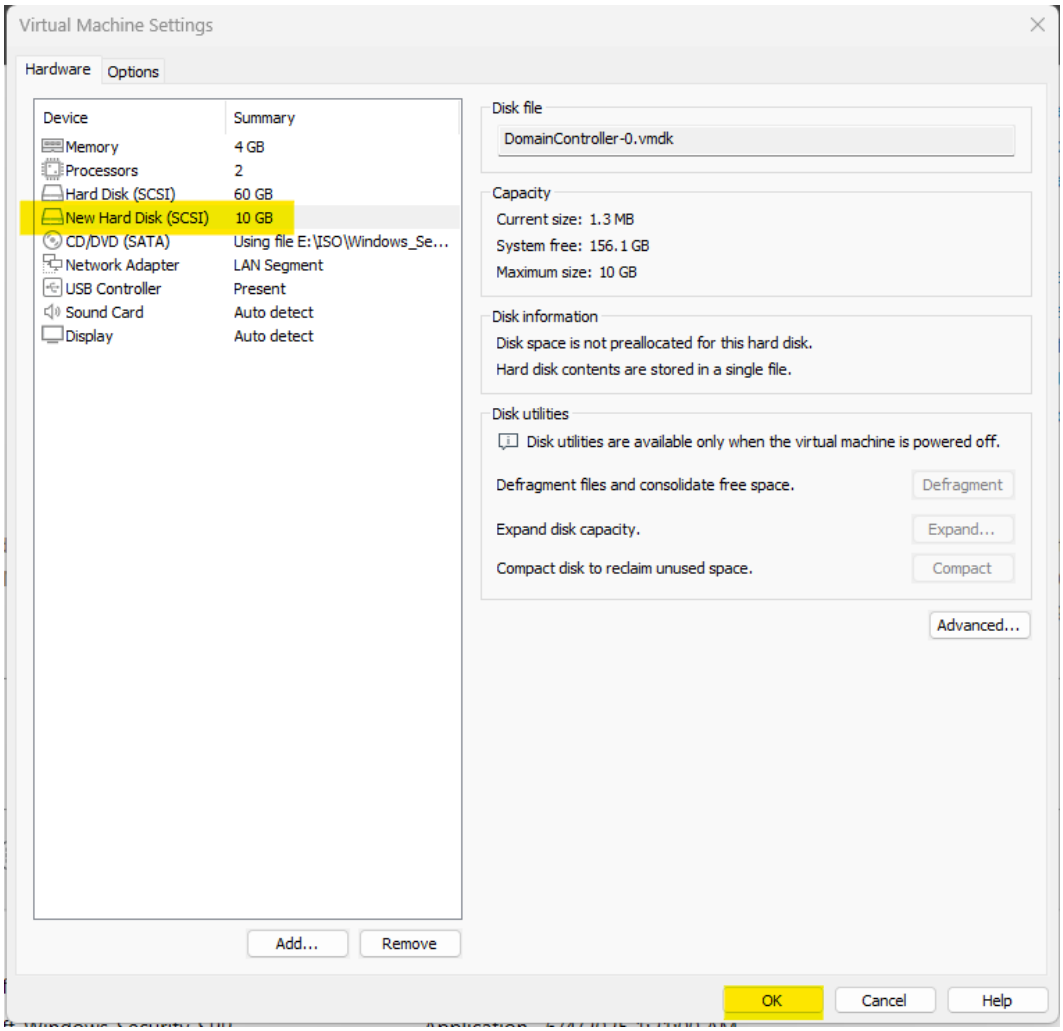
Specify disk size:



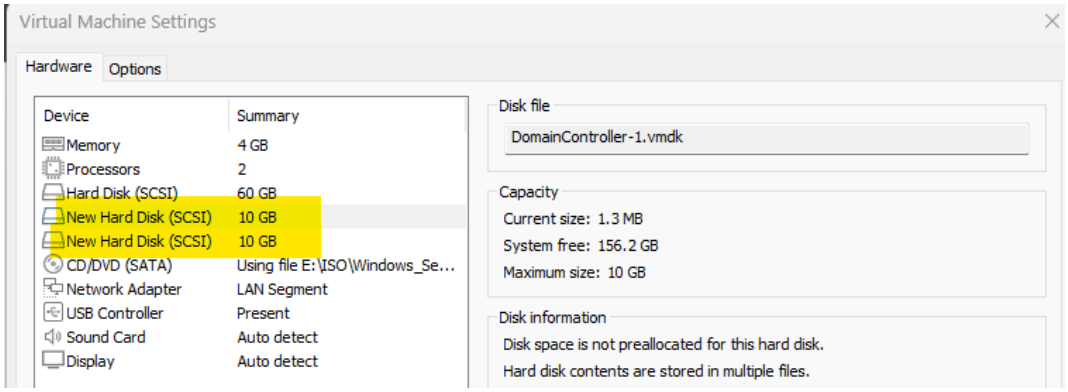
Specify disk name & click Finish



Verify:

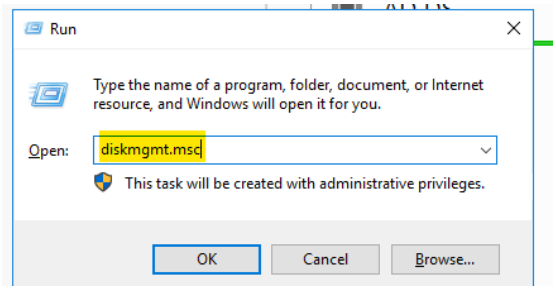


Adding another disk of 10GB to DC machine again.

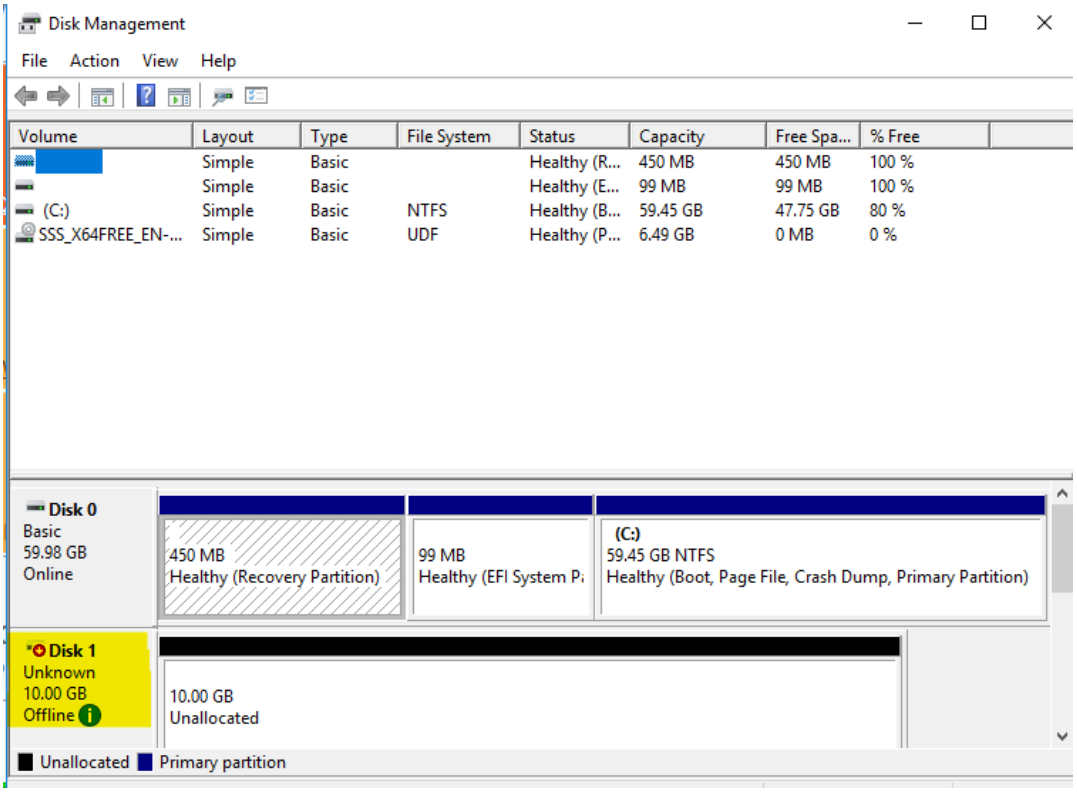


Note – just for precaution, reboot your DC virtual machine to check if the write disk is booting. If in case after reboot you get installation window or OS not found error, then change the boot sequence using firmware in VMWare workstation.

Now to access the disk, use cmd → diskmgmt.msc



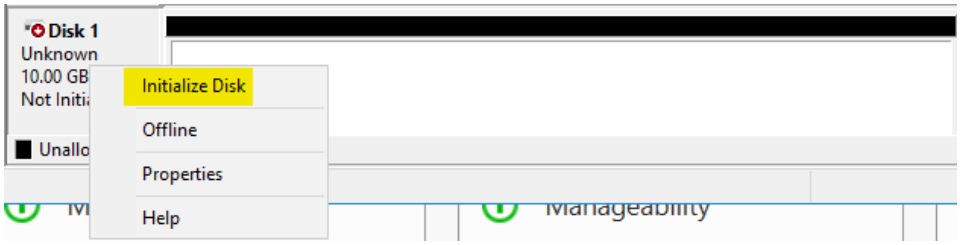
Currently disk is 'offline', so we need to initialize the disk and then make it 'online'.



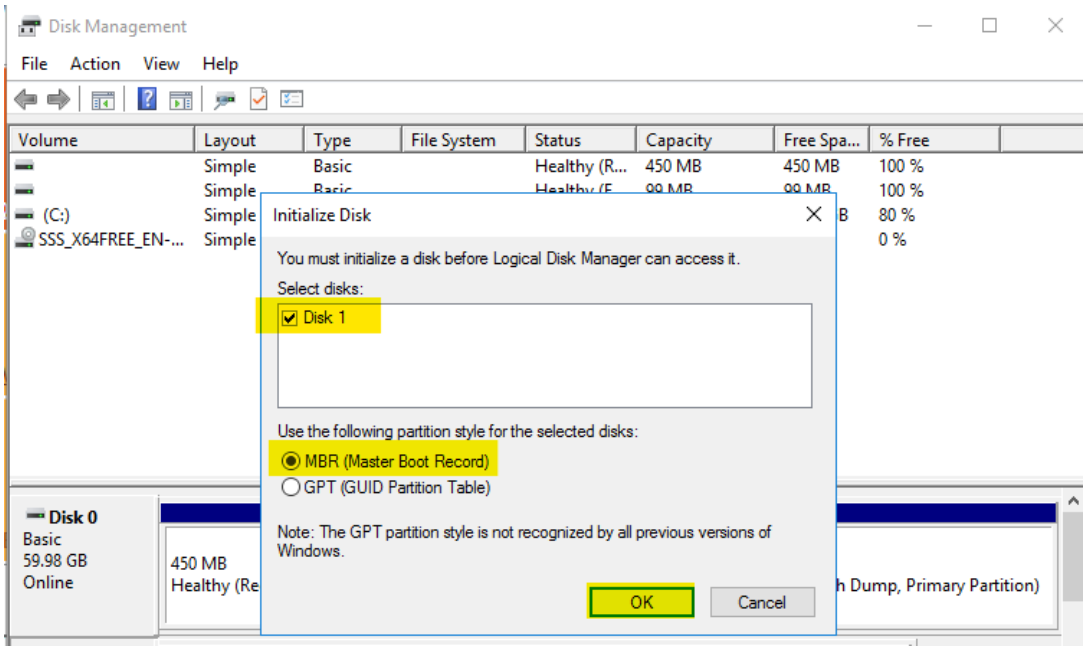
To make the disk online, right-click on the Disk1 (in your case, check your disk number) & then click online.

After making it 'online', we need to initialize the disk.

So right-click on the disk and then initialize disk



Verify the disk name & select the partitioning style. Since our disk is less than 2TB, MBR is good enough for this practical.

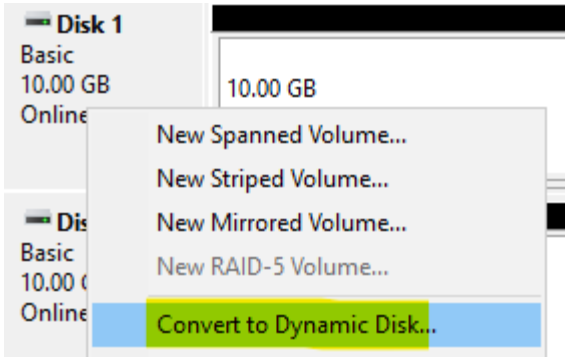


& verify:

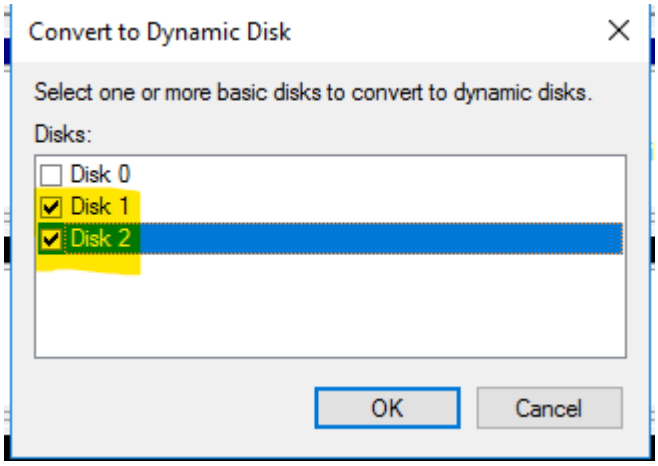
Similarly add another 10GB disk and initialize it.

Create a dynamic disk (spanned volume) using Disk 1 & Disk 2.

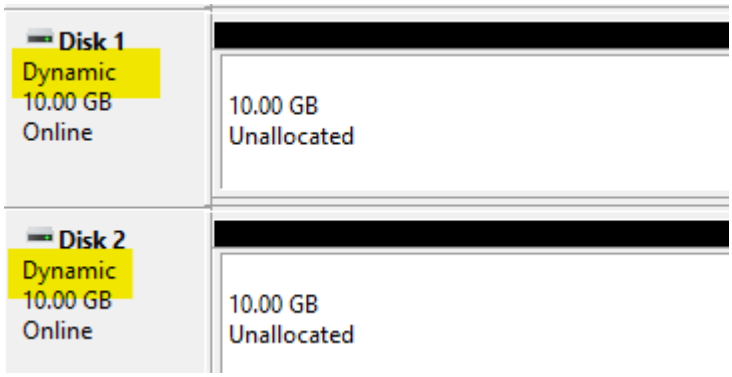
Right-click on Disk 1 and select dynamic disk



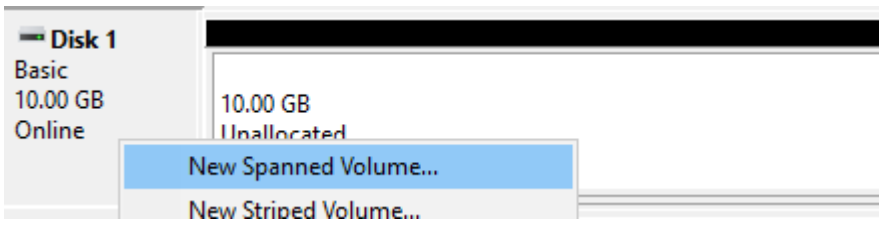
Select both disks (as we need to convert both to dynamic disks)



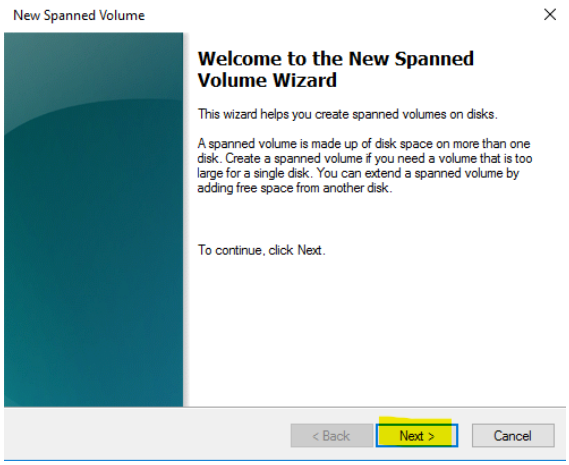
Verify:



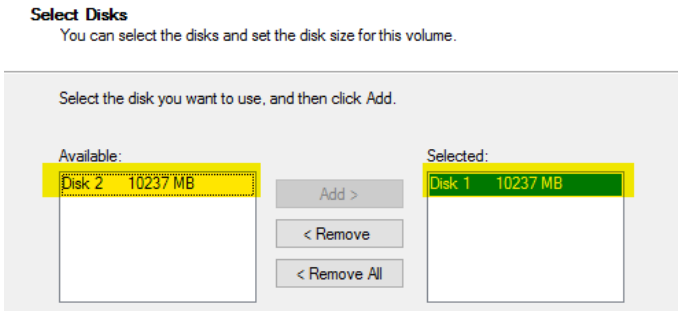
Right-click on Disk 1 → New Spanned Volume …



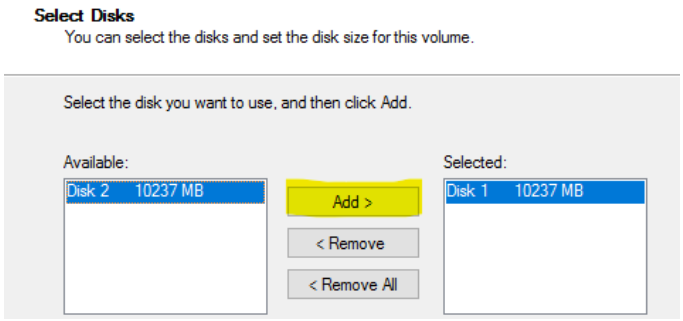
Click Next on “Welcome wizard”



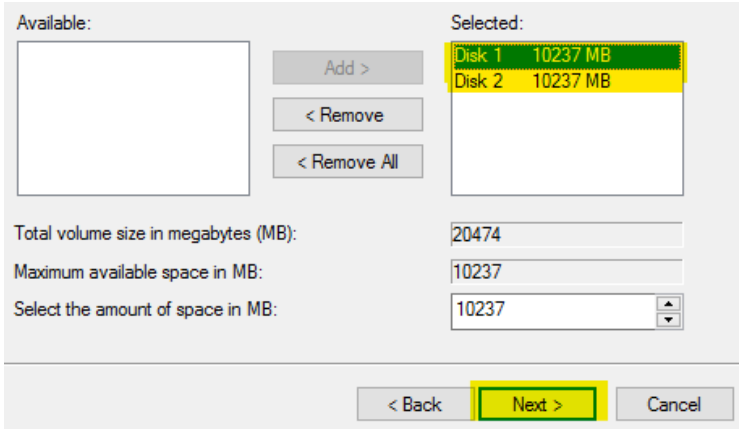
Select the Disk 2



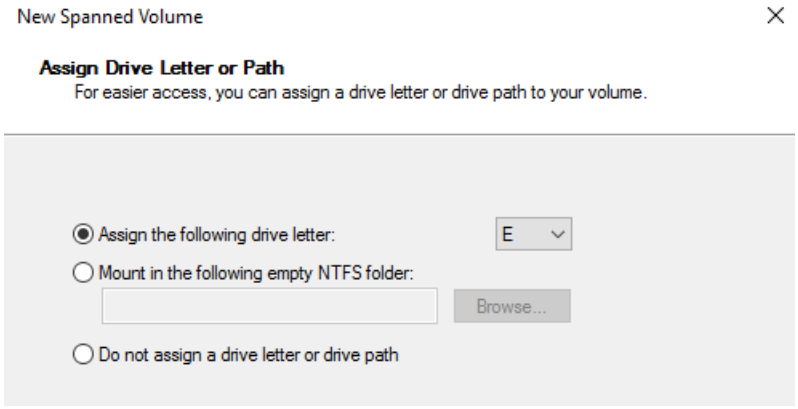
And click on “Add >”



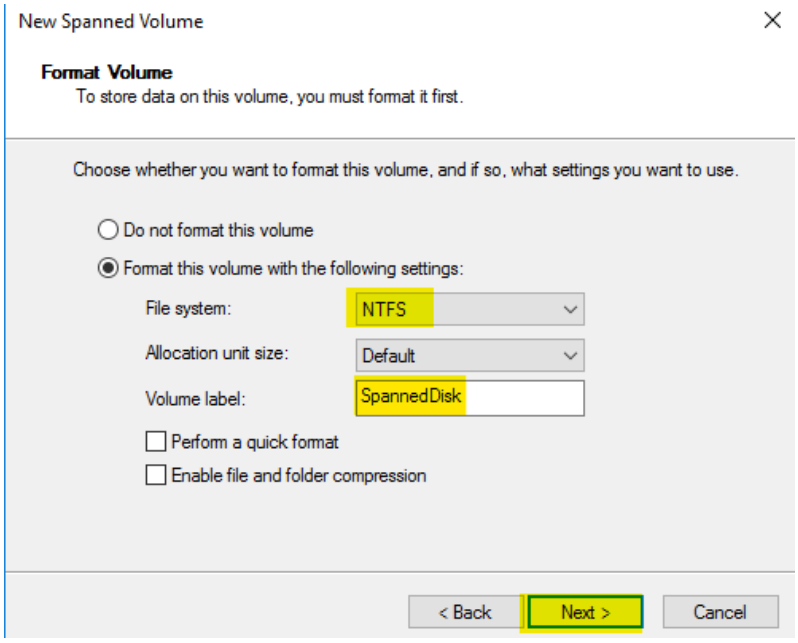
Once disks are present under ‘selected’ option, click Next.



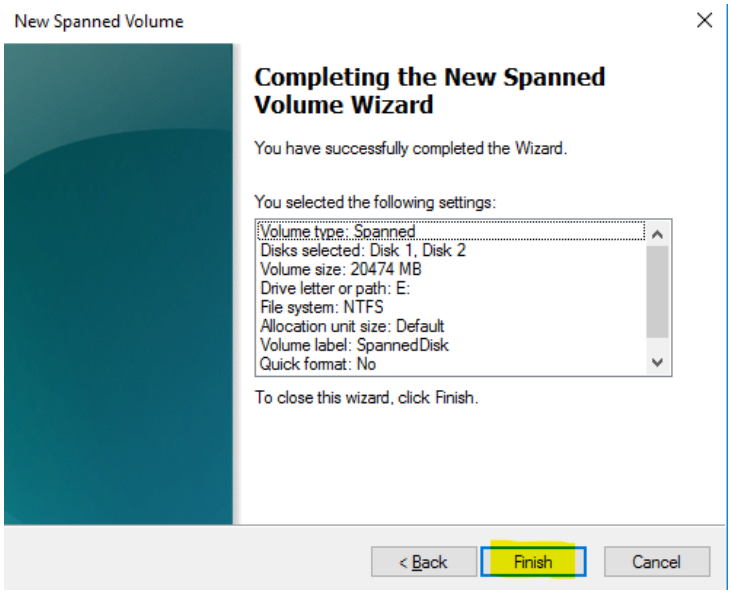
Select a mount point for this disk:



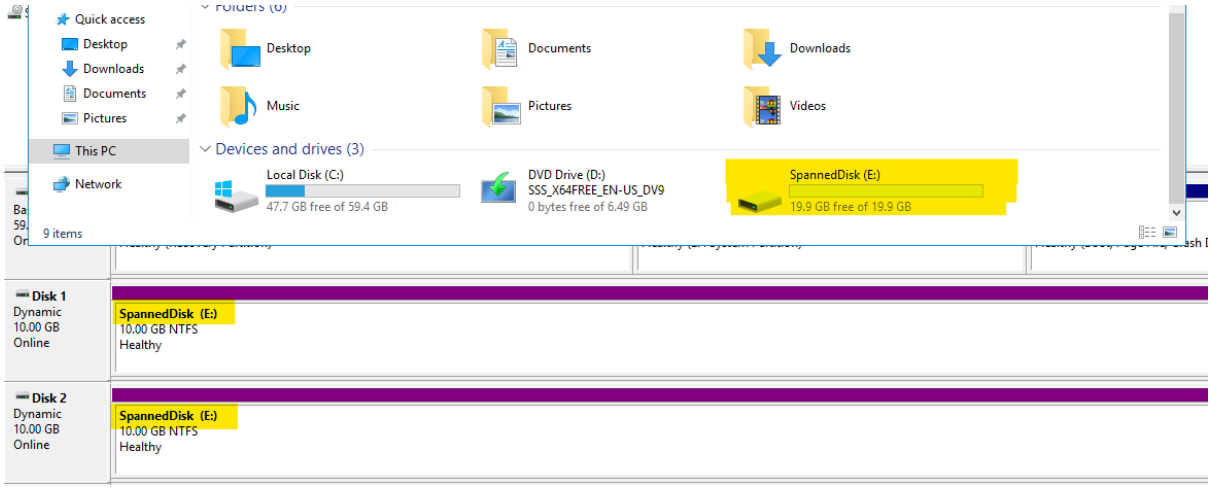
Select the following and click Next:



And click “Finish”



Verify ~20GB (approx.) disk is present.



Installing and configuring iSCSI target server on DC

What is iSCSI?

iSCSI (Internet Small Computer Systems Interface) is a network-based storage protocol that allows a client (called an initiator) to send SCSI commands to storage devices (called targets) over TCP/IP networks, typically Ethernet.

It enables block-level storage over standard networks, allowing servers to access storage devices as if they were locally attached disks.

Why Use iSCSI?

- Inexpensive (uses standard Ethernet instead of costly Fibre Channel).
- Scalable and flexible.
- Enables centralized storage management.
- Supports high availability and clustering.

iSCSI Core Terms and Definitions:

Term	Description
Initiator	The **client-side component** (usually a server or OS) that initiates a connection to the storage. Sends SCSI commands to the target.
Target	The **storage device/server** that presents logical units (LUNs) over the network to initiators. Responds to SCSI commands.
LUN (Logical Unit Number)	A **logical volume** or partition on the storage presented by the target to the initiator. Seen as a "disk" by the client OS.
IQN (iSCSI Qualified Name)	A unique identifier used for both initiators and targets to identify themselves on the network. Format: iqn.yyyy-mm.reverse.domain:unique_name
Portal	The **IP address and TCP port** (default: 3260) on which the iSCSI target listens.
Discovery	Process where the **initiator queries the target** to find available LUNs. Two methods: Static or SendTargets.
CHAP (Challenge-Handshake Authentication Protocol)	An authentication method used to secure communication between initiator and target. Ensures the identity of participants.
iSNS (Internet Storage Name Service)	A discovery protocol that provides automatic discovery and management of iSCSI devices across the network.
MPIO (Multipath I/O)	Technique used for **redundancy and load balancing** by providing multiple paths to the same iSCSI storage (for high availability).

Term	Description
iSCSI Session	A **connection between an initiator and a target**, identified by IQNs and IP address/port.
iSCSI Software Initiator	A **driver or built-in OS component** that allows a machine to act as an iSCSI initiator without special hardware.
iSCSI Hardware Initiator (HBA)	A physical device (Host Bus Adapter) that offloads iSCSI processing from the CPU. Offers better performance.
iSCSI Boot	Allows a computer to **boot from an iSCSI LUN** (e.g., diskless servers) using BIOS or UEFI that supports iSCSI boot.

Security Features in iSCSI:

- CHAP/Mutual CHAP – ensures only authorized initiators can connect.
- IPsec – encrypts iSCSI traffic for secure data transfer.
- Access Control Lists (ACLs) – restrict access to specific IQNs or IPs.

Tools and Commands (Windows):

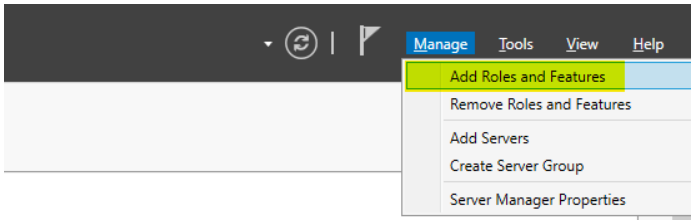
Tool	Purpose
iscsicpl.exe	Open iSCSI Initiator GUI
iscsicli	Command-line tool for advanced iSCSI configuration
diskmgmt.msc	Format/mount discovered LUN
mpclaim	Manage MPIO settings
Windows Features	Add iSCSI Target Server role using Server Manager

iSCSI vs. Other Storage Protocols

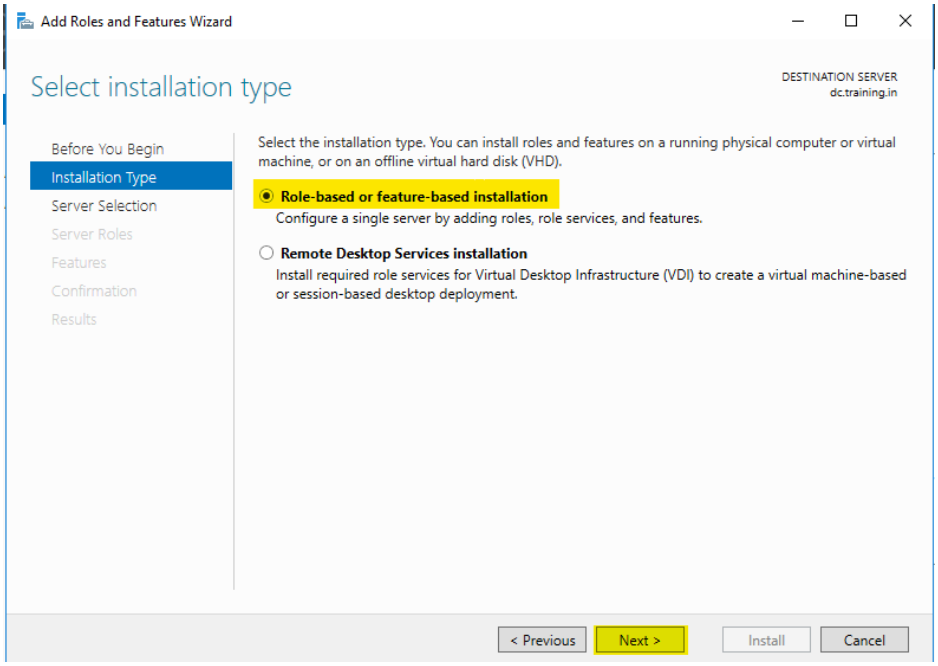
Protocol	Type	Transport	Used In
iSCSI	Block-level	IP (Ethernet)	Enterprise and SMB environments
NFS	File-level	IP	Unix/Linux file shares
SMB/CIFS	File-level	IP	Windows file shares
Fibre Channel (FC)	Block-level	Fiber-optic network	High-end data centers
FCoE	Block-level	Ethernet (Layer 2)	Converged networks

Installing and configuring iSCSI target server

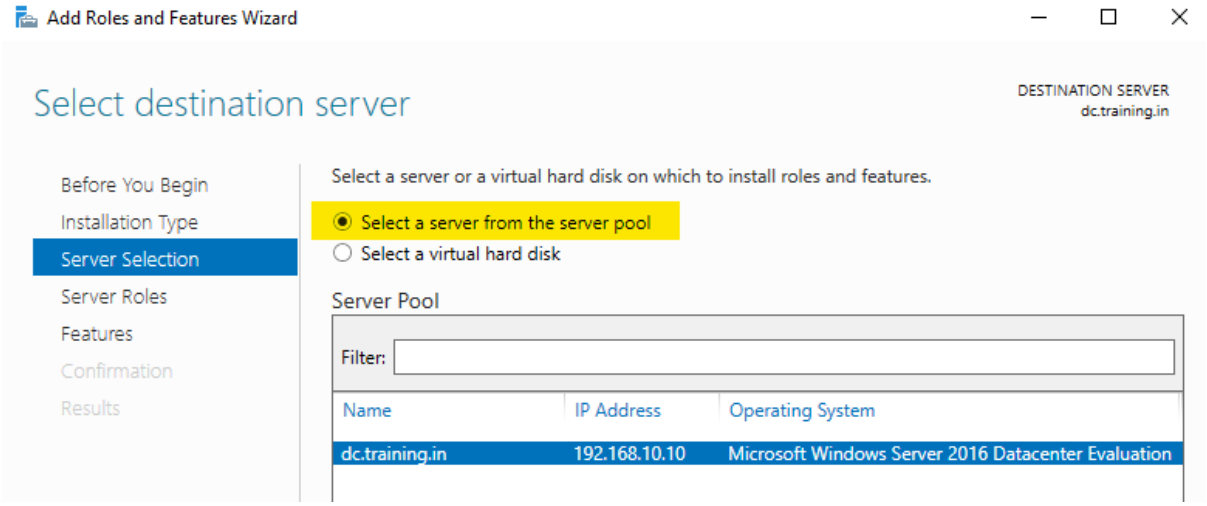
To install the iSCSI target server, go to Server dashboard page →Manage → Add roles and features



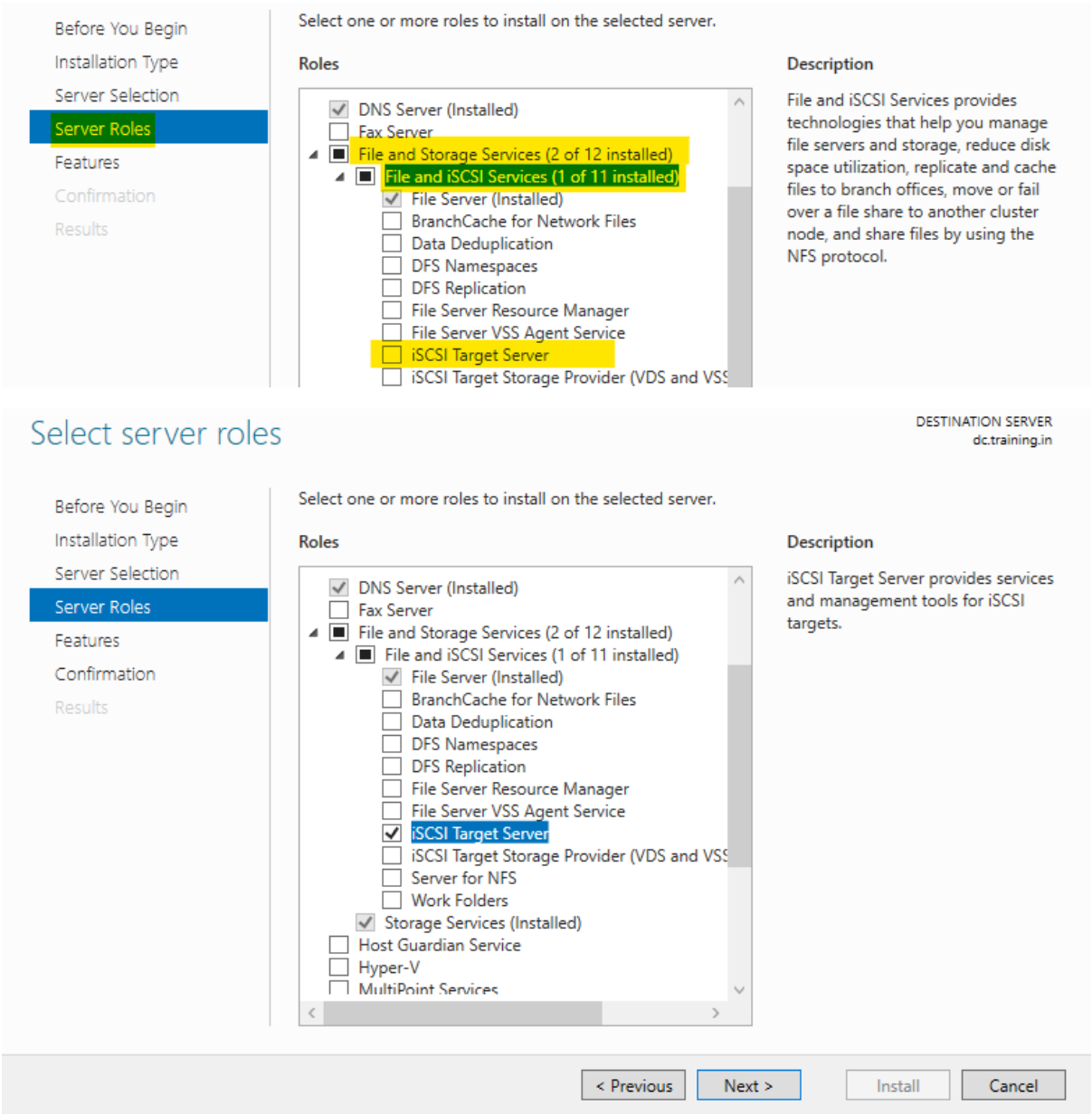
Select installation type as “Role-based or feature-based installation”



Select destination server as server pool:

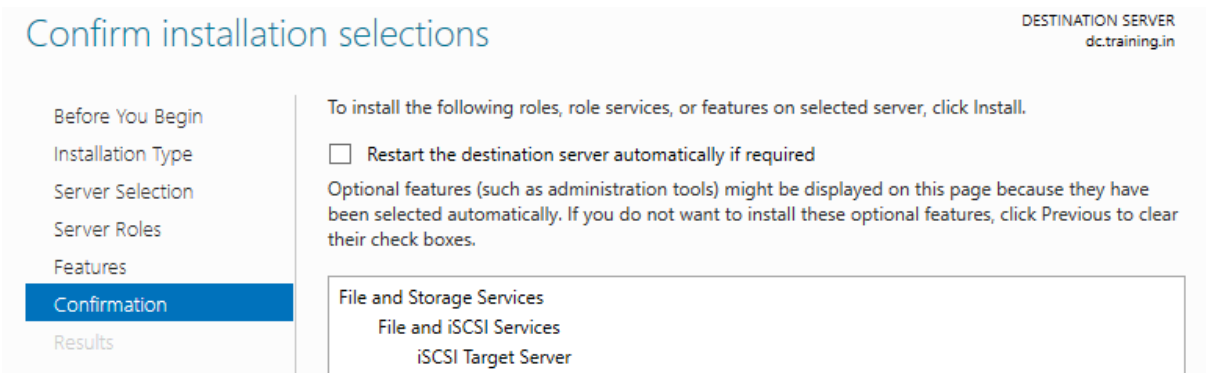


Check “iSCSI target server”



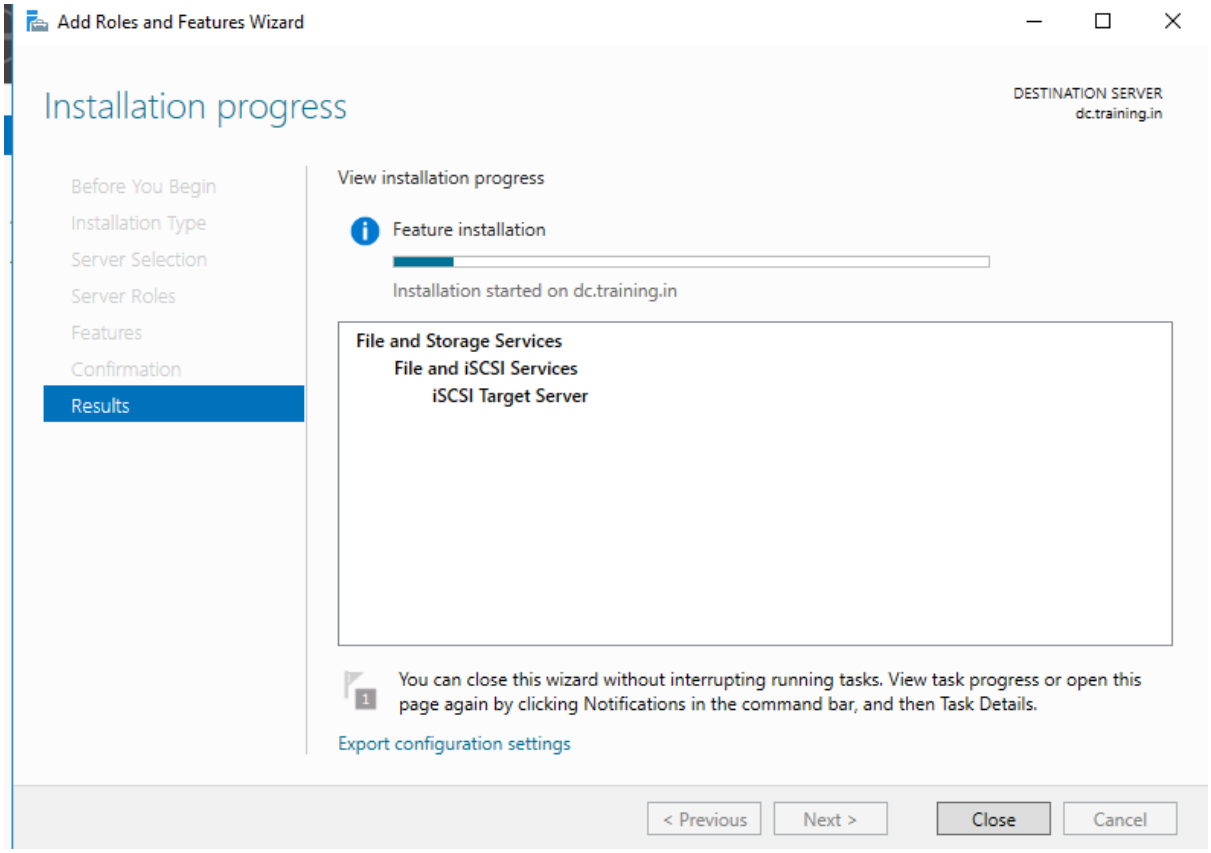
And click on “Next”.

- No additional features required.

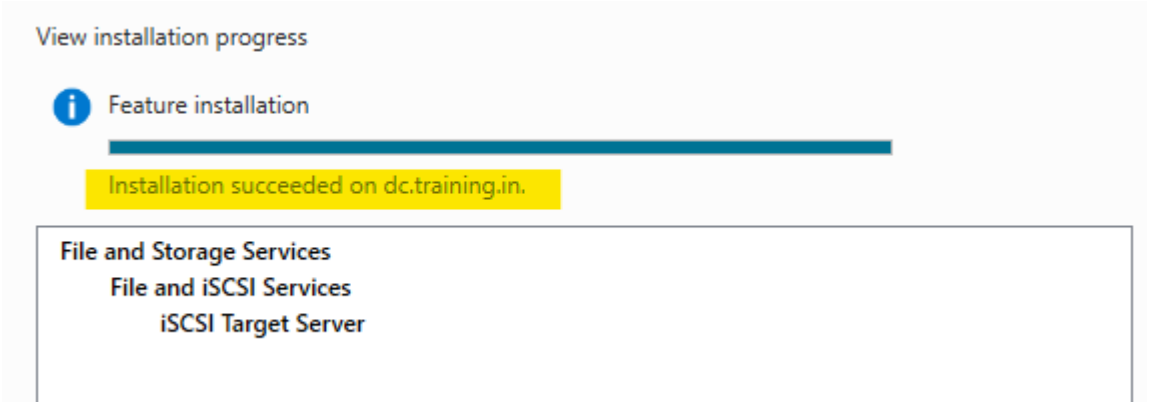


No restart is required, post installation → click on “install” button.

Wait until iSCSI role is installed.



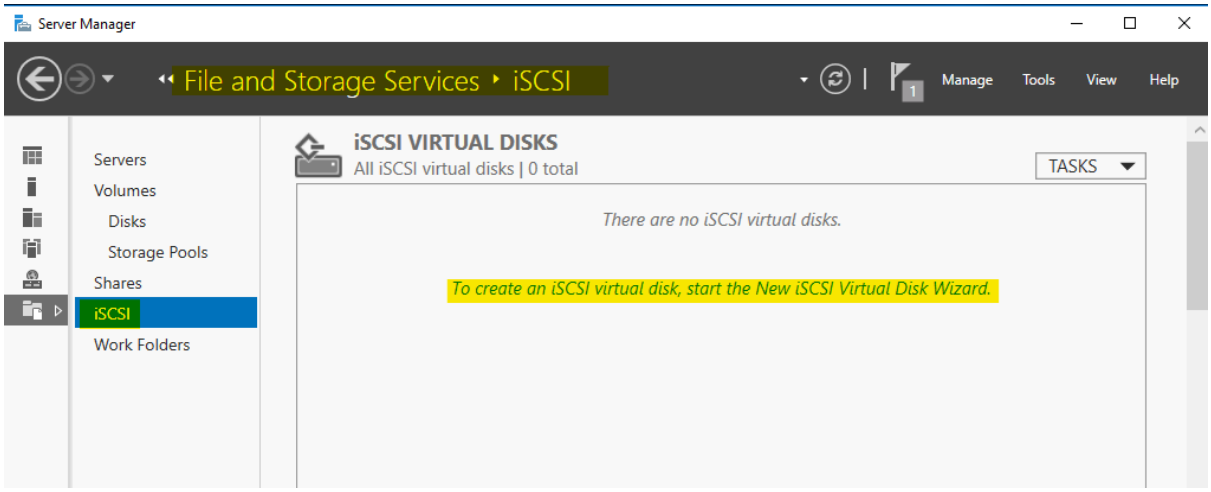
Verify:



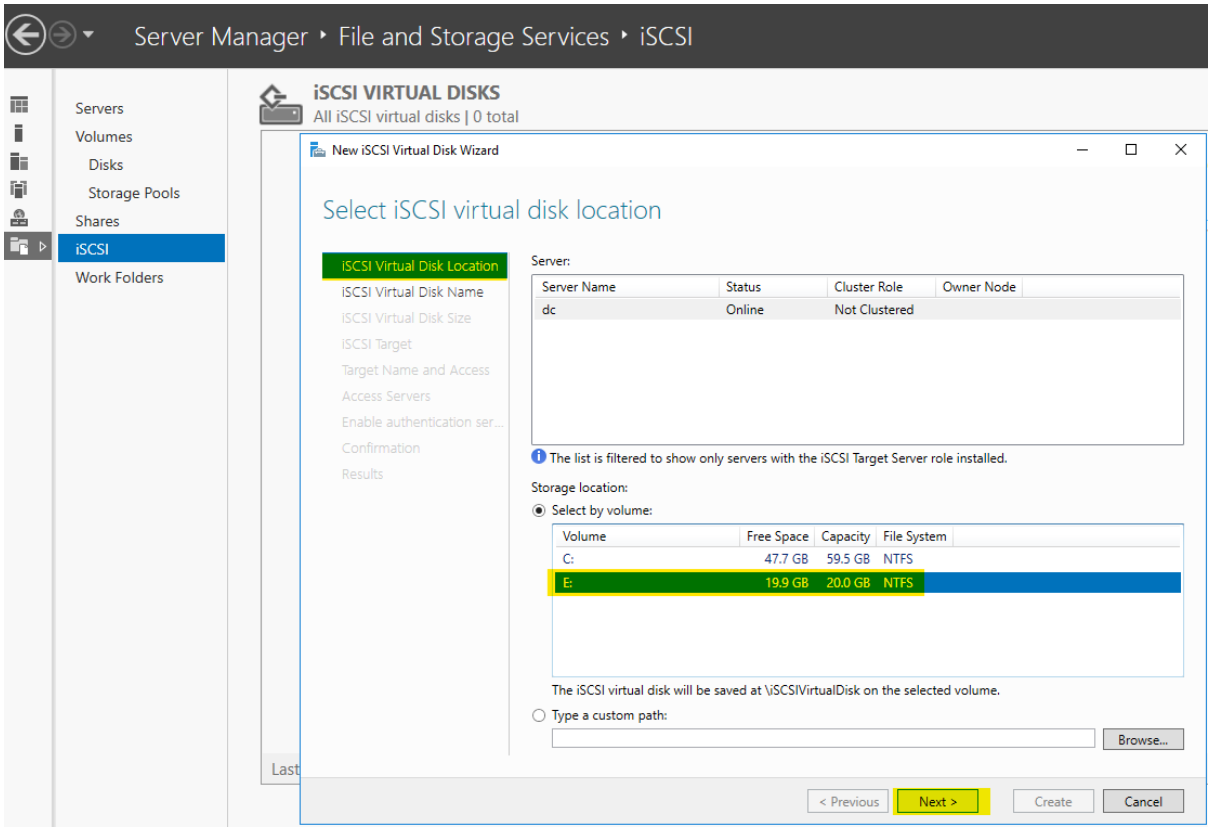
Then click on close.

To configure iSCSI on DC

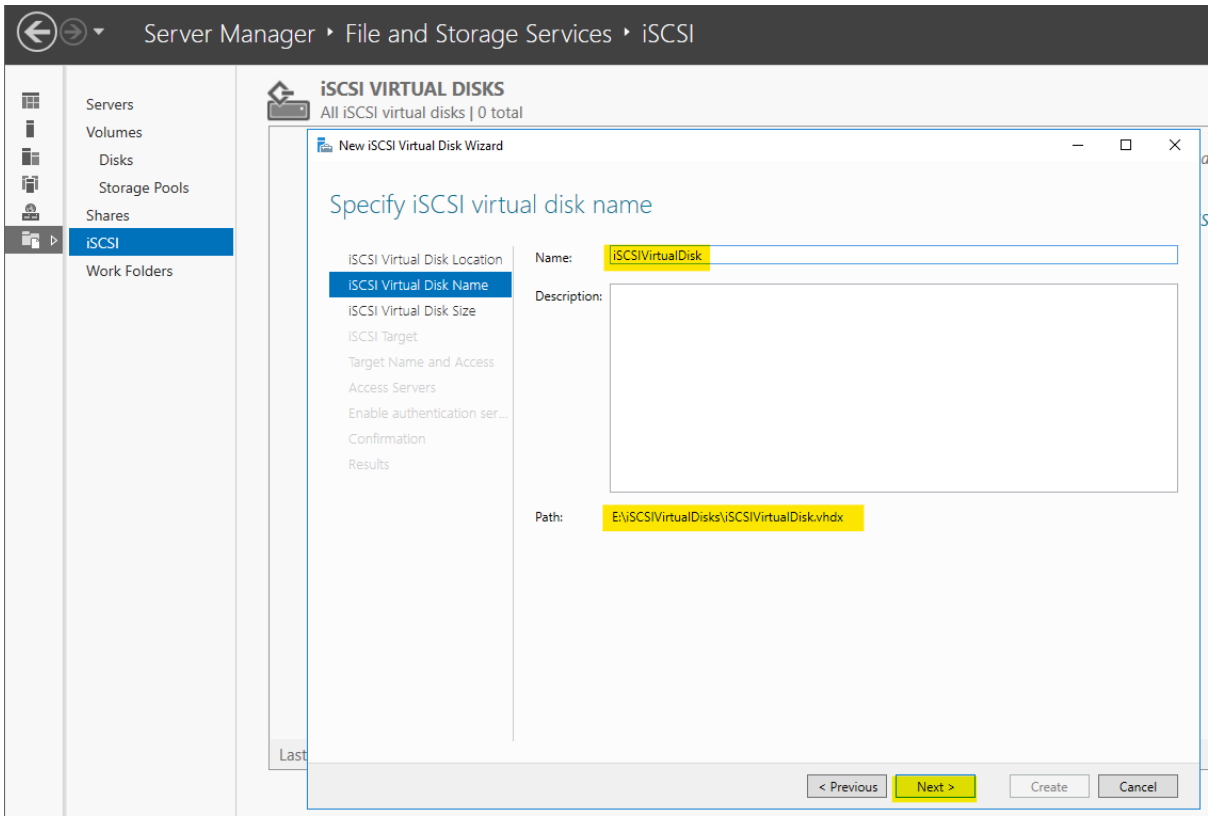
Go to server manager dashboard → File and storage services → iSCSI



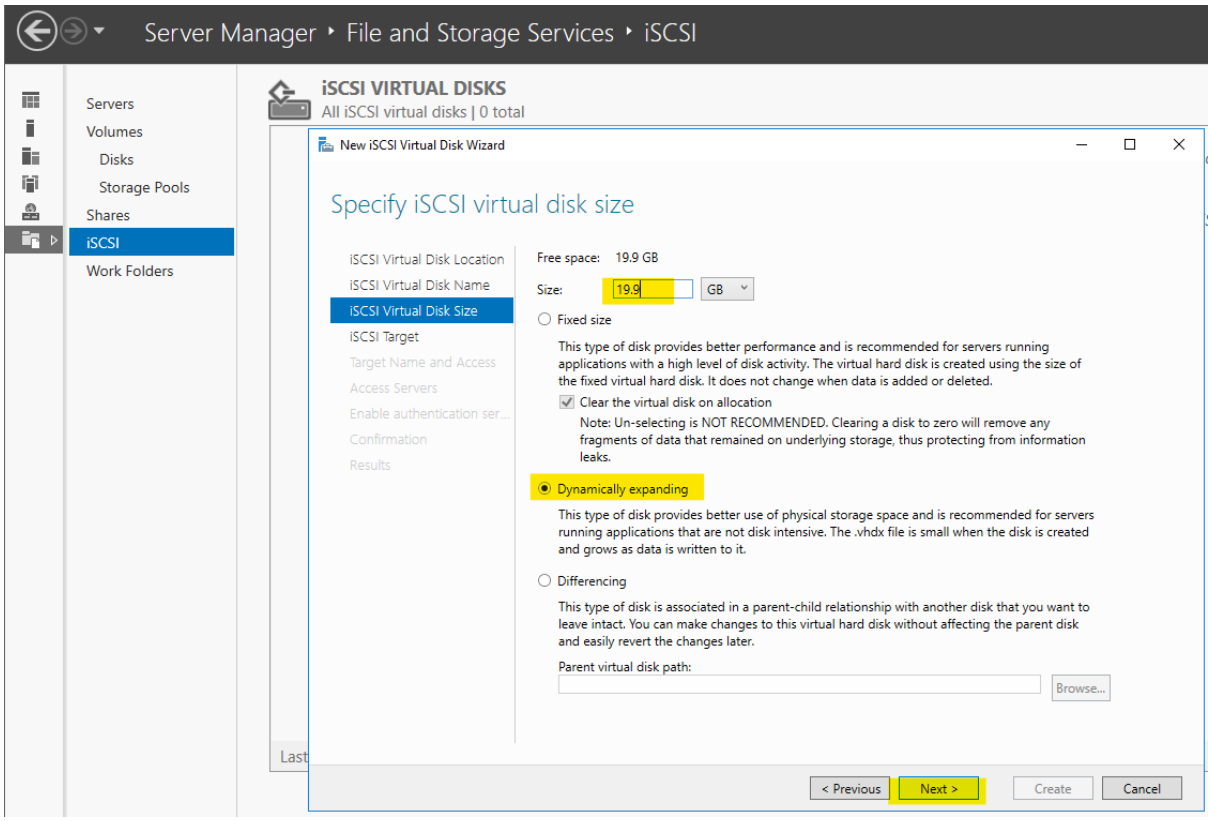
Now click on “To create an iSCSI virtual disk, start the New iSCSI Virtual Disk Wizard” & select the new added disk (E:\ in my case)



Provide a disk name and click on Next.

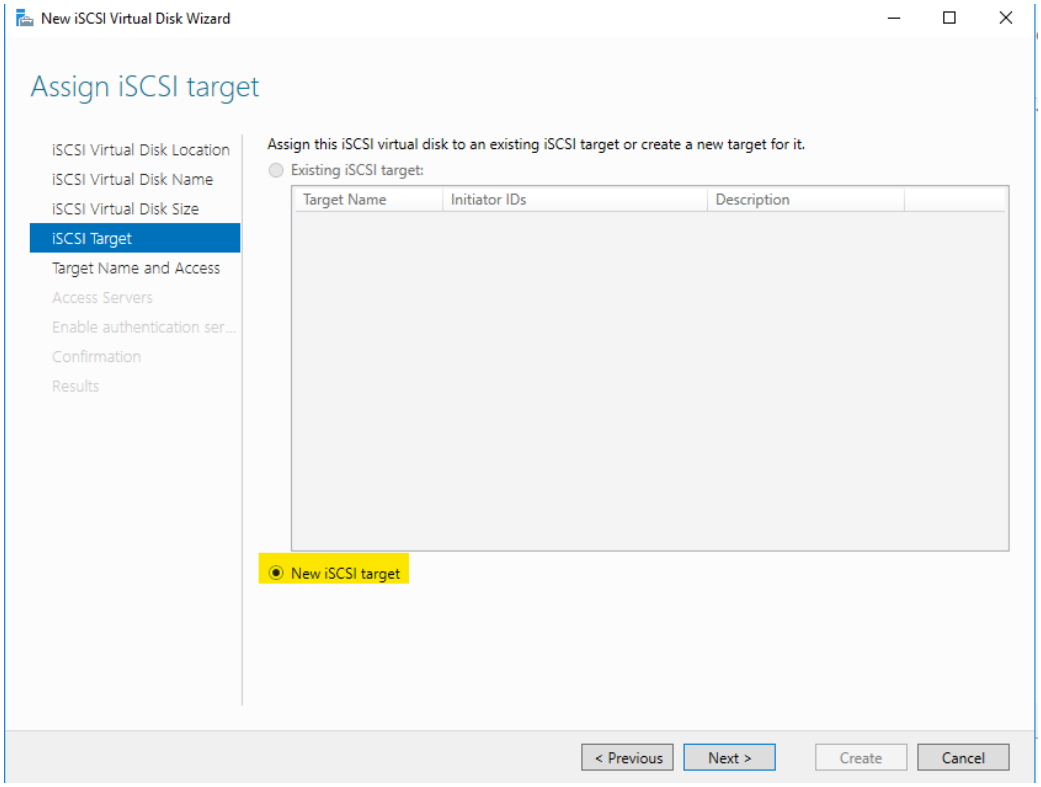


Provide the disk size and select ‘dynamically expanding’ disk

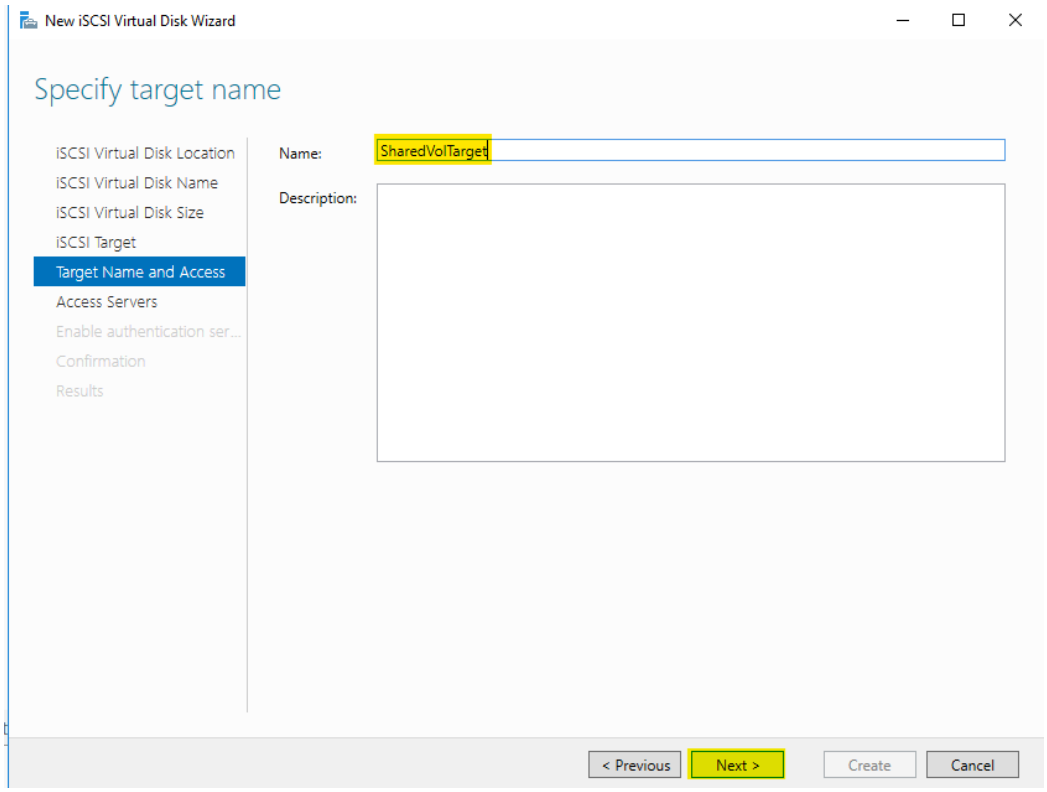


And click on Next.

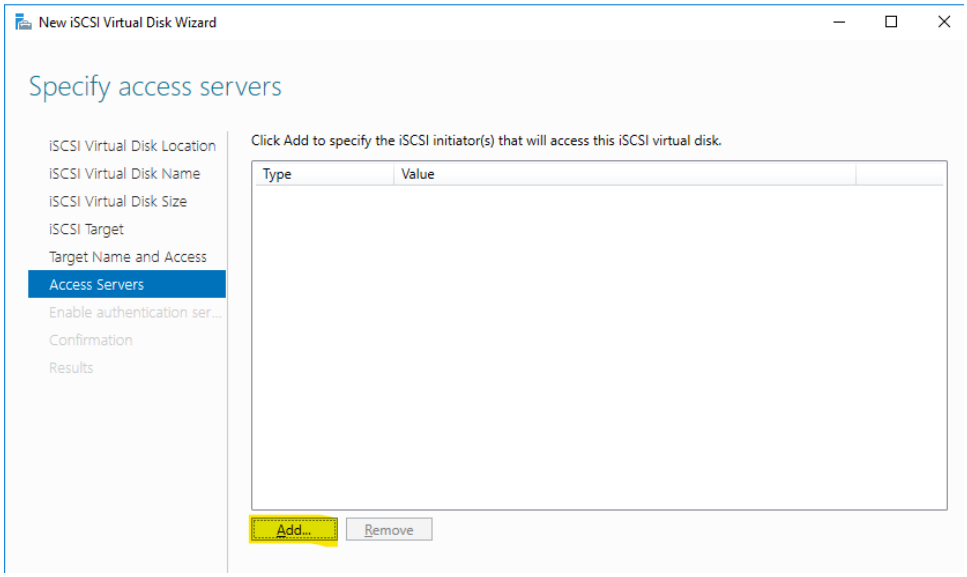
Select “New iSCSI target”



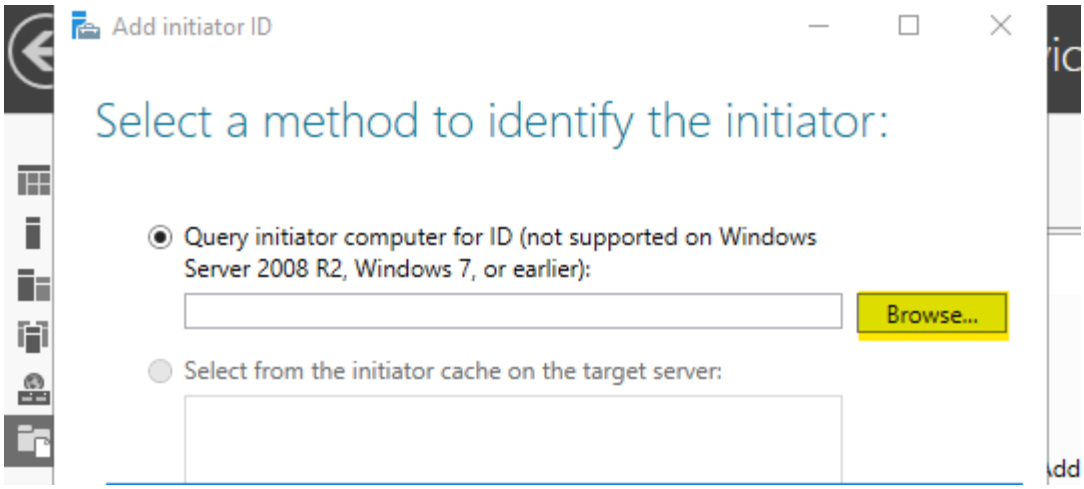
Provide a shared volume name:



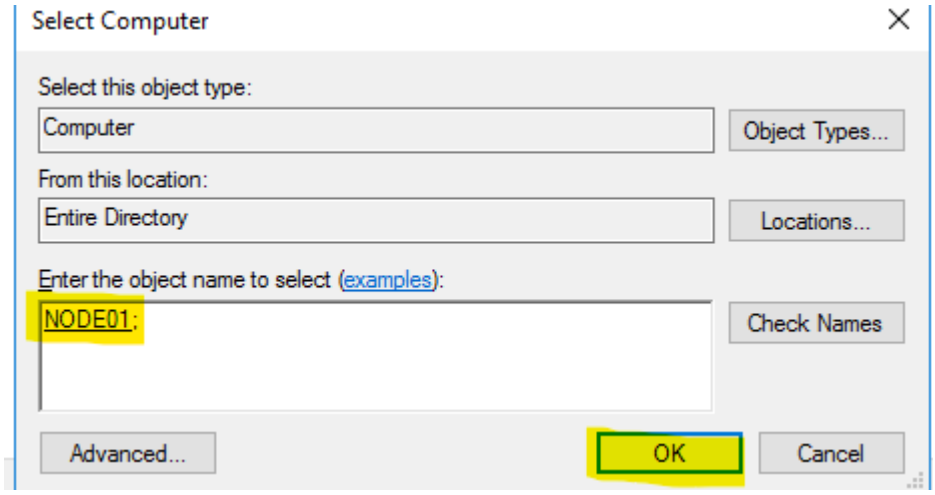
Click on “Add” to access servers on which this iSCSI disk will be accessed.



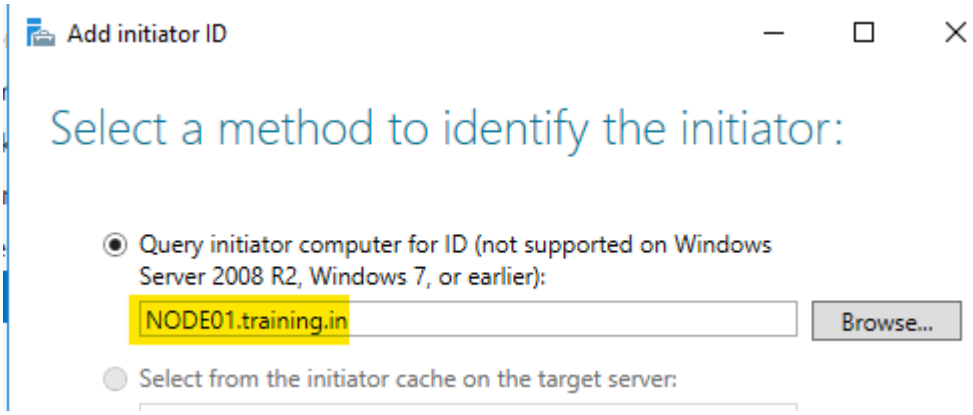
Click on “browse” and type the computer/member names (in my case, Node01 & Node02)



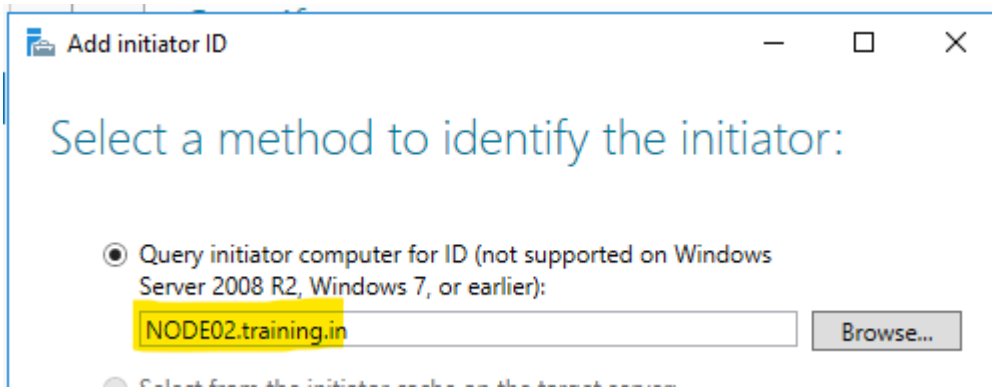
Search both names one by one & then click on OK.



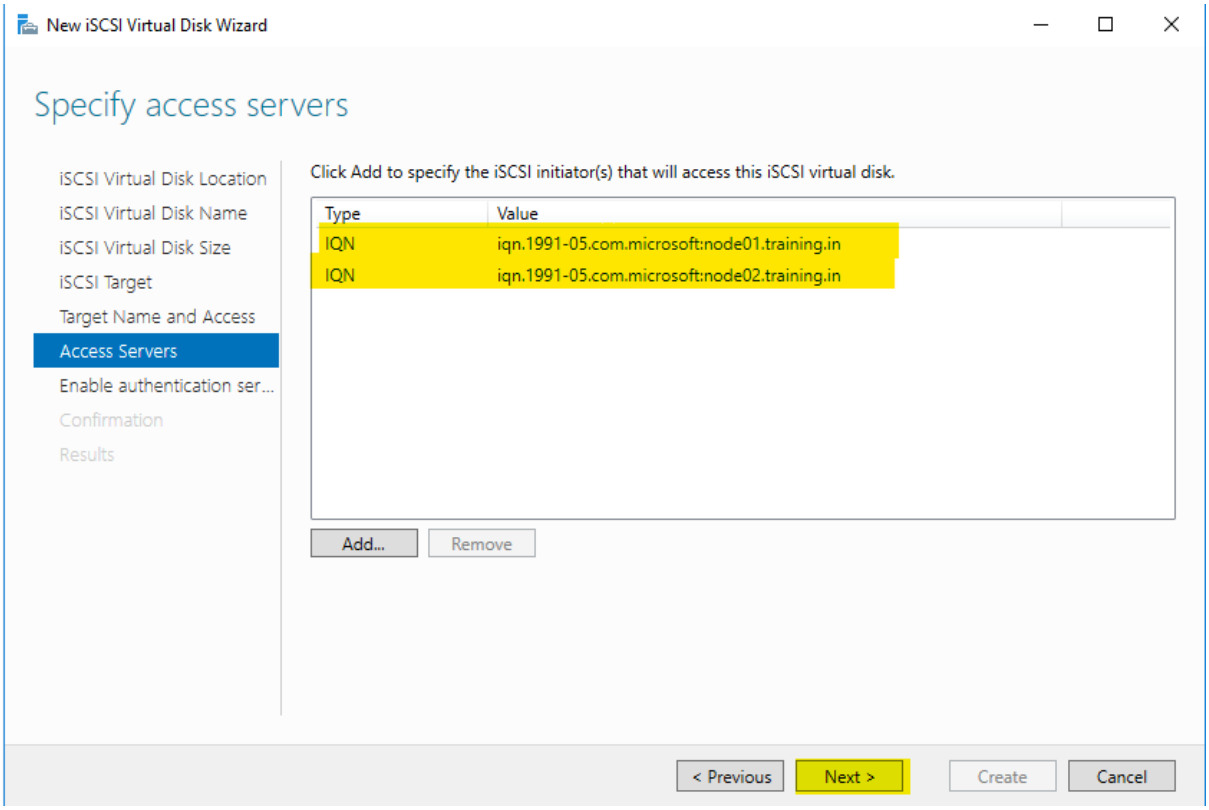
Verify:



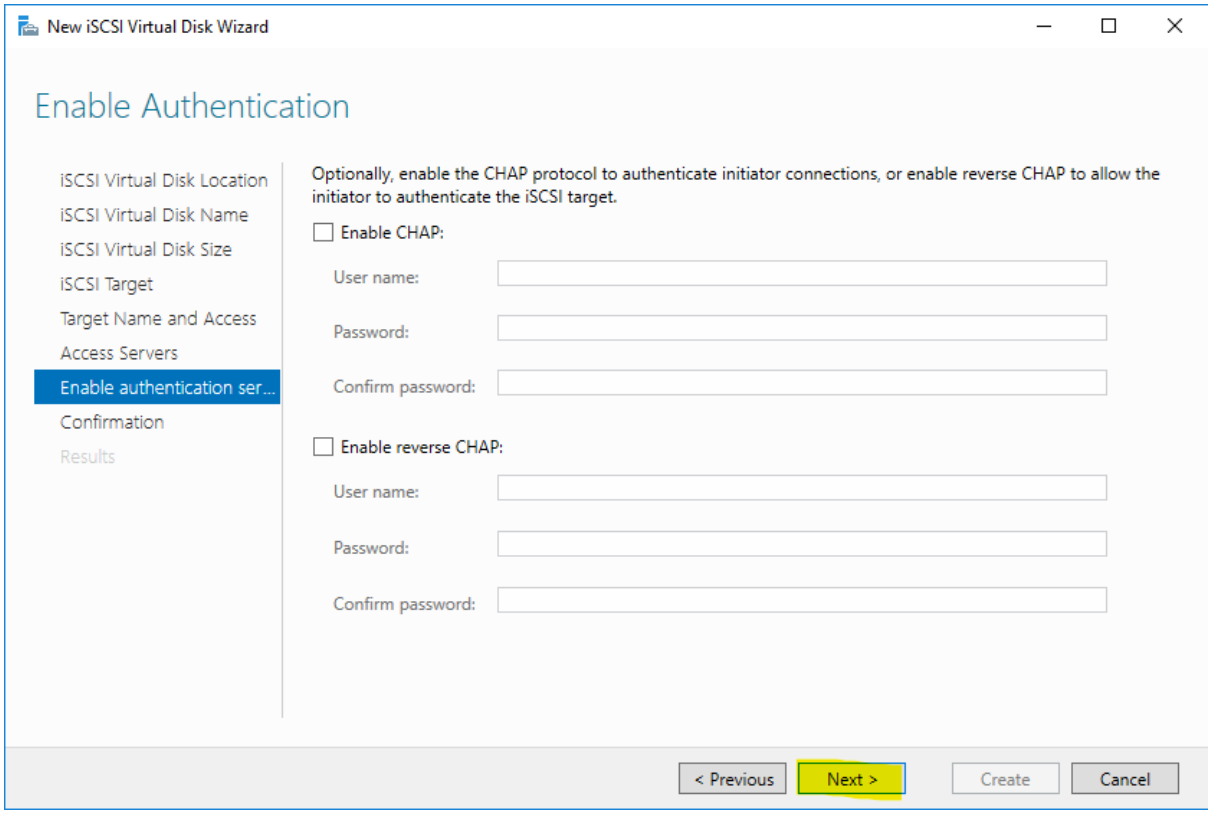
Similarly, select Node02



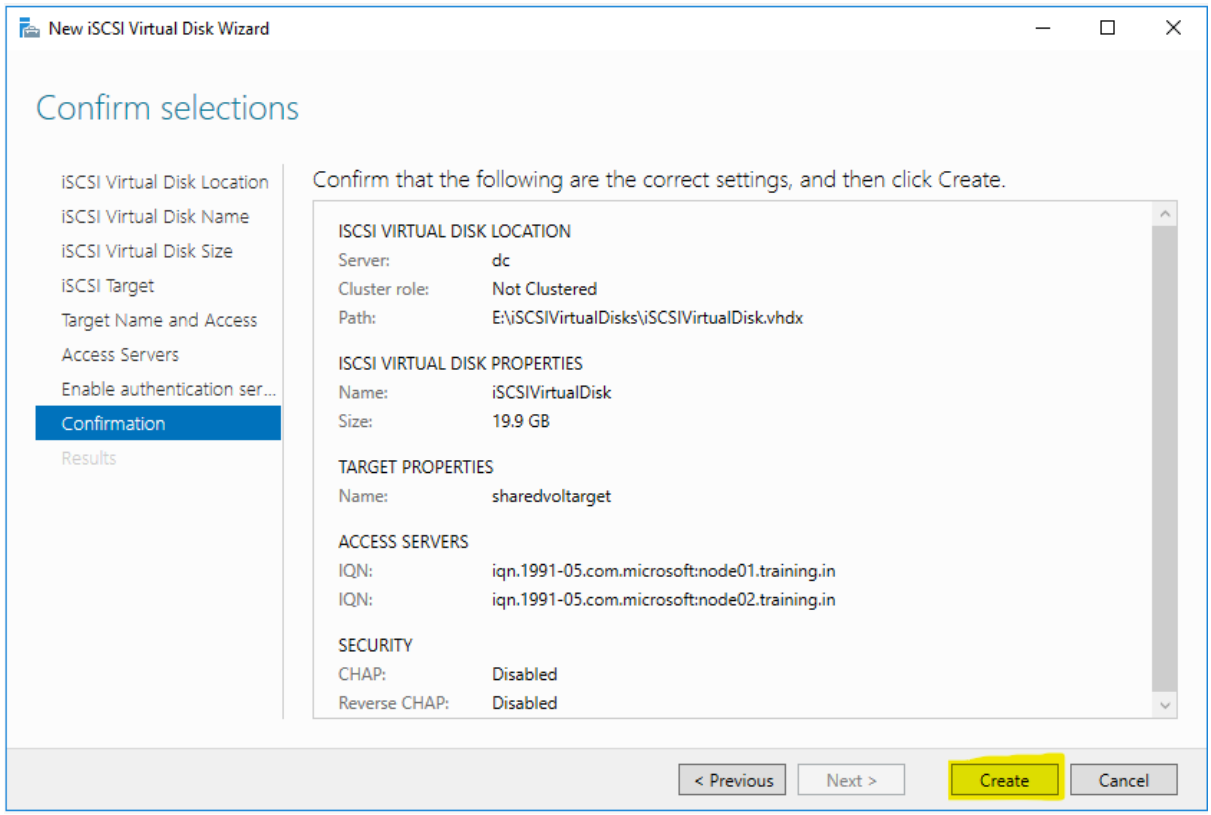
Verify:



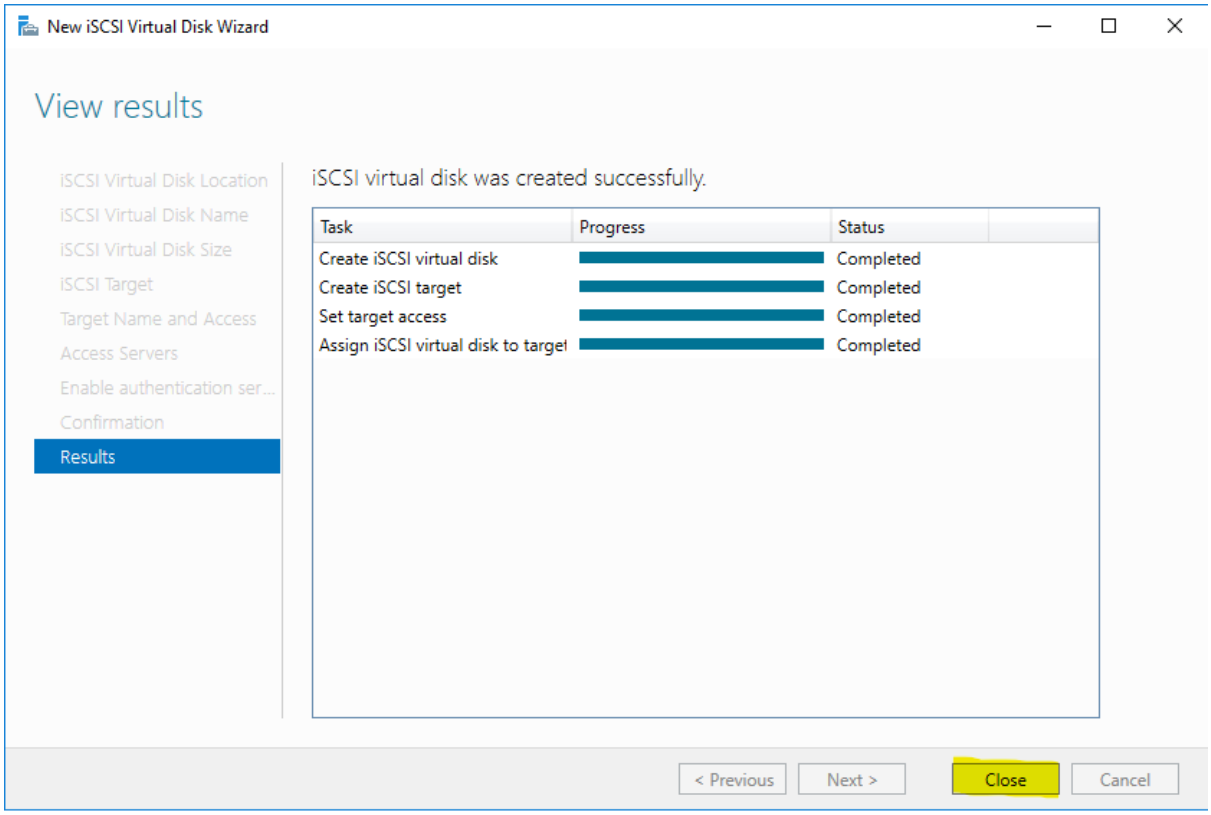
Leave authentication and click on Next



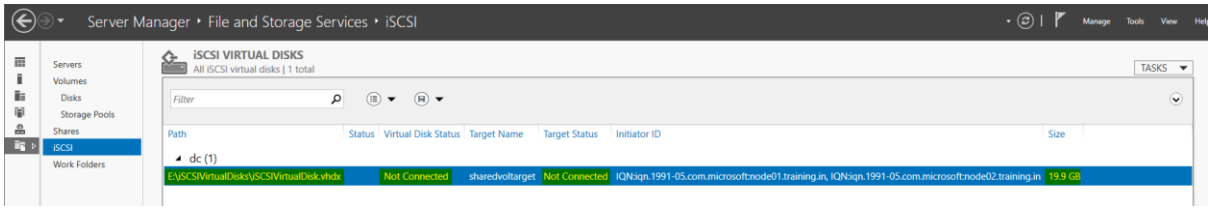
Verify & click “create” button.



Once all tasks are completed successfully, close the prompt.

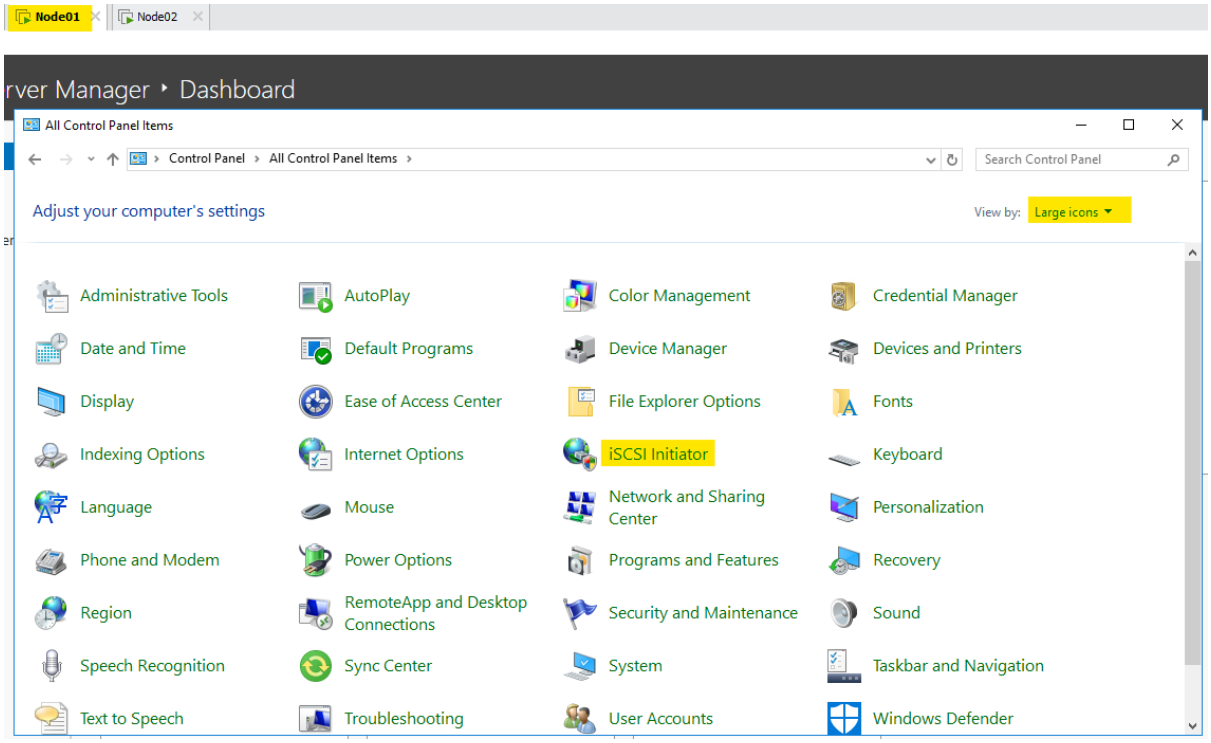


Verify the dashboard, it says “Virtual Disk Status” as “Disconnected”

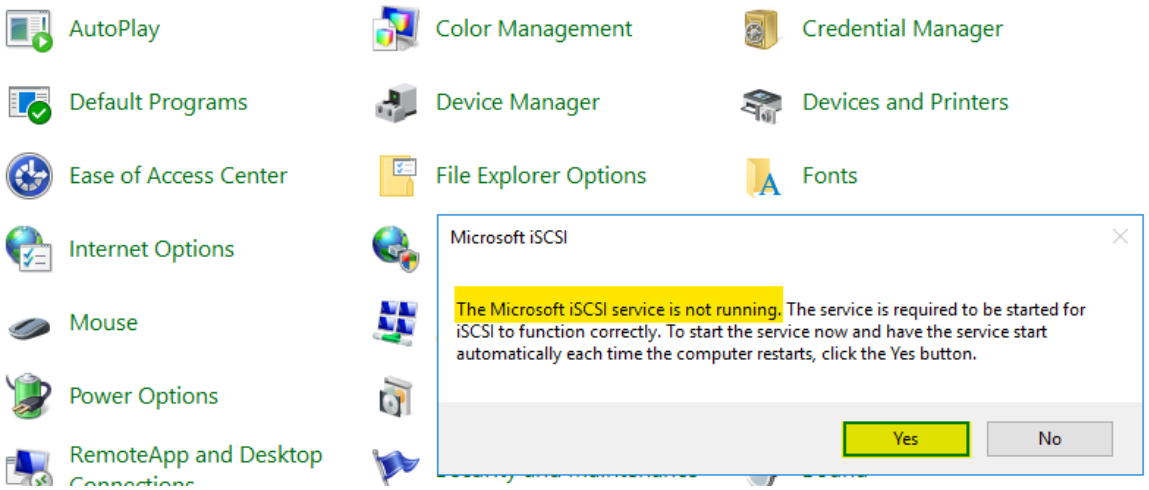


This is expected output as we need to access this on both nodes one by one.

Switch to Node01 and configure iSCSI using control panel (View by: Large icon)

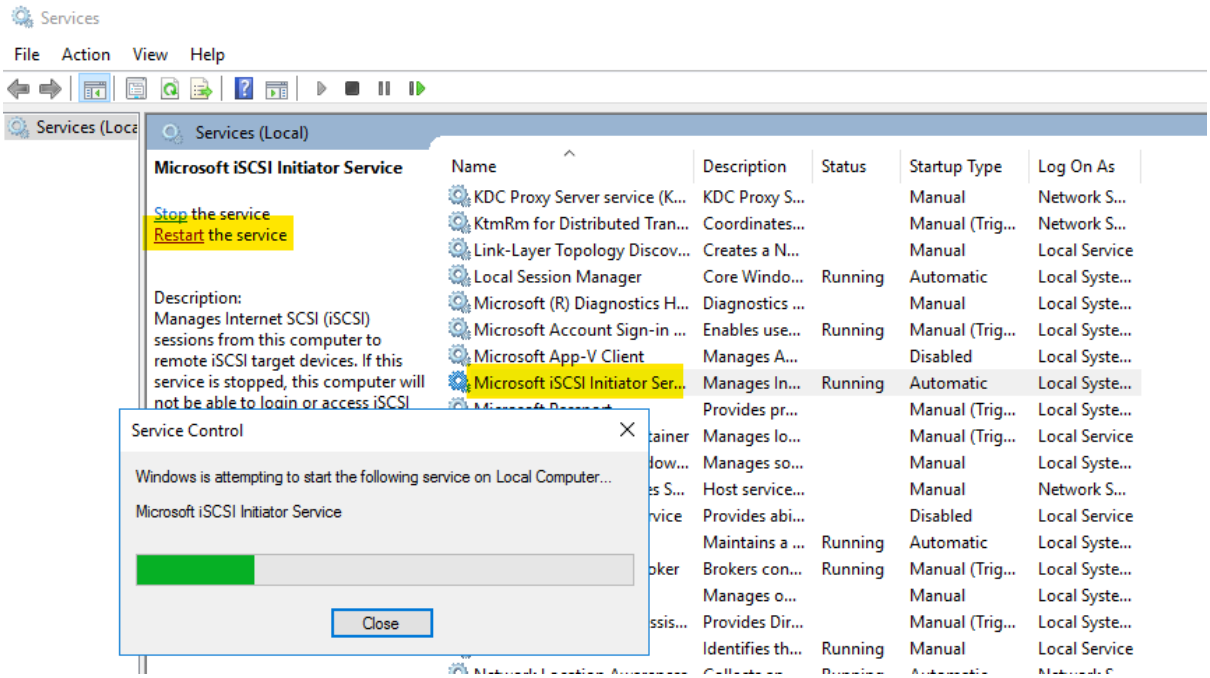


In case you get the below error:

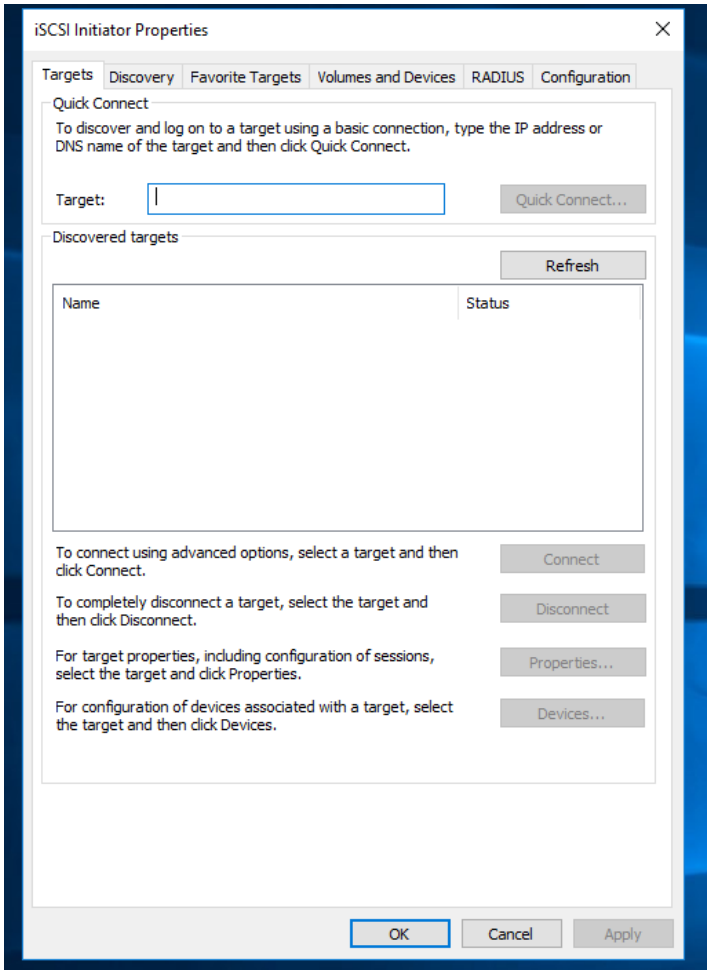


Then start the service,

Services.msc → search for “” & start/restart the service

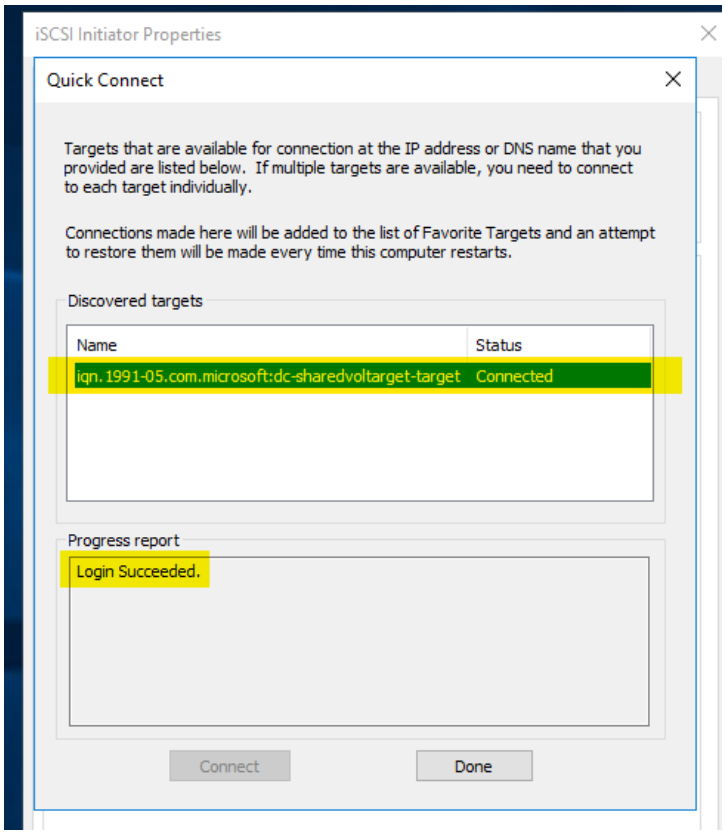


Then again go to control panel → iSCSI initiator.

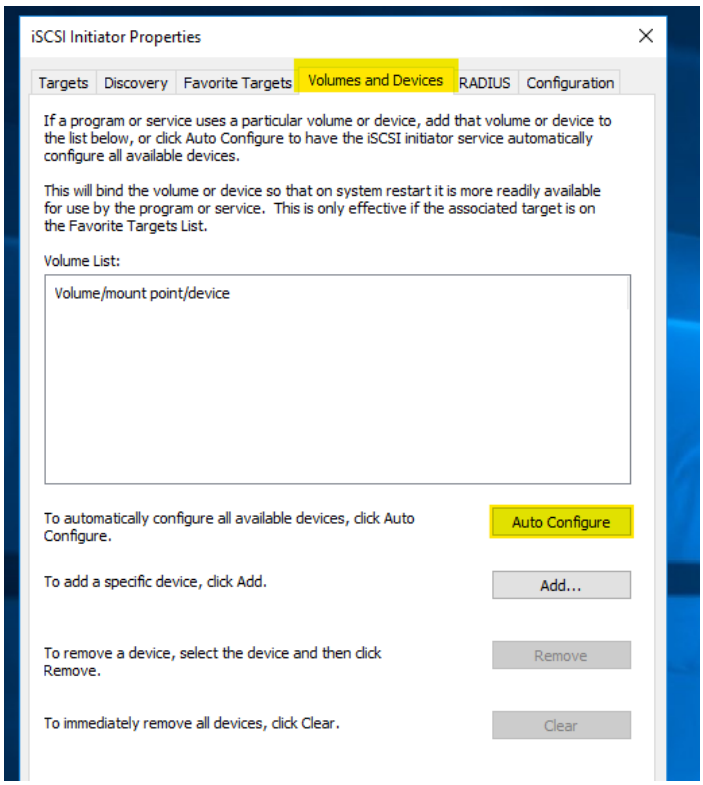


Go to target and fill the iSCSI target source on both Nodes (01 & 02) & click on quick connect:

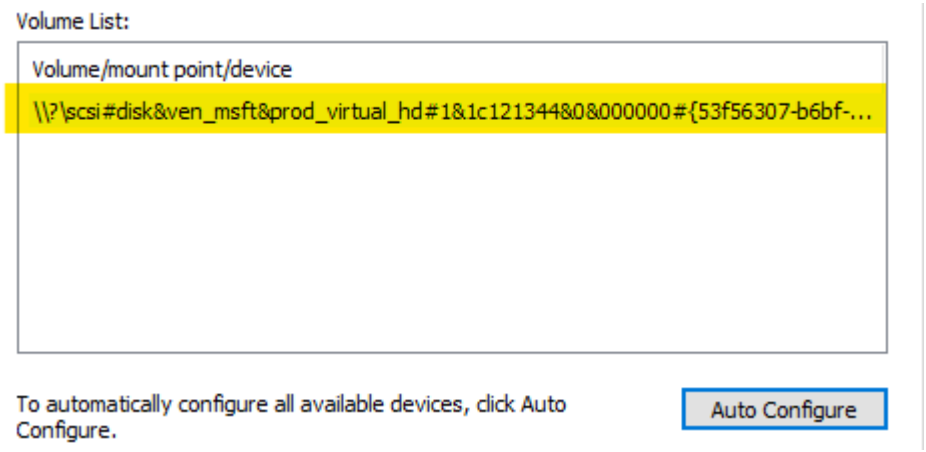
In target, type your domain controller name (dc in my case) & click on quick connect. It must show “login successful” and click on Done.



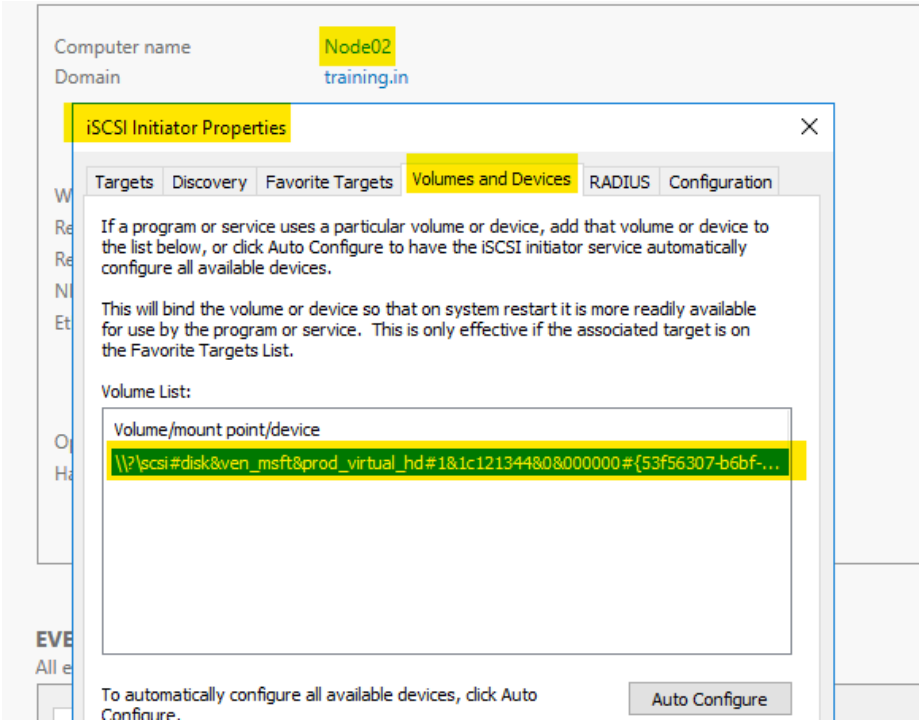
After this, click to “Volumes and Devices” tab and click on “autoconfigure” button.



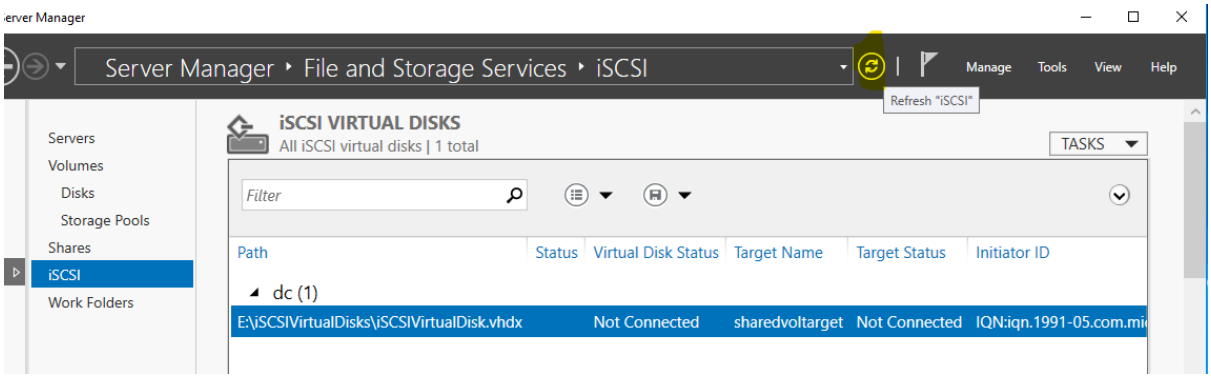
Verify and then click on OK.



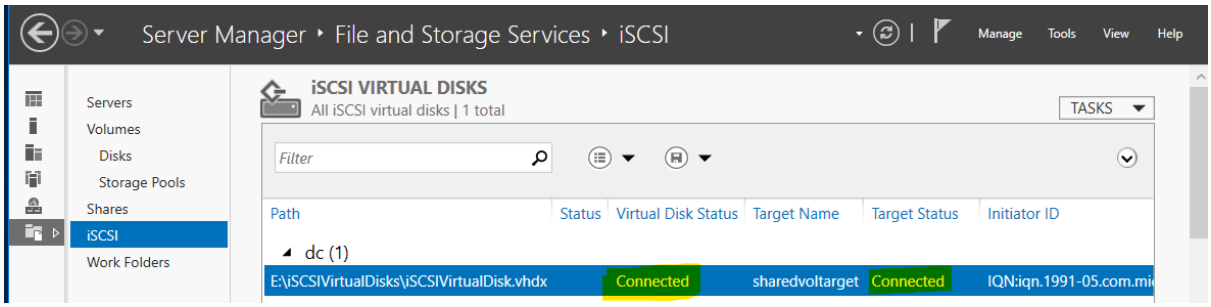
Perform the similar on Node02 and verify.



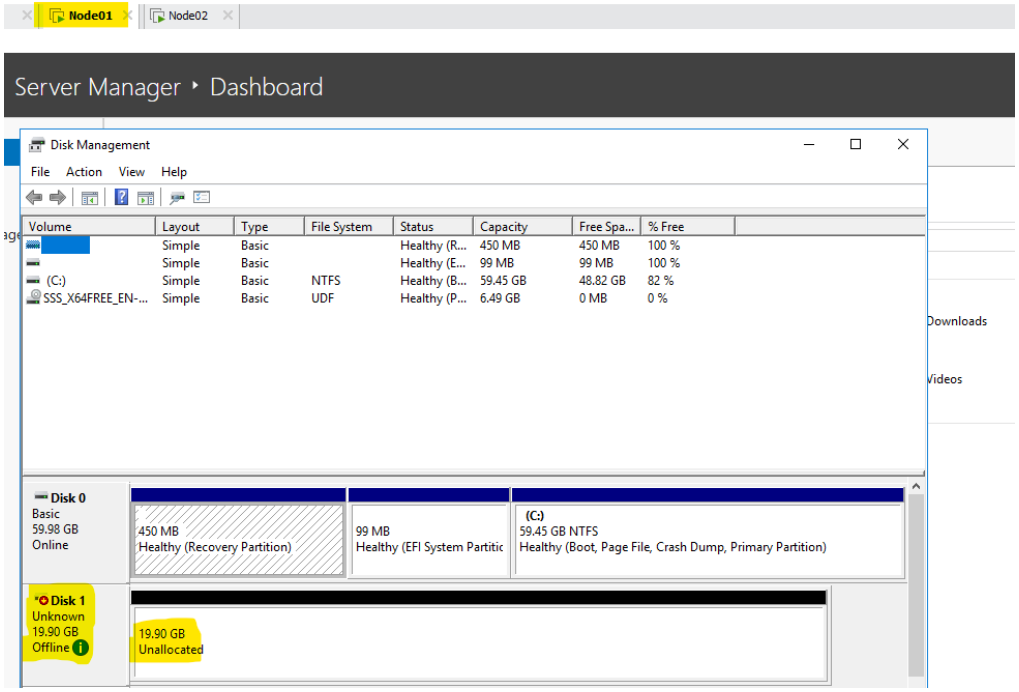
Switch to DC



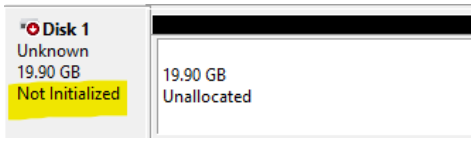
And refresh the dashboard



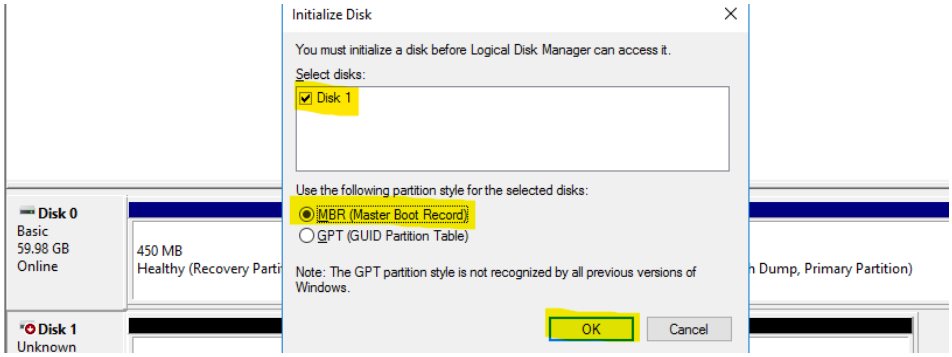
Once it shows connected, switch to Nodes one by one and configure disk using diskmgmt.msc



Right-click on Disk 1 → Online

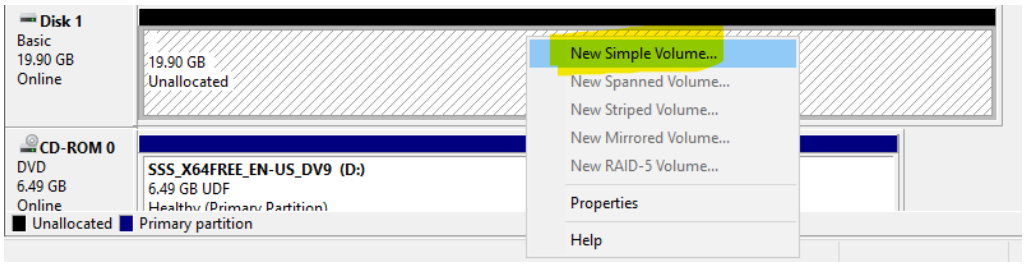


Right-click on Disk 1 → Initialized Disk & select MBR.

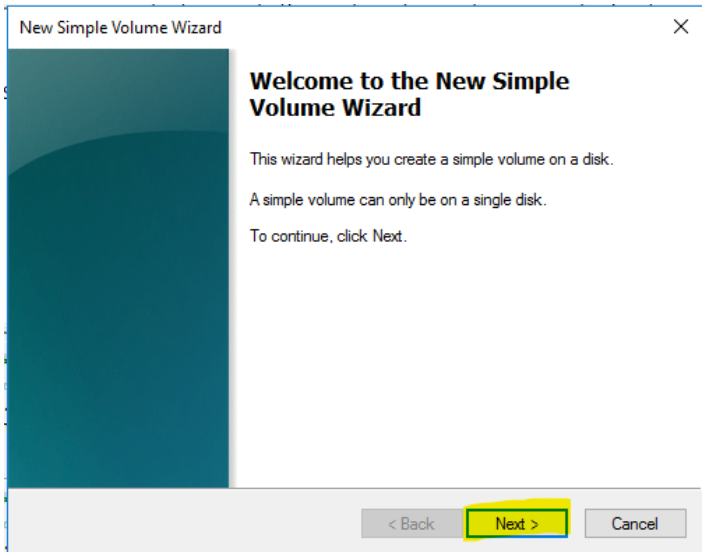


Once initialized, create new volume from this disk.

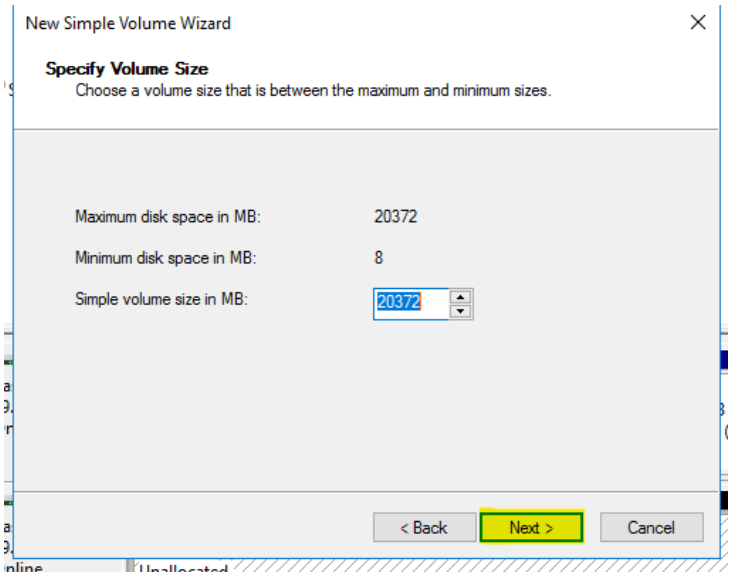
Right-click on the ‘unallocated’ area & click on New Simple Volume…



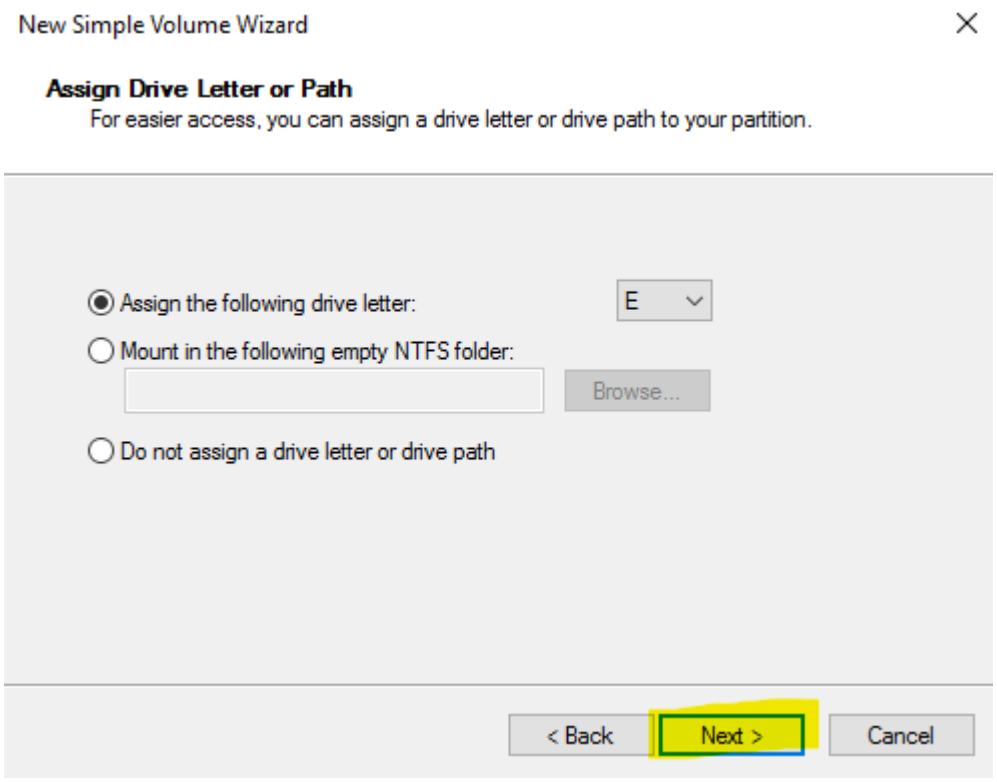
Click on Next on “Welcome Wizard”



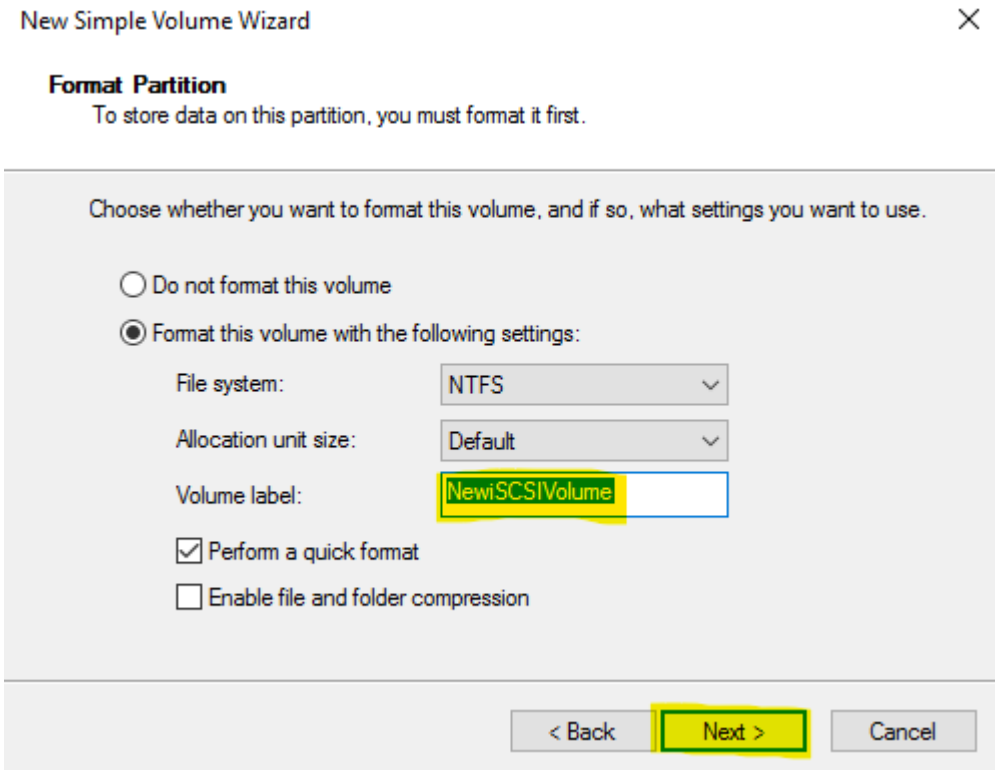
Set the disk size and click on Next.



Allocate a mount point:

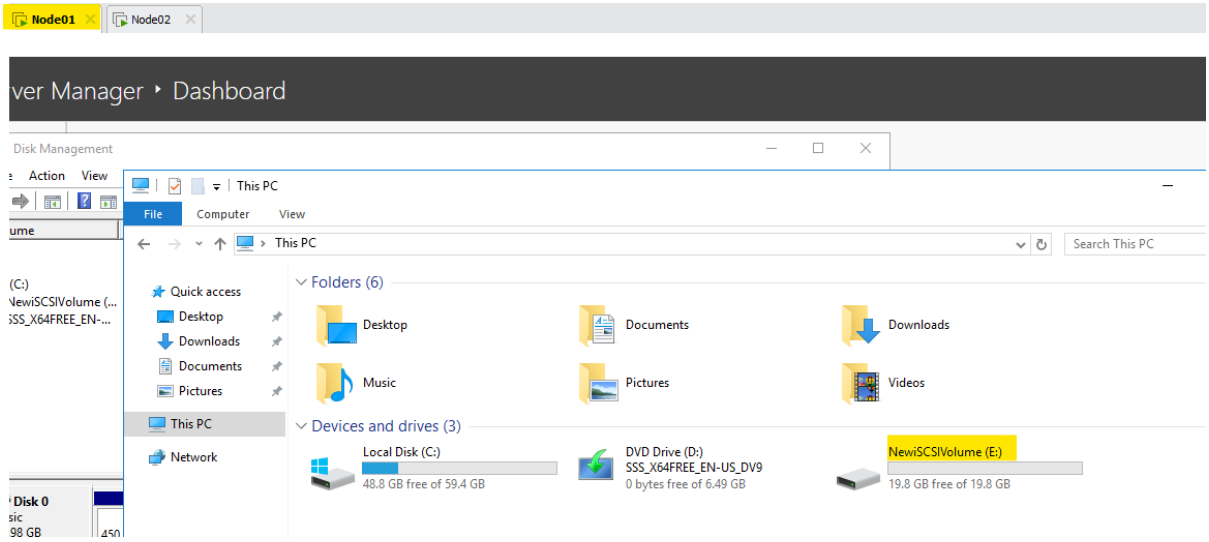


Give a disk name

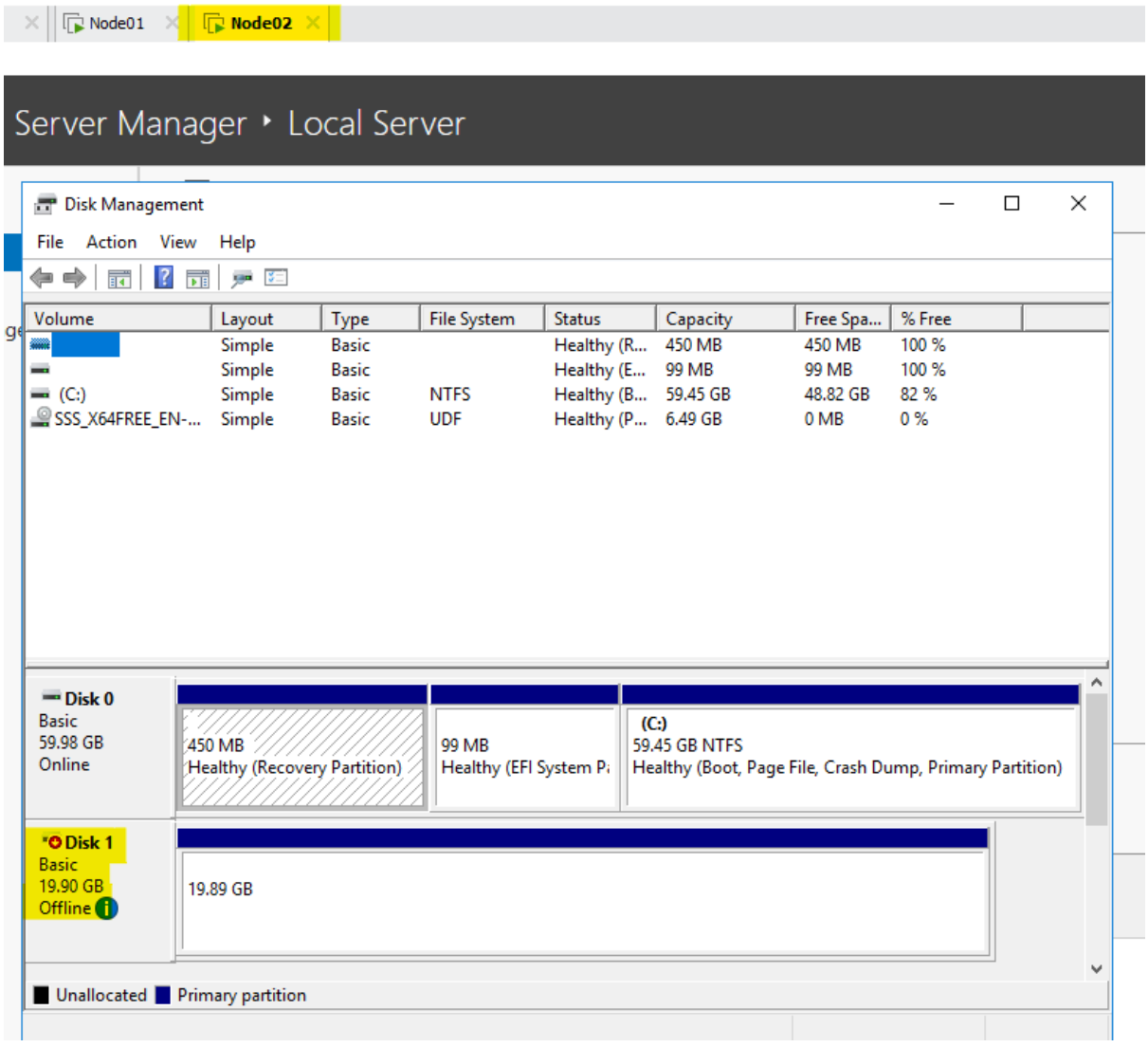


And click on Next & then Finish.

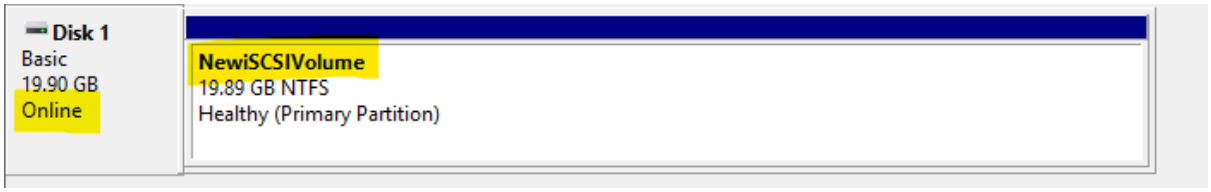
Verify on Node01



Similarly, on Node02, go to diskmgmt.msc and initialize size.

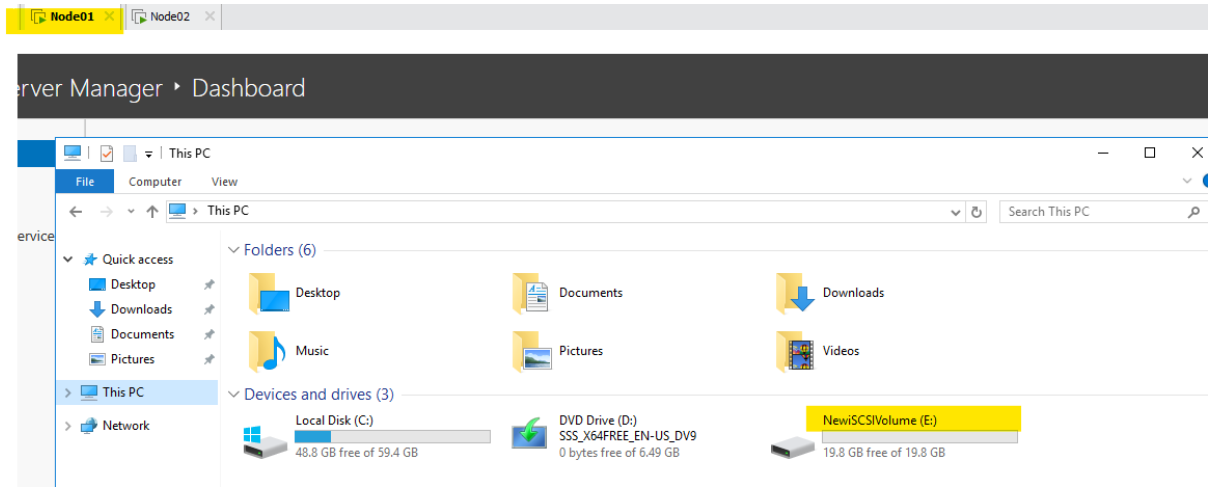


Disk will be automatically present after making disk “online”

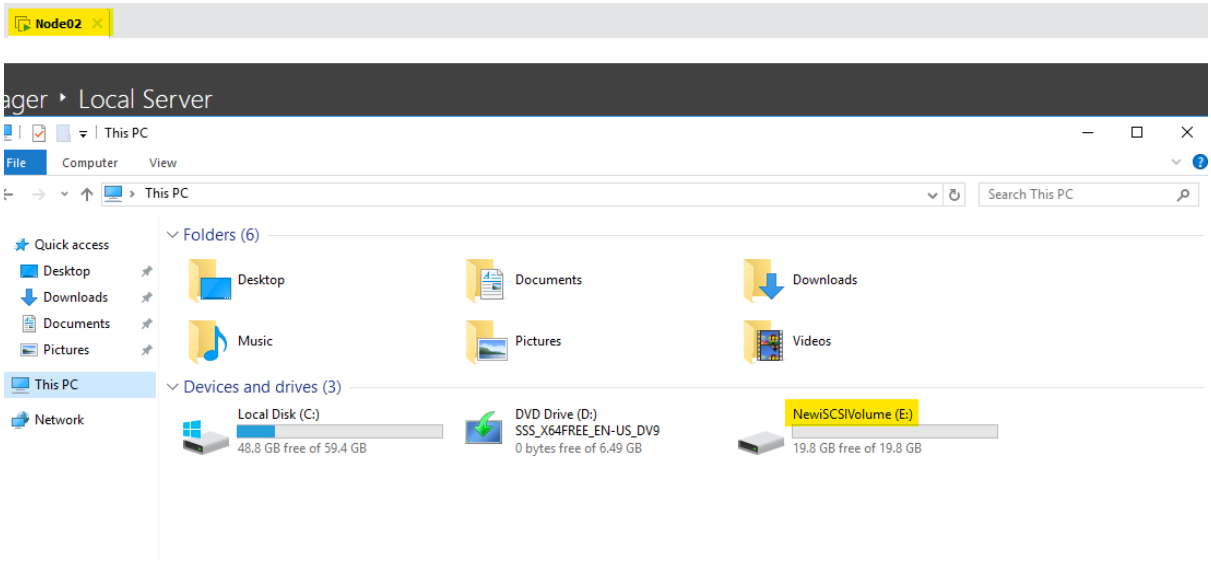


Go to This PC and verify on Node01 & Node02.

Node01



Node02



Note – If the same disk is present on both nodes, it means that iSCSI is configured successfully.

Configuring NFS (Network File Sharing) on DC

What is Network File Sharing (NFS)?

NFS (Network File System) is a protocol developed by Sun Microsystems that allows a computer (client) to access files over a network as if they were on its local hard drive. It's primarily used in Unix/Linux environments but can also be configured on Windows.

What is an NFS Server?

An NFS Server is a system that hosts shared directories or files and makes them available over the network using the NFS protocol. Clients mount these shared directories and access the files transparently.

How Does NFS Work?

- The NFS Server exports one or more directories.
- The NFS Client mounts the exported directories.
- File operations (read, write, execute) on mounted directories are sent over the network using NFS protocol calls.
- The server responds to these calls, allowing remote file access.

Key Concepts and Terms in NFS

Term	Definition
Export	The directory or filesystem that the NFS server shares. Defined in the server's /etc/exports file (Linux) or NFS management on Windows.
Mount	The process by which an NFS client connects to an exported directory and attaches it to its own file system tree.
Mount Point	The directory path on the client where the remote NFS share is accessible.
RPC (Remote Procedure Call)	The underlying communication method used by NFS to send file operation requests between client and server.
UID/GID Mapping	NFS uses user IDs (UID) and group IDs (GID) to manage permissions, so client and server must have synchronized or compatible UID/GID mappings.
NFS Versions	Versions include NFSv2, NFSv3, NFSv4. NFSv4 adds stateful operations, security improvements (Kerberos), and better performance.
Stateless vs Stateful	Older versions (v2, v3) are stateless (server doesn't keep track of clients), whereas NFSv4 is stateful.
Portmapper (rpcbind)	A service that maps RPC program numbers to network port numbers, essential for NFS operation.
Anonymous Access	NFS can allow access to unauthenticated users, but it's usually restricted for security.

Term	Definition
Kerberos Authentication	Optional secure authentication method to protect NFS traffic and verify users.

NFS on Windows Server

- Available as a Role/Feature in Windows Server (since 2008).
- Allows Windows servers to share files with Unix/Linux clients using NFS.
- Supports NFS versions 3 and 4.
- Integration with Active Directory for UID/GID mapping.
- Configured via Server Manager or PowerShell cmdlets (New-NfsShare, Grant-NfsSharePermission).

Security in NFS

- Traditional NFS has limited security; relies on client IP and UID/GID.
- NFSv4 supports Kerberos authentication for secure identity verification.
- Firewall and network segmentation recommended to protect NFS traffic.
- Use no_root_squash carefully — it grants root-level access to clients, a security risk.

Advantages of NFS

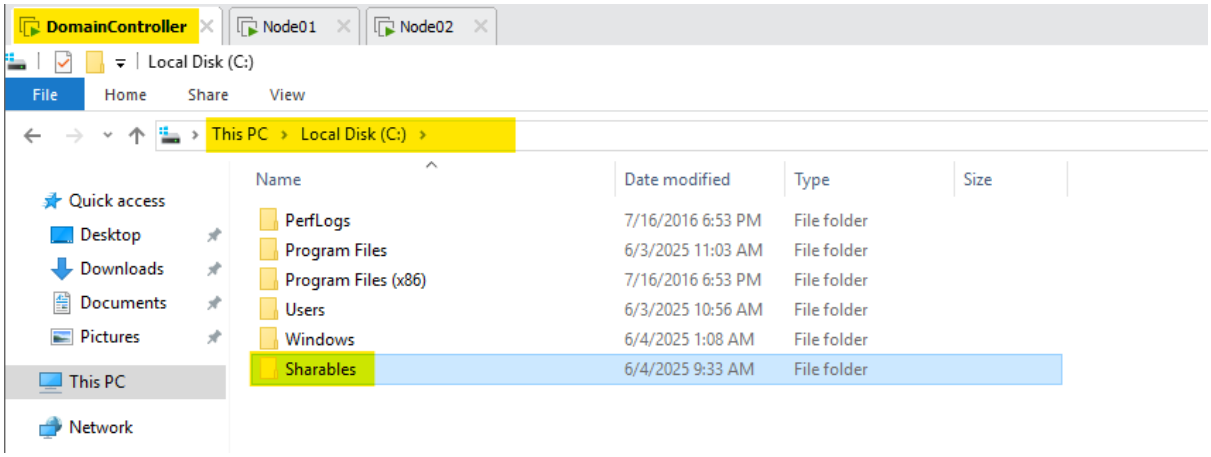
- Transparent remote file access.
- Widely supported on Unix/Linux.
- Integrates well with existing Unix permissions.
- Lightweight protocol, efficient for network file sharing.

Limitations

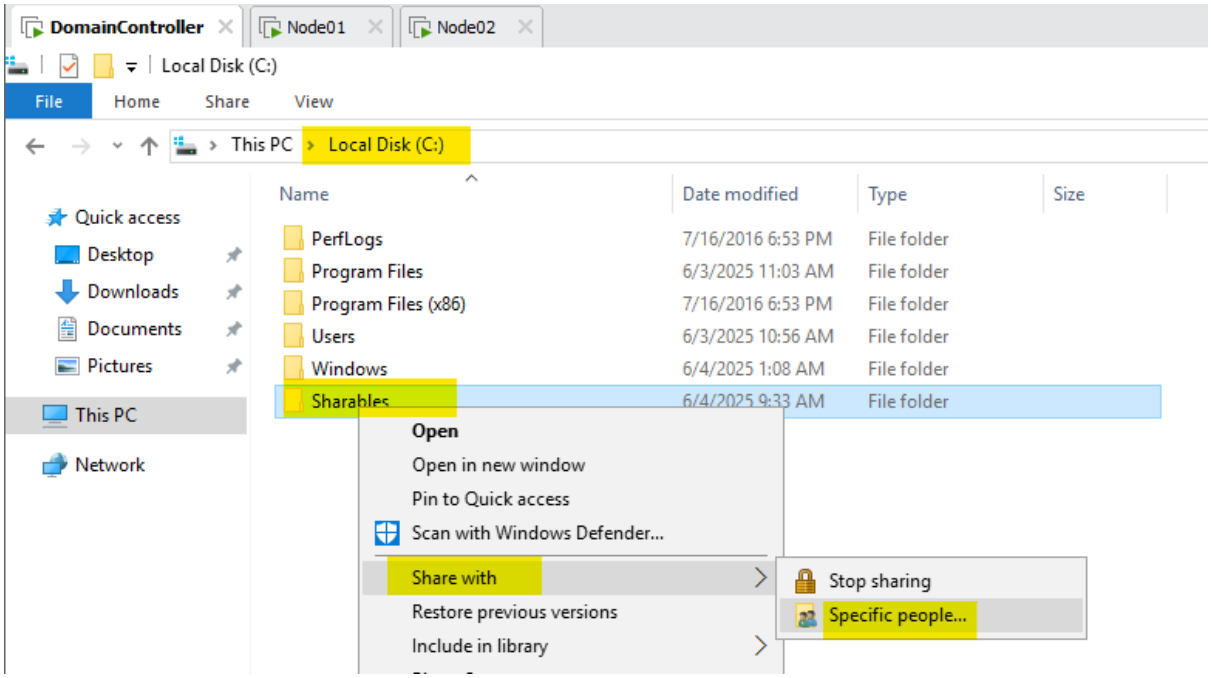
- Performance depends on network speed.
- Security weaker than SMB/Active Directory environments unless Kerberos enabled.
- Requires careful UID/GID synchronization

Creating NFS Folder and accessing it on a remote system

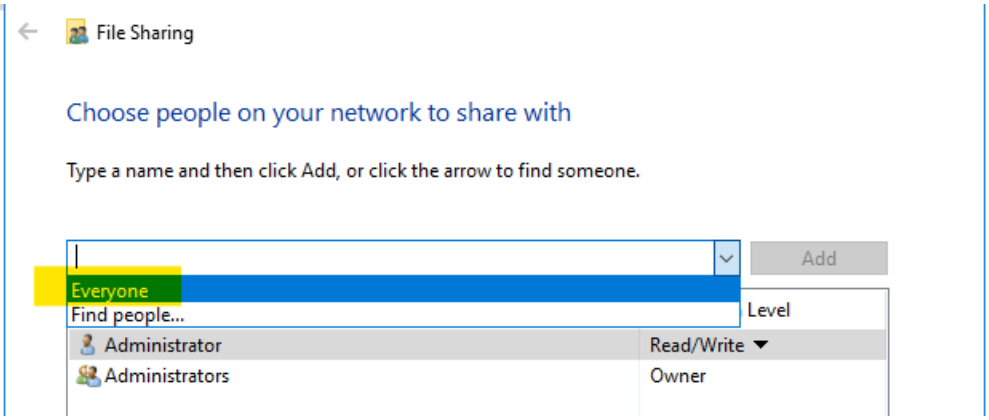
Go to DC and create a new folder under C:\ drive as “Sharables”



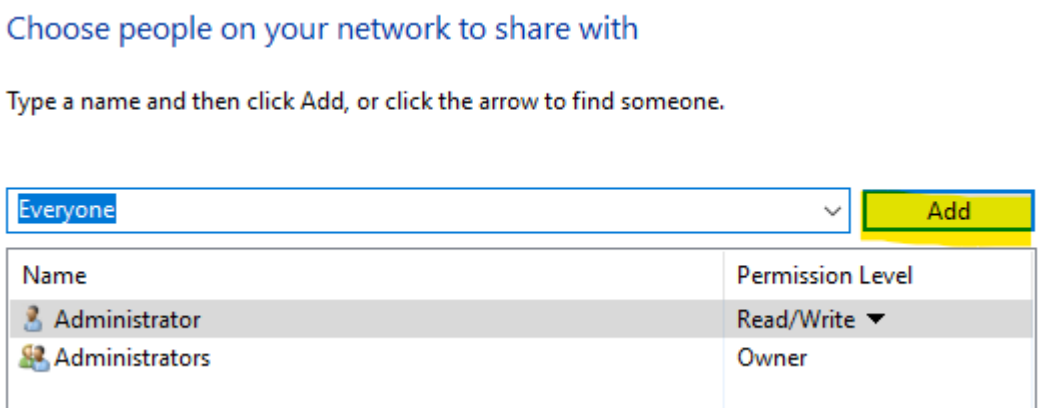
Right-click on the Sharables folder → “Share with” → “Specific People…”



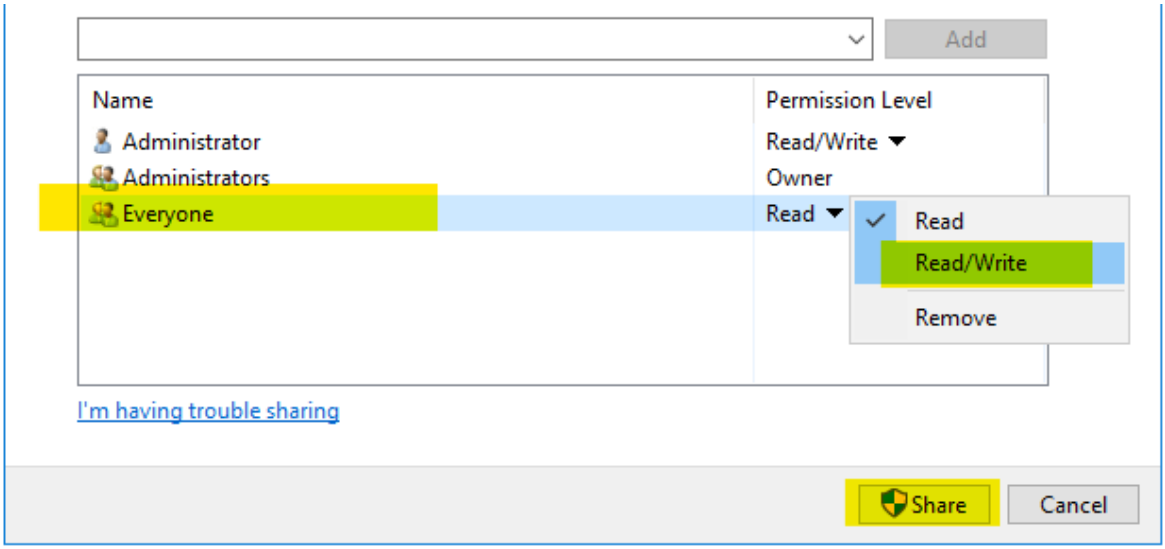
Select “Everyone”



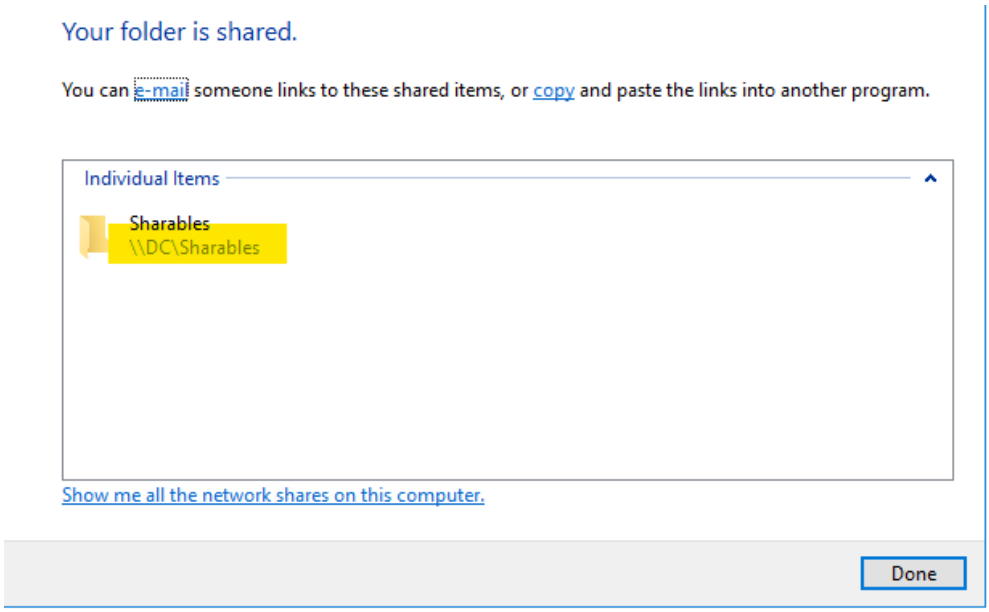
Click on “Add” button



Click on drop down and give Read/Write permission

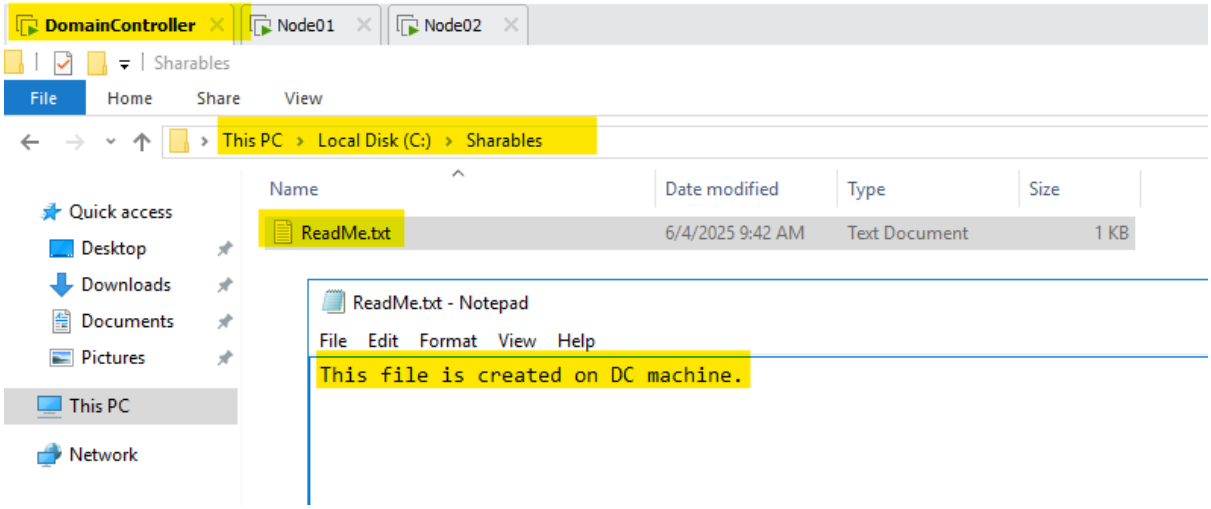


And click on “Share” button.



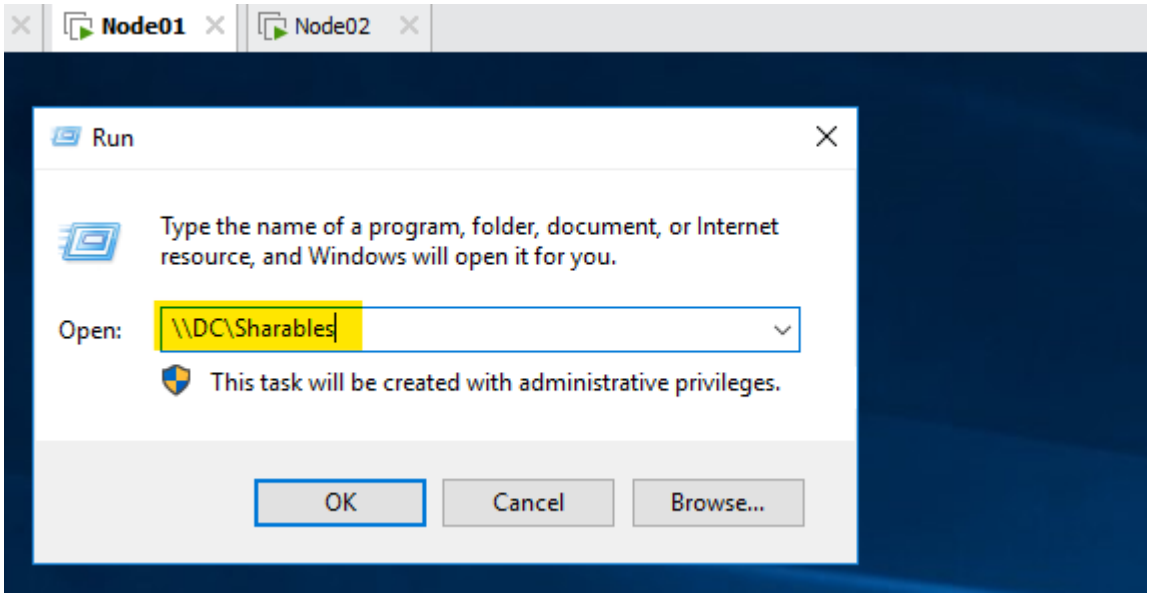
Note – copy this path (\\DC\Sharables), as this will be useful on Node01 and Node02.

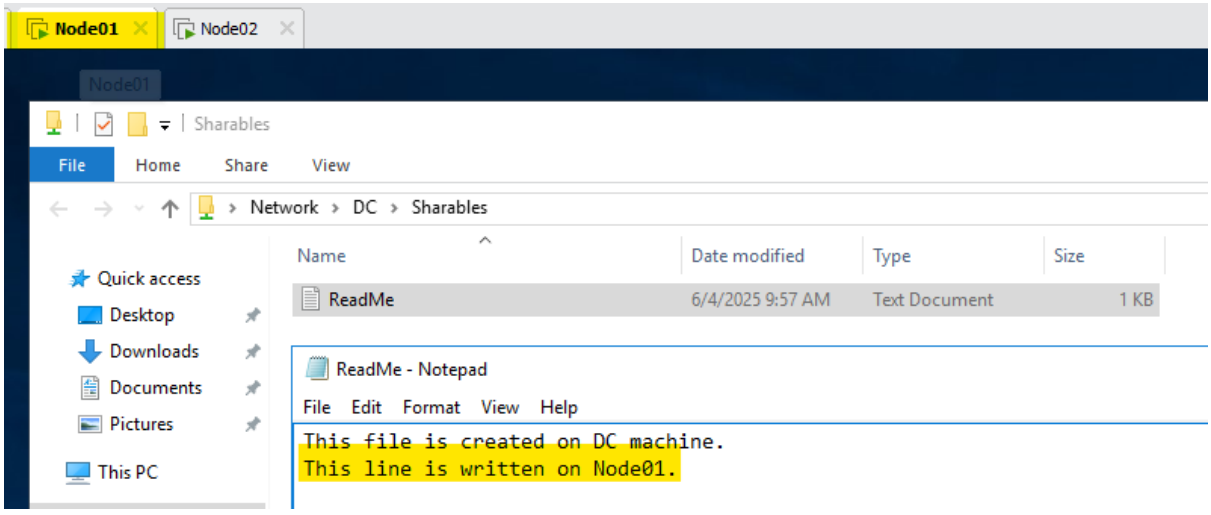
Create some files and folders within this NFS shared folder.



Now access this shared folder on Node01 and Node02.

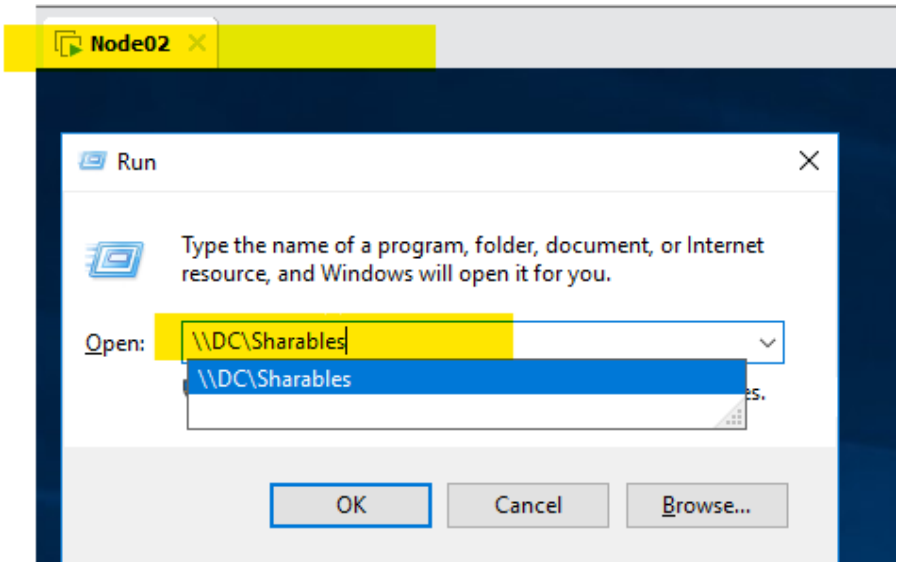
Run → \\DC\Shareables

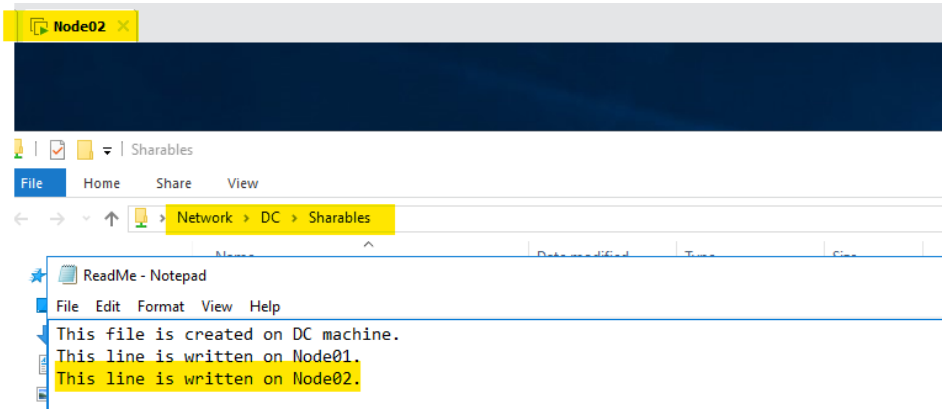




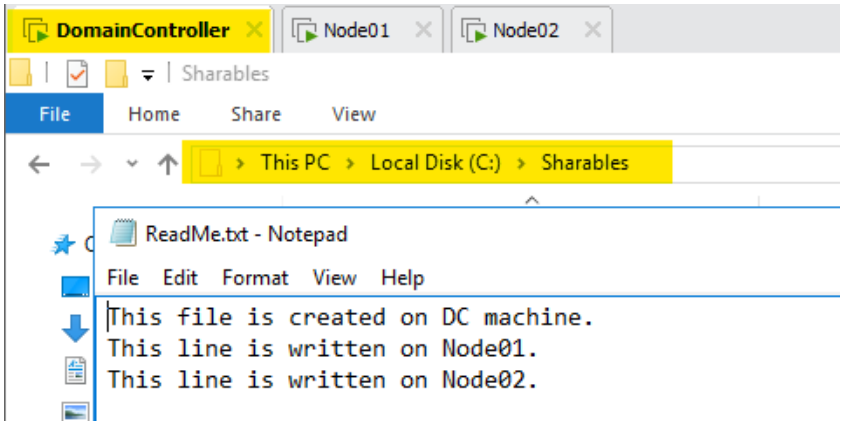
Now access this shared folder on Node01 and Node02.

Run → \\DC\Shareables





Verify on DC.



Note – End of NFS

Network Load Balancer (NLB)

What is a Network Load Balancer (NLB)?

- A Network Load Balancer (NLB) is a device or software that distributes incoming network traffic across multiple servers (called nodes or hosts) to ensure:
    - High availability
    - Scalability
    - Fault tolerance
- It helps prevent any single server from becoming a bottleneck or point of failure by balancing load intelligently.

How Does NLB Work?

- Incoming client requests (TCP/UDP/IP traffic) arrive at the NLB's virtual IP address.
- The NLB distributes requests to one of the available servers based on a load balancing algorithm.
- It monitors the health of servers and removes unresponsive servers from the pool.
- Clients interact with the NLB IP, not directly with individual servers.

Key Components and Terms in NLB:

Term	Description
Cluster	A group of servers (hosts/nodes) participating in load balancing.
Virtual IP (VIP)	The single IP address assigned to the NLB cluster that clients connect to.
Host Priority	A numeric value assigned to each host to control the order in which hosts get traffic or take over if others fail.
Affinity	Defines how client requests are mapped to servers:- **None:** Each request can go to any server.- **Single:** Requests from the same client IP always go to the same server.- **Class C:** Requests from clients in the same Class C subnet go to the same server.
Load Balancing Algorithm	Method NLB uses to distribute traffic:- **Round Robin:** Distribute evenly.- **Least Connections:** Send to server with fewest active connections.- **Weighted:** Based on server priority or capacity.
Port Rules	Define which ports are load balanced and how traffic on those ports is handled.
Heartbeat	Periodic signals sent between cluster hosts to check health and availability.
Convergence	The process where cluster nodes synchronize and adjust when a node joins, leaves, or fails.

Microsoft NLB (Windows Server)

- Built-in feature available on Windows Server editions.
- Supports both unicast and multicast network modes.
- Supports affinity settings for stateful applications.
- Can load balance TCP and UDP traffic.
- Used commonly for web servers, terminal servers, and application servers.

Modes of Operation

- Unicast Mode
    - Each NLB node uses the same MAC address (the cluster MAC). Good for small clusters but may cause switch flooding.
- Multicast Mode
    - NLB nodes have both unique and multicast MAC addresses. Better for large clusters or complex switches.
- IGMP Multicast Mode
    - Uses IGMP protocol to control multicast group membership, reduces switch flooding compared to regular multicast.

Common Use Cases

- Load balancing web servers (HTTP/HTTPS)
- Load balancing terminal servers / remote desktop servers
- Distributing application servers
- Increasing fault tolerance in multi-node environments
- Managing high traffic scenarios

Benefits of NLB

- High availability: Traffic automatically redirected if a node fails.
- Scalability: Add/remove nodes to scale out/in.
- Cost-effective: Uses existing network infrastructure.
- Transparent: Clients use a single IP, unaware of backend complexity.

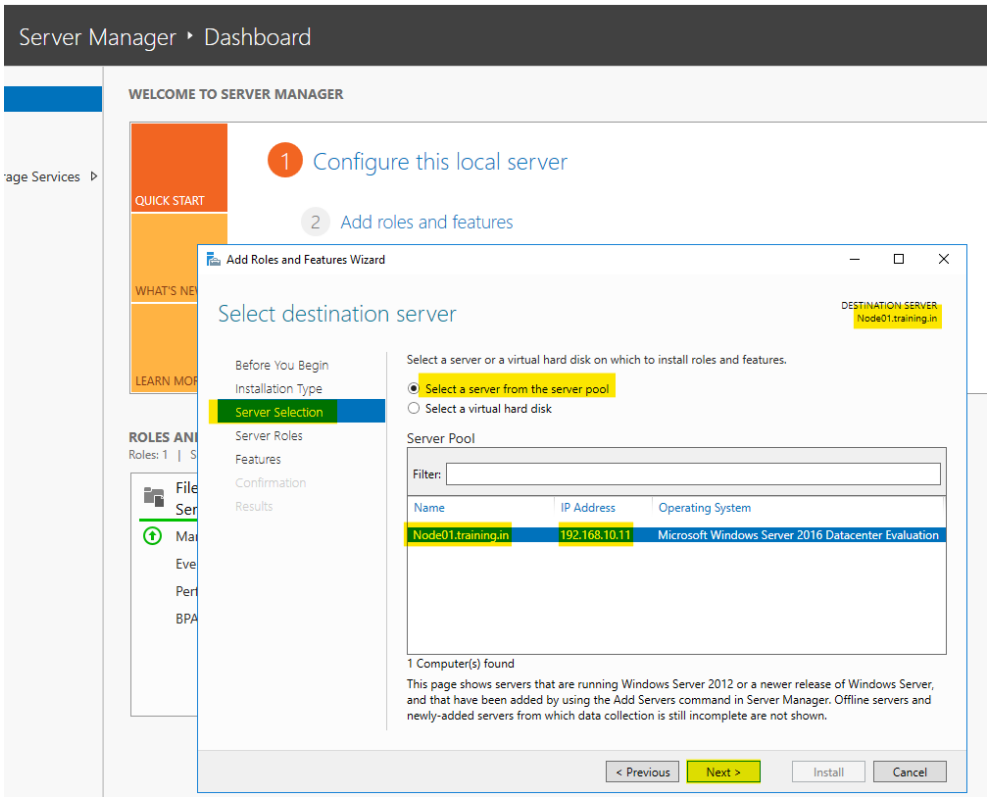
Limitations and Considerations

- Works at Layer 4 (Transport Layer) — does not inspect HTTP content or do advanced routing.
- Not ideal for stateful applications unless affinity is used.
- May require careful network switch configuration (especially with multicast).
- Does not provide SSL offloading or advanced Layer 7 features (use Application Load Balancer or reverse proxy for that).

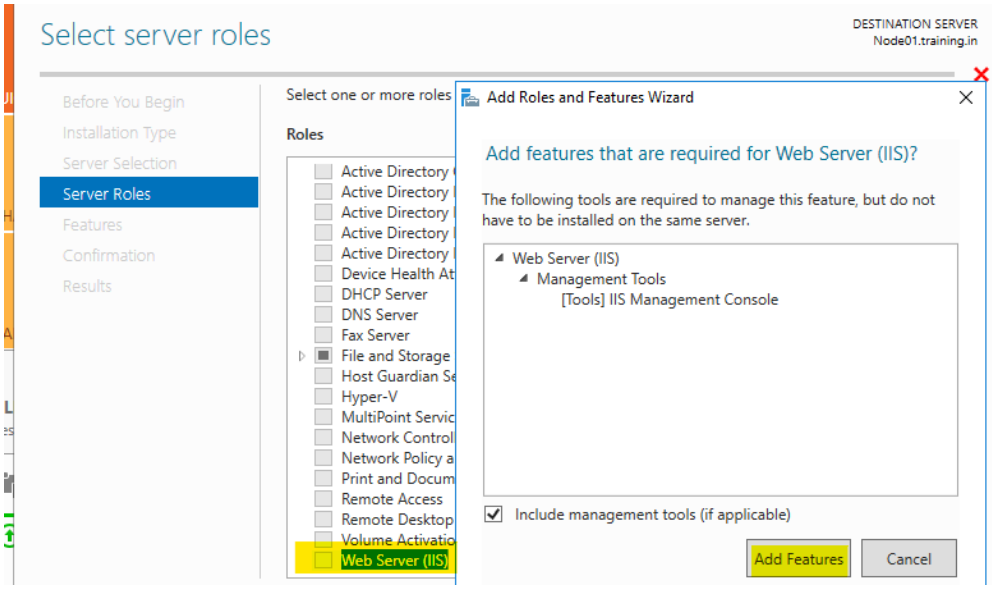
*Note – Uninstall/remove **failover clustering** before NLB (if created already) and reboot.*

Installing IIS web server role on each Node (01 & 02):

Node 01 → Server manager dashboard page → add roles and features

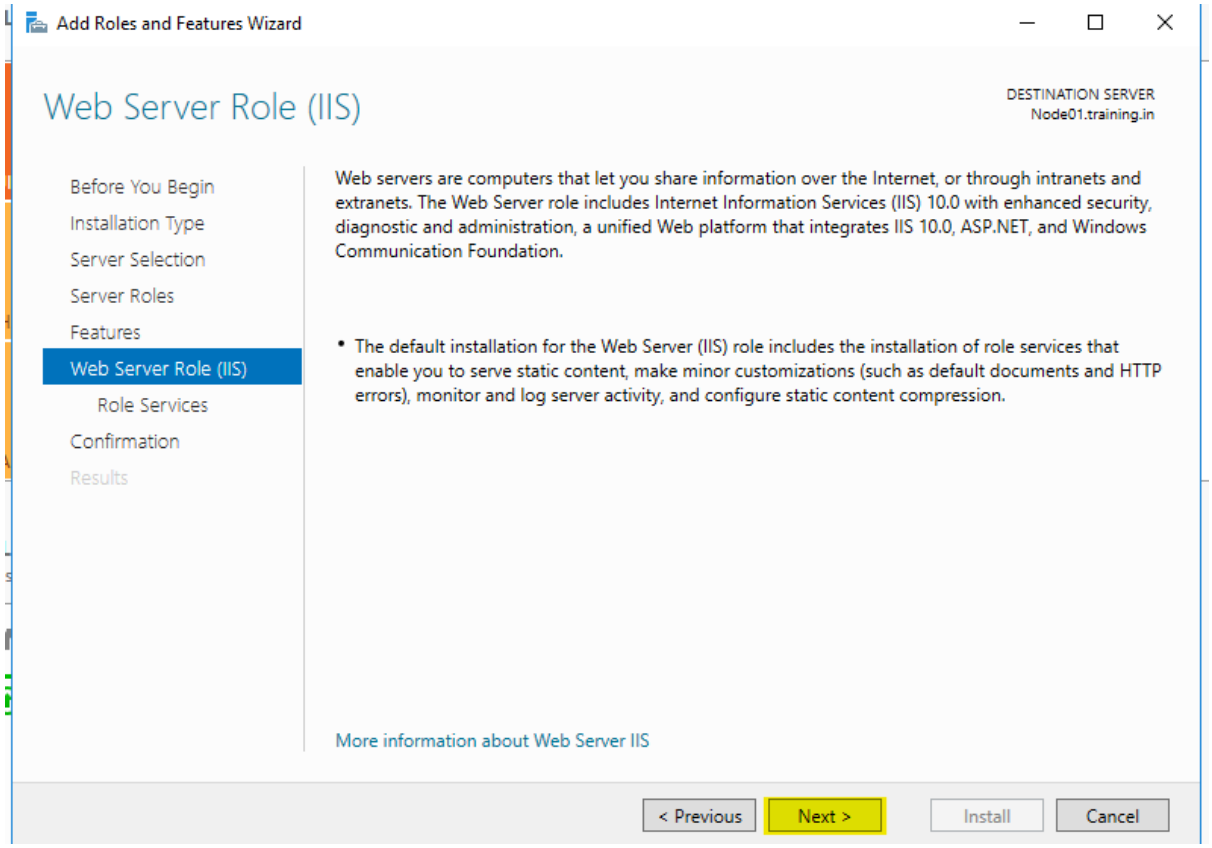


Select “Web Server (IIS)” role on Node01 and add all required features

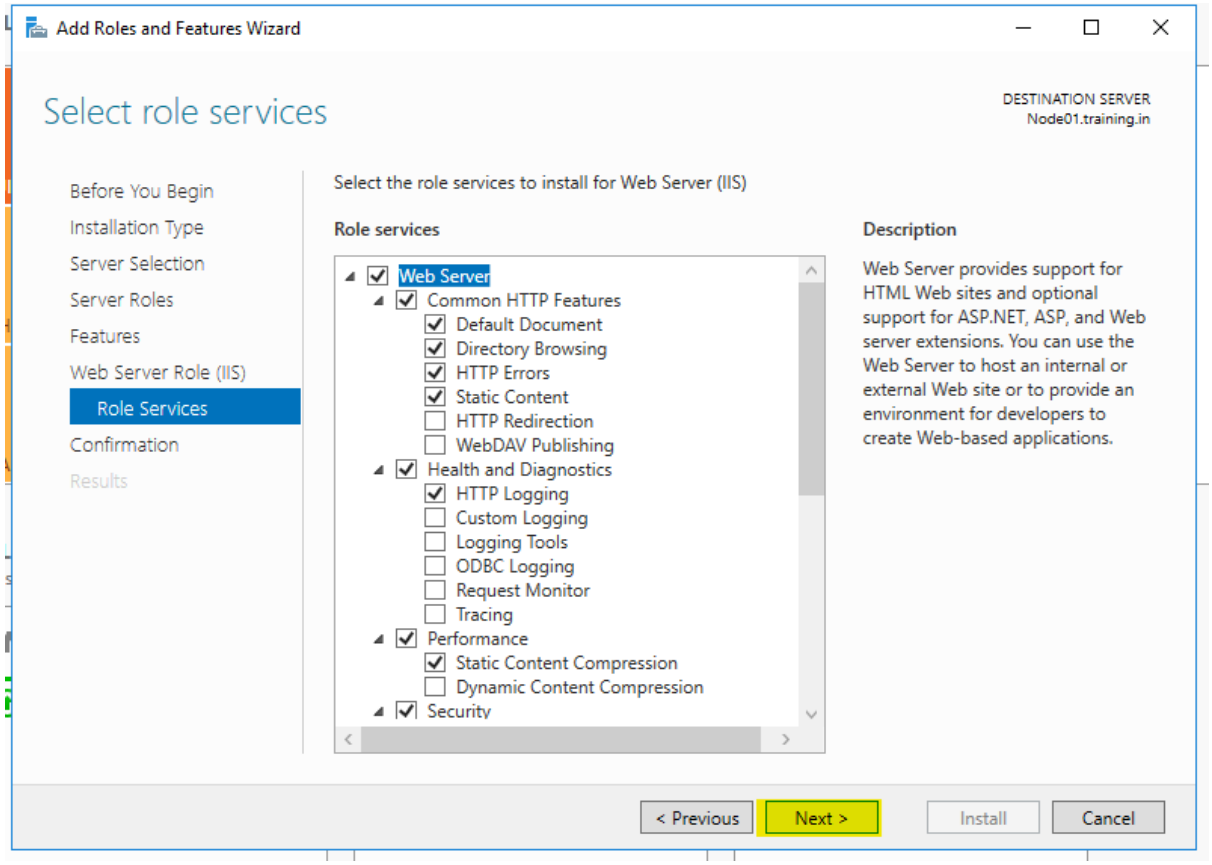


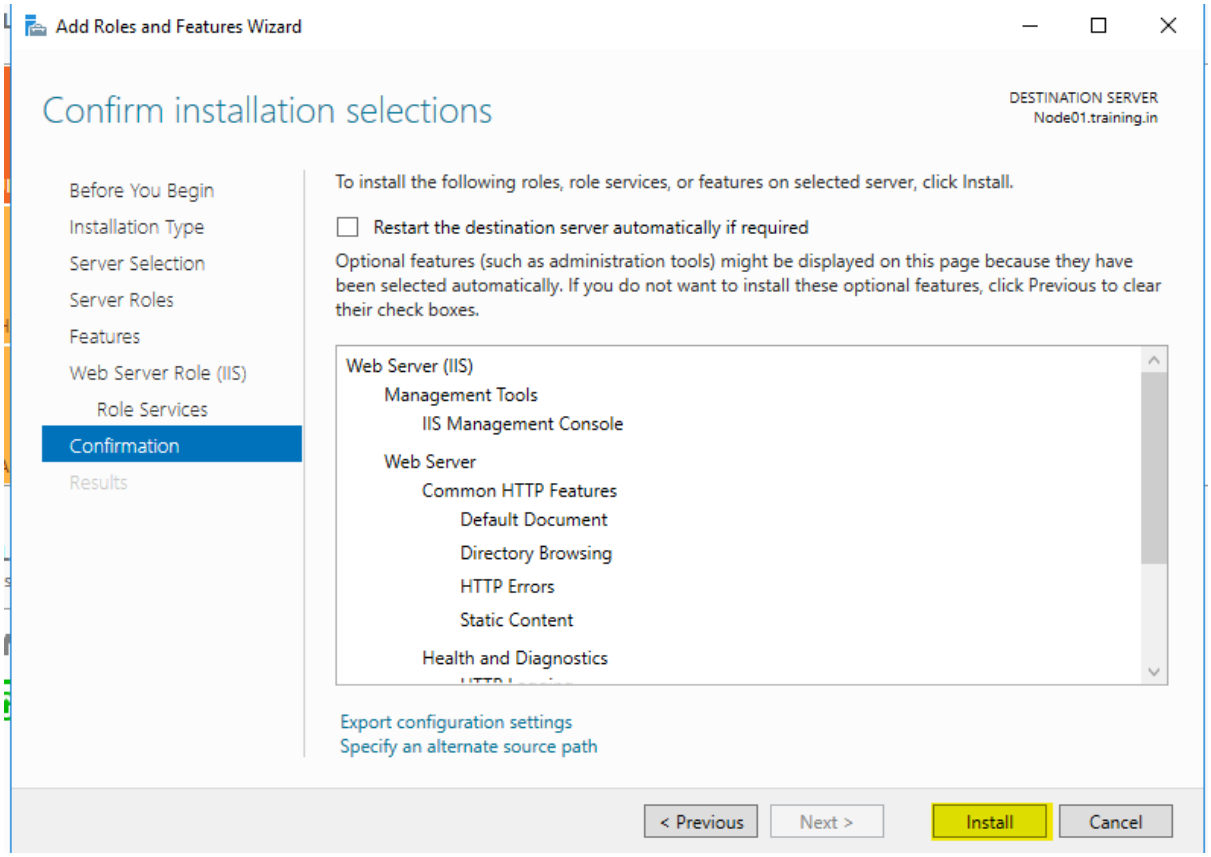
Then click “Next”

Just click on Next:

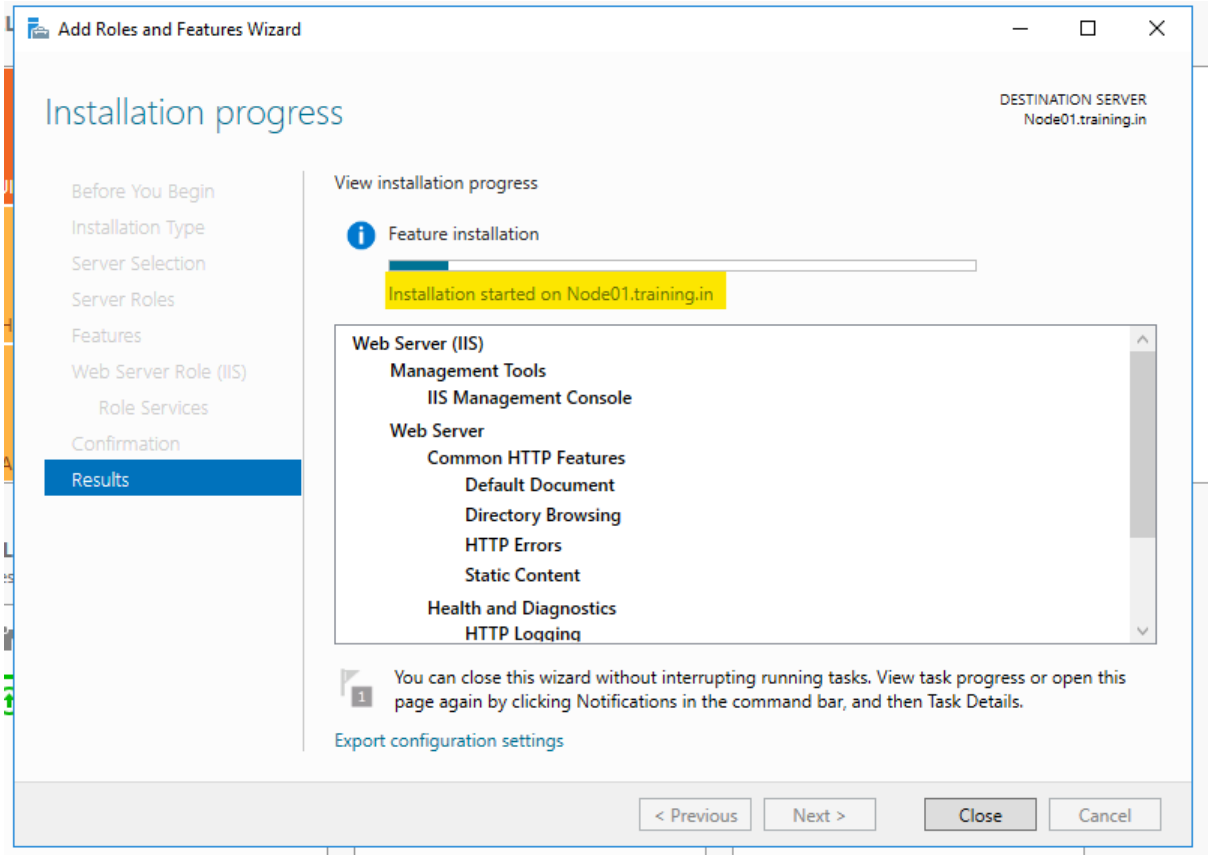


Select all default 'role services'



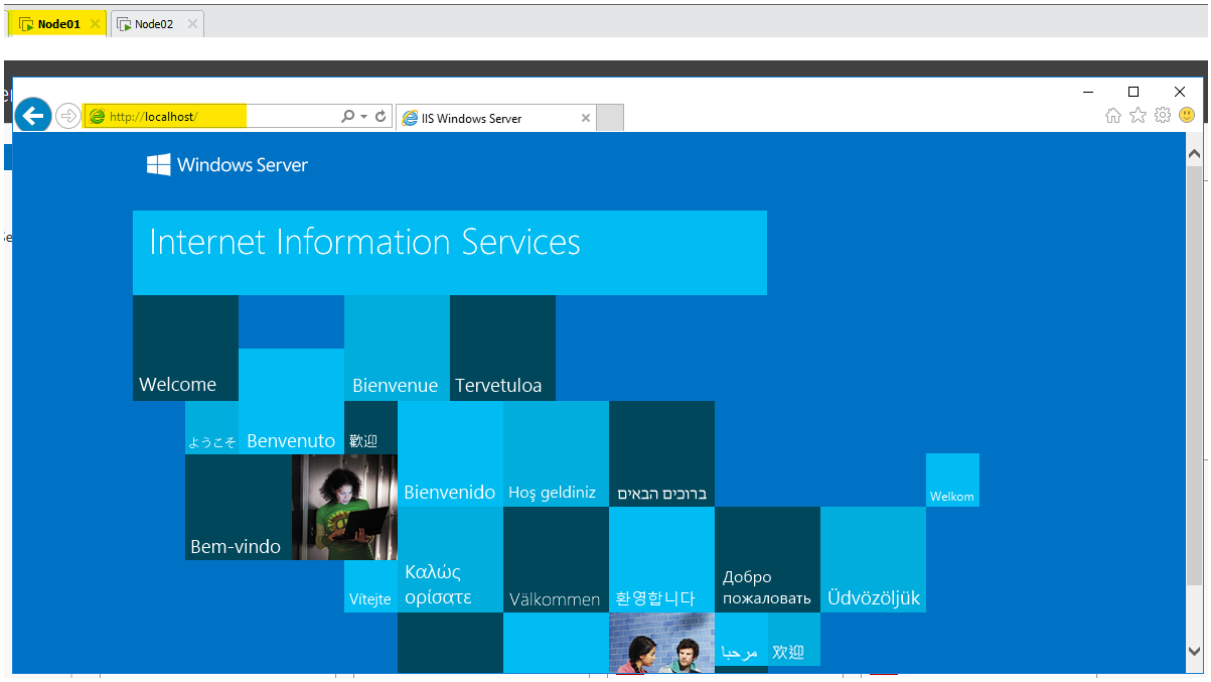


Wait until the installation is succeeded

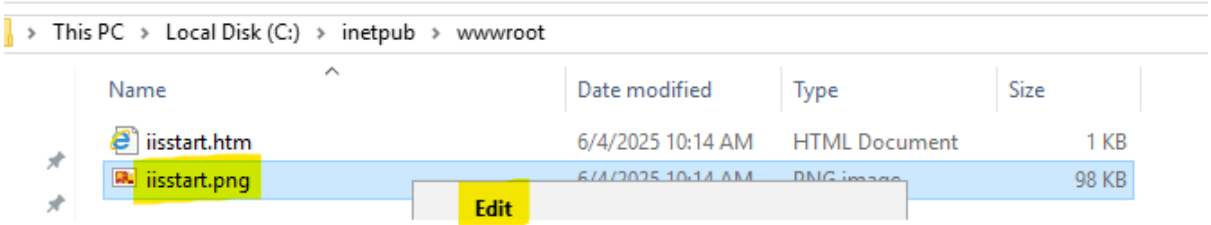


After installation, click on “close”.

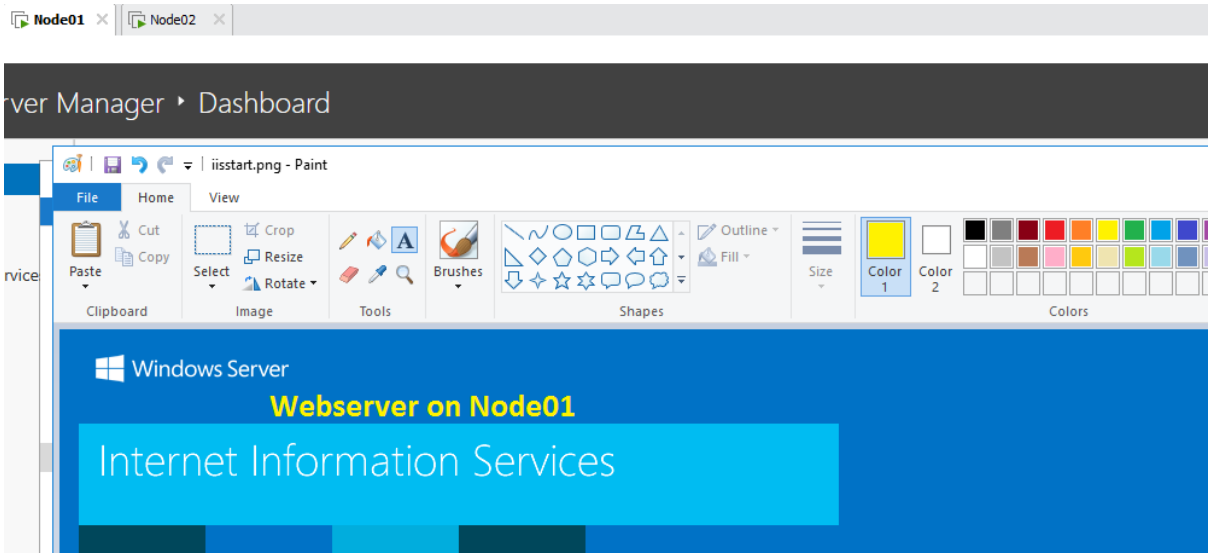
To validate installation on Node01, open internet explorer and type “http://localhost”



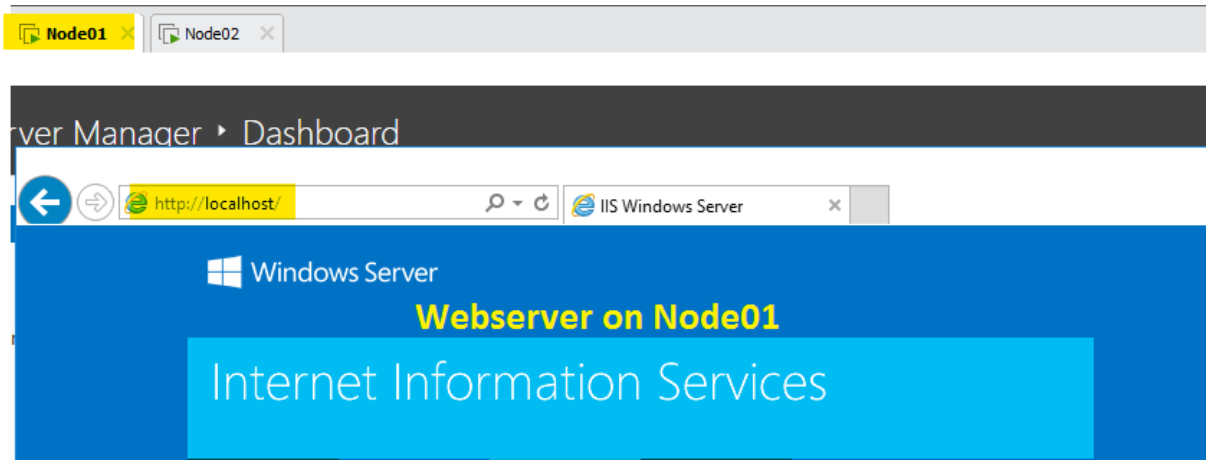
We can also modify this web page. Go to “C:\inetpub\wwwroot” and right-click on the file “iistart.png” and then right-click on “Edit”.



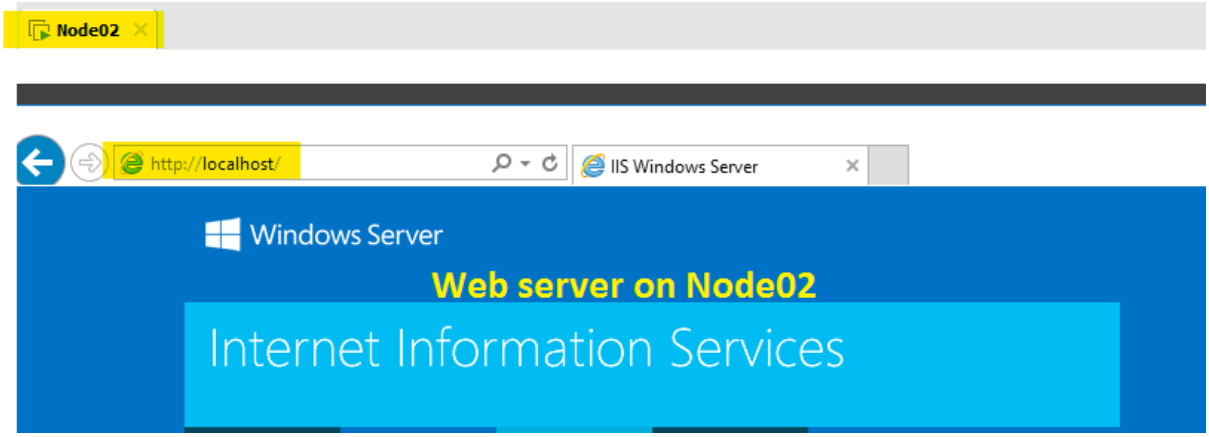
Make some changes using MSPAINT application.



Go back to Internet Explorer and just refresh the page.



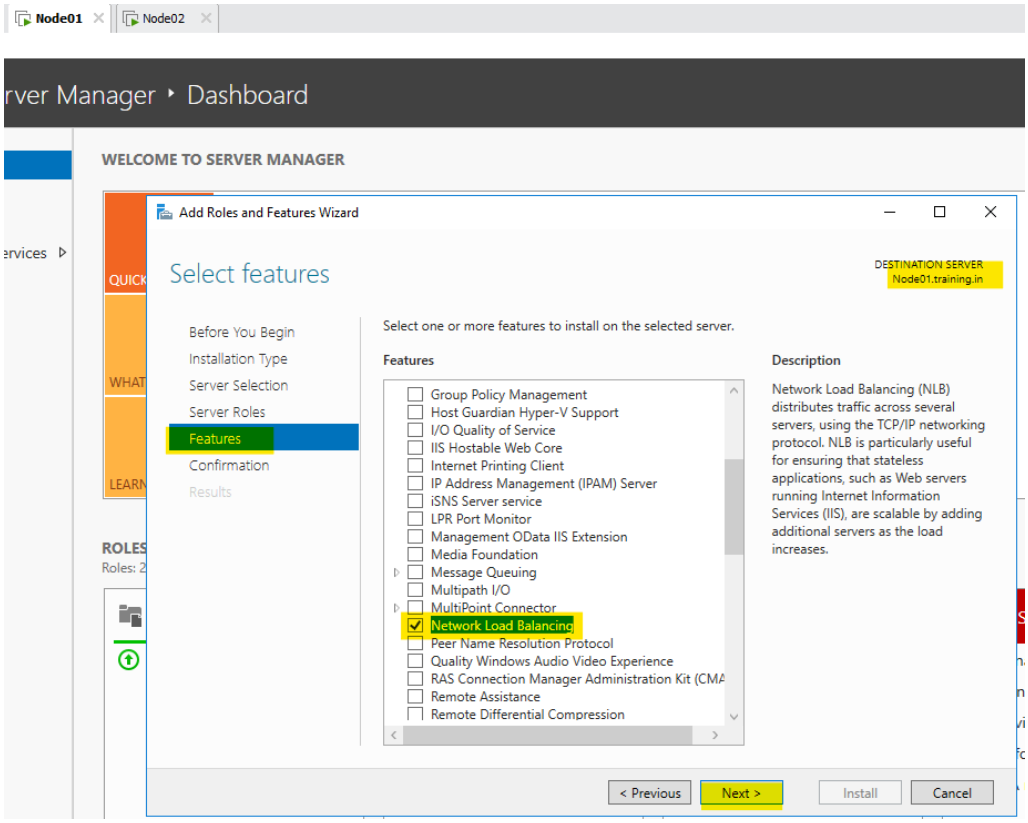
Similarly, install IIS on Node02 and edit the default IIS webpage and verify it on browser.

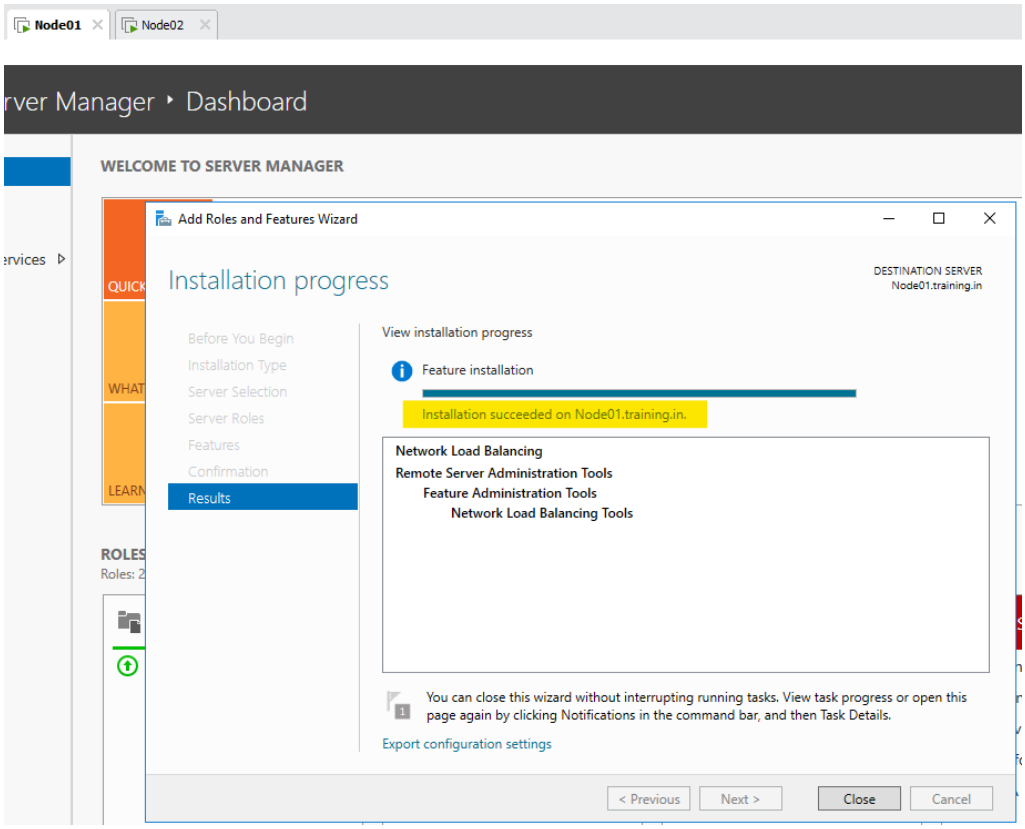


Once IIS installation is completed on both Node01 and Node02, we can now install NLB on both Nodes (01 and 02) one-by-one.

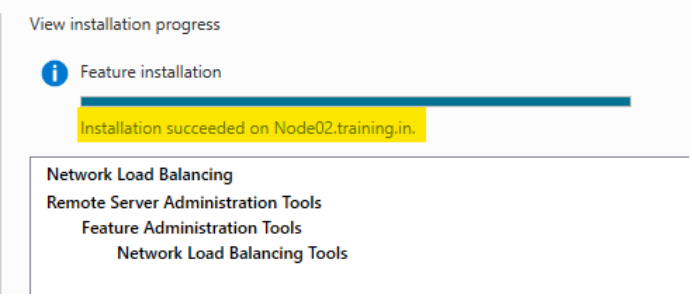
Network Load Balancer (NLB) on both Nodes 01 & 02

Node01 → Dashboard page → Install Feature → NLB → Add features →install.

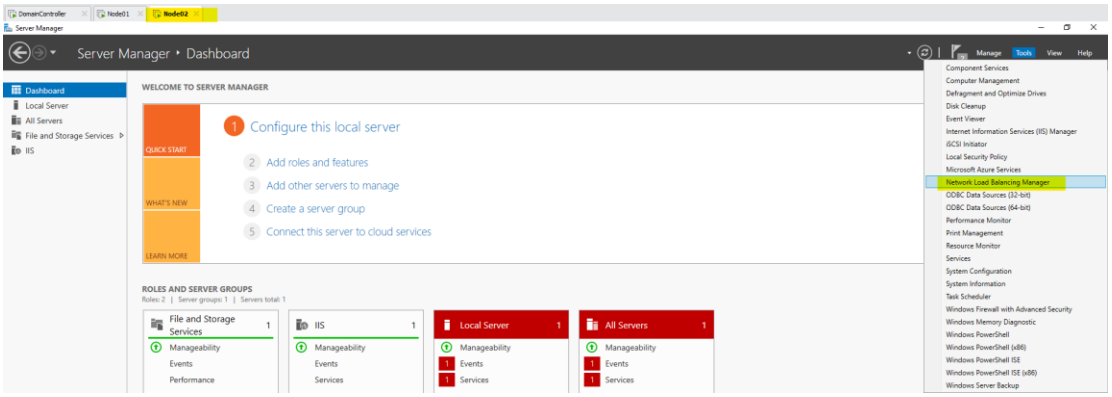




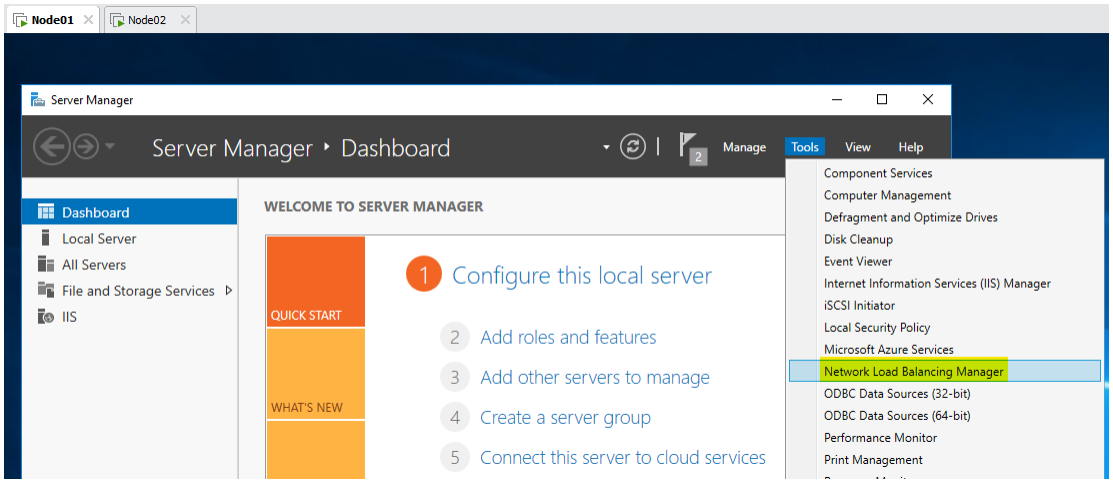
Similarly install NLB on Node02 and verify.



Verify using dashboard.

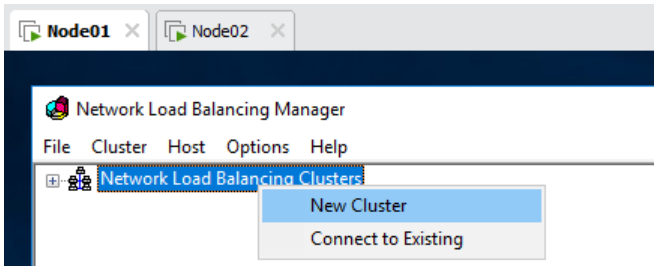


Now go to Node01 → dashboard → tools → Network Load Balancing Manager.

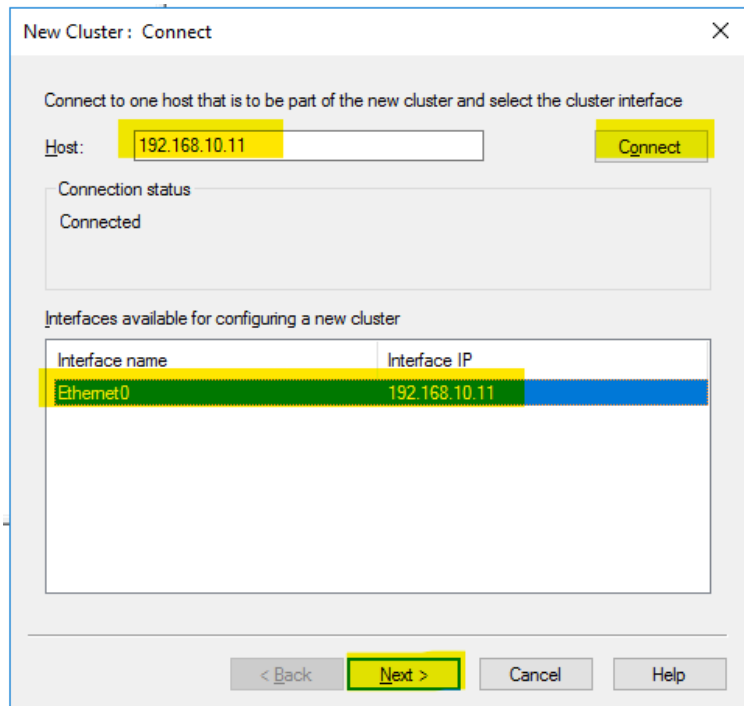


And start the configuration.

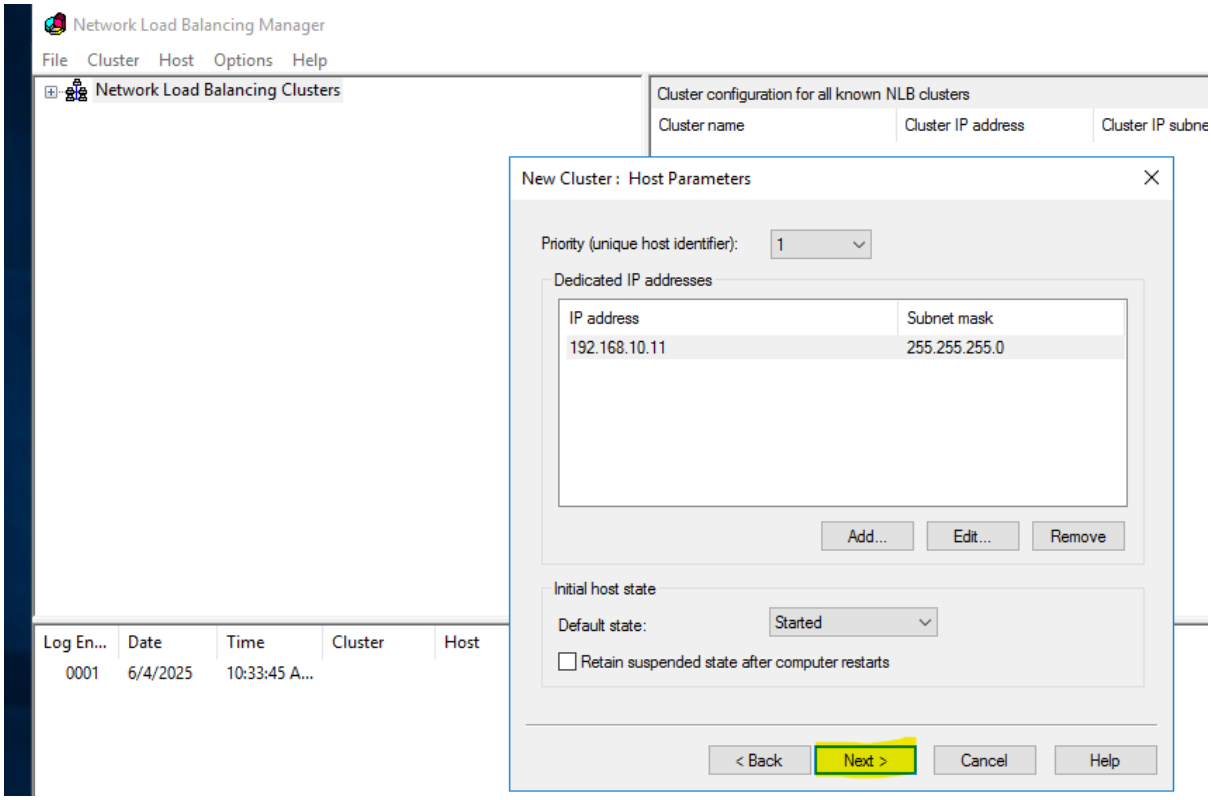
Network Load Balancing Manager → Right-click on Network Load Balancing Clusters → New Cluster



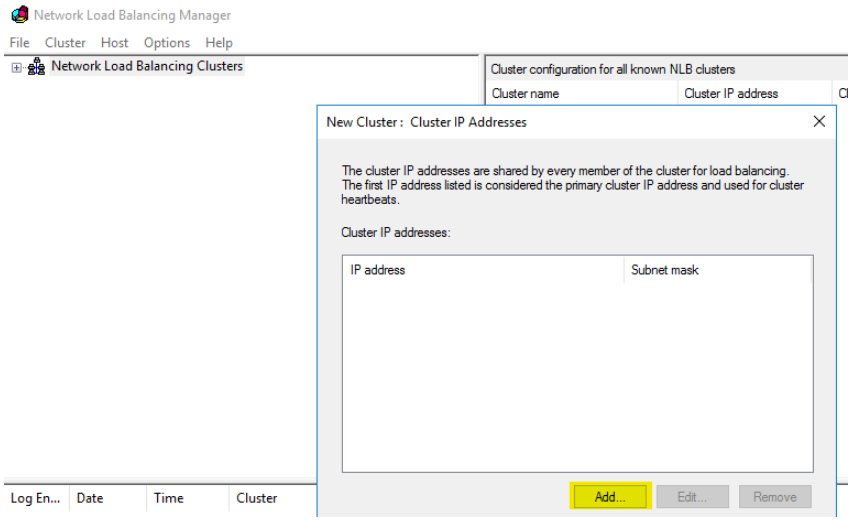
Enter Node01 (IP Address: 192.168.10.11) & click on “Connect”

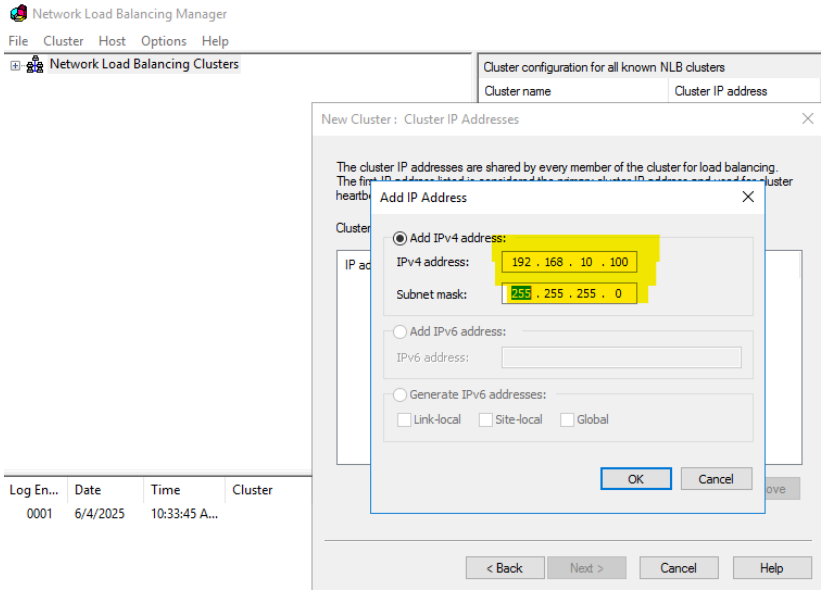


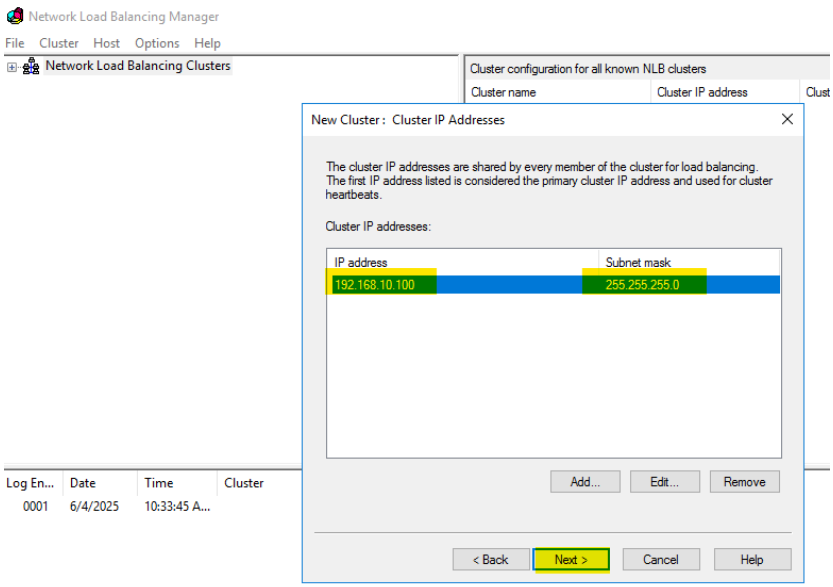
Leave all the values as it is, and click next.



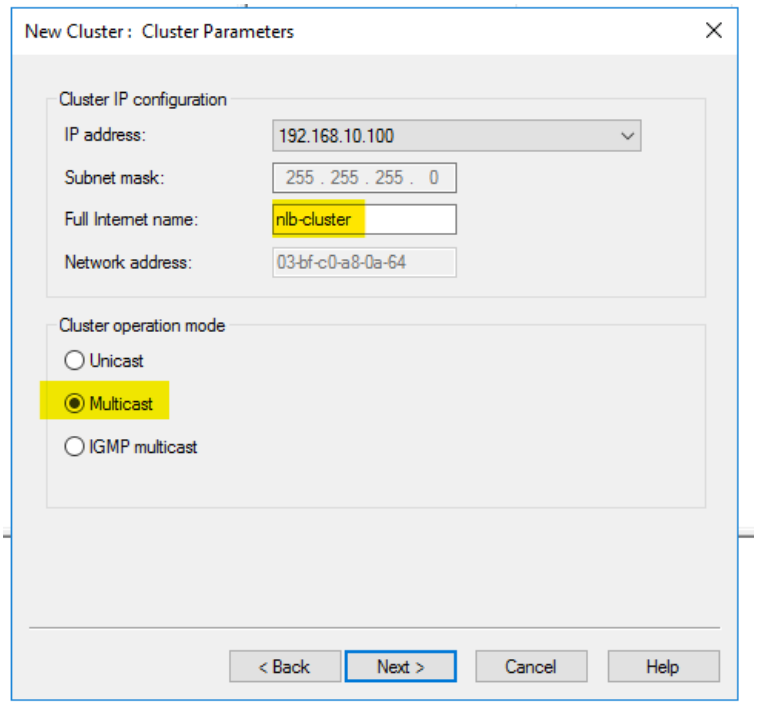
Add a new IP address (192.168.10.100) with subnet mask, this IP will be used by client to connect as URL.



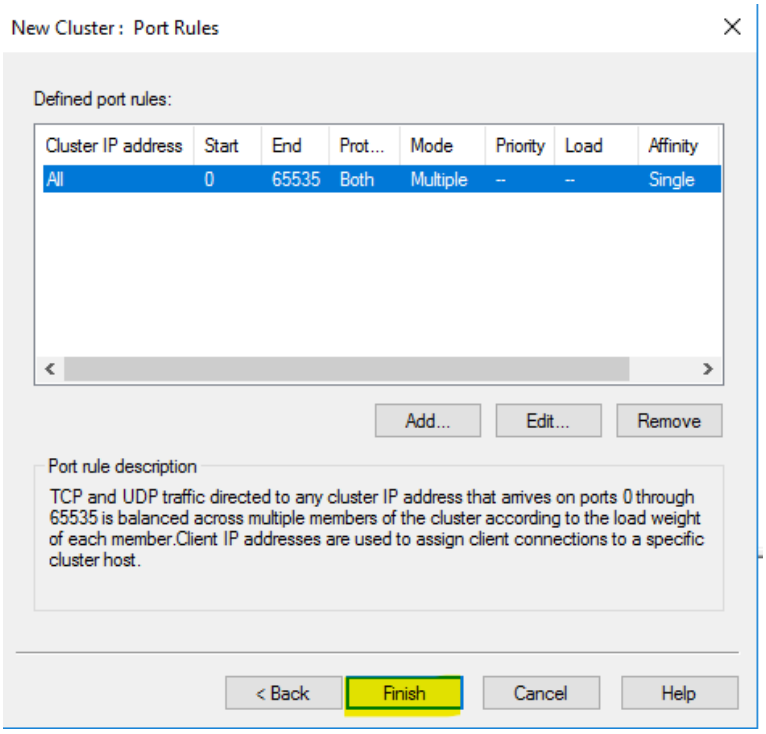




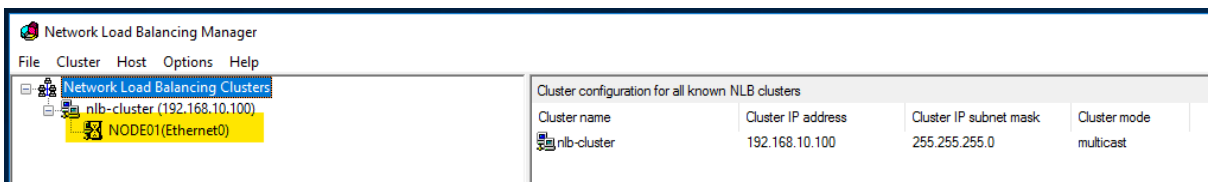
Specify the name for this new cluster (nlb-cluster), so that clients can access it using name.



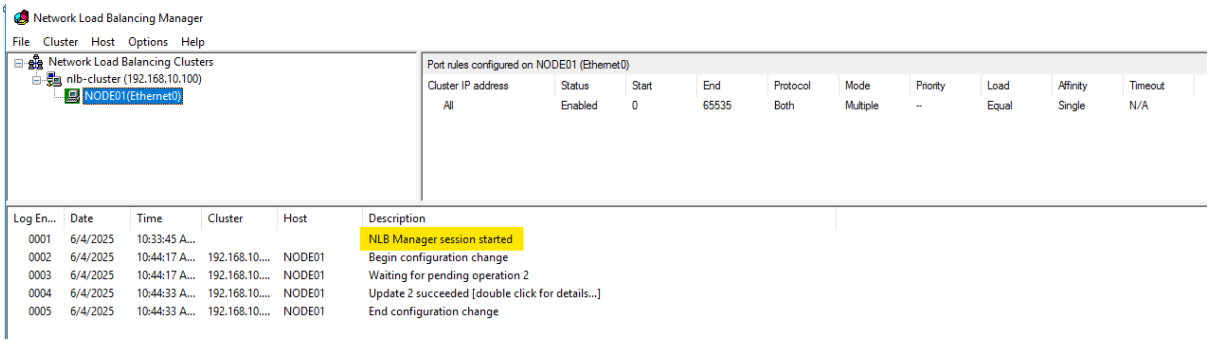
Click “Finish”



Wait for some time.



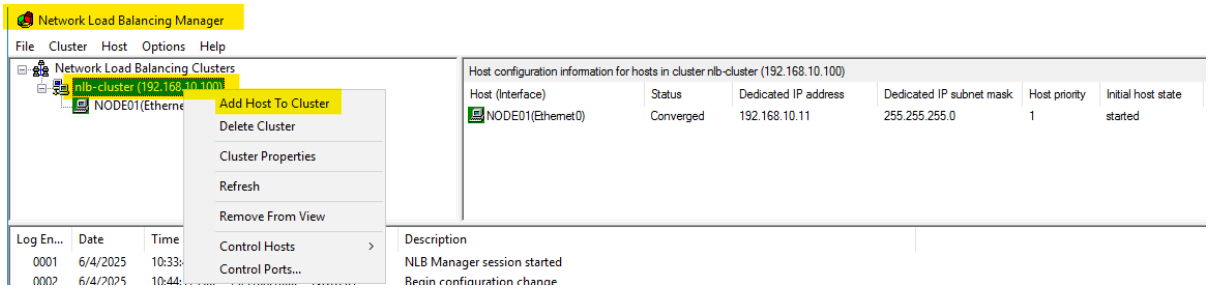
Once done, it looks something like this.



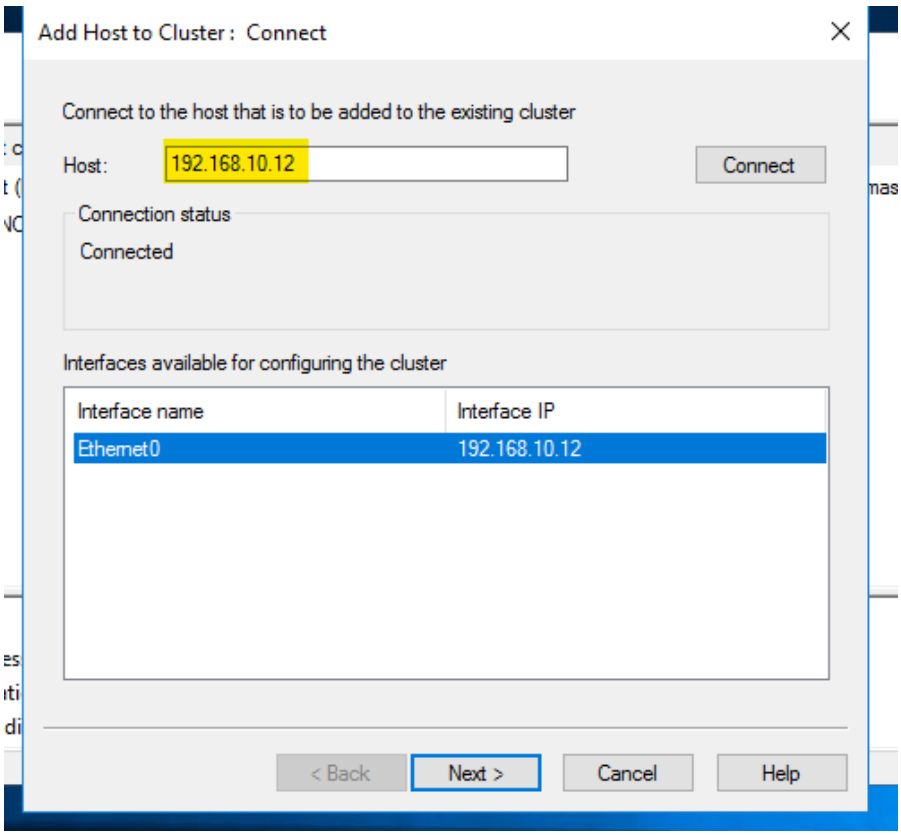
Note – same cluster will be used by Node02 (and all the other nodes), no need to create another cluster.

Now adding the Node02 on the same cluster (nlb-cluster).

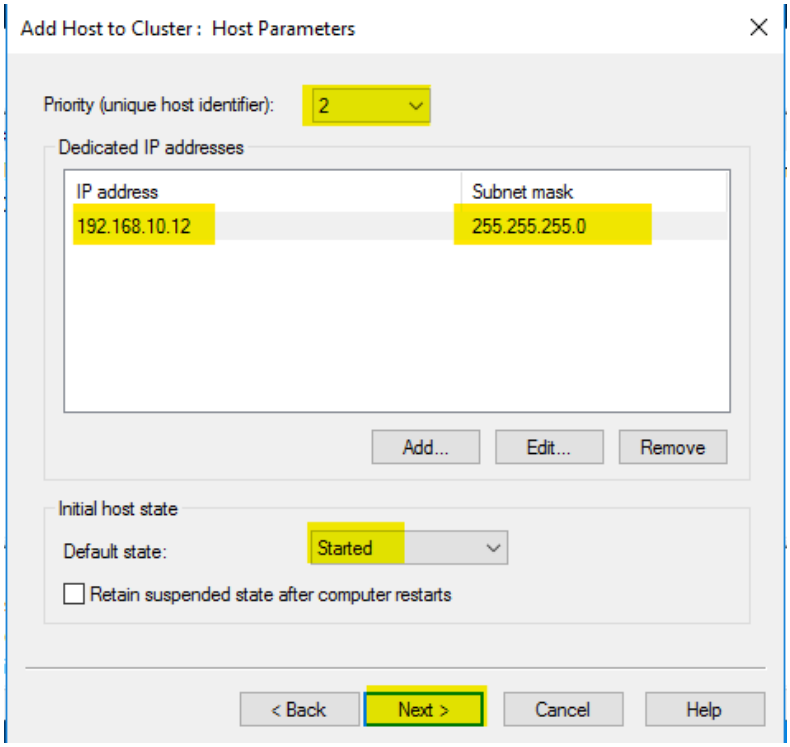
Go to Node01 → Network Load Balancing cluster → right-click and "Add Host to Cluster".



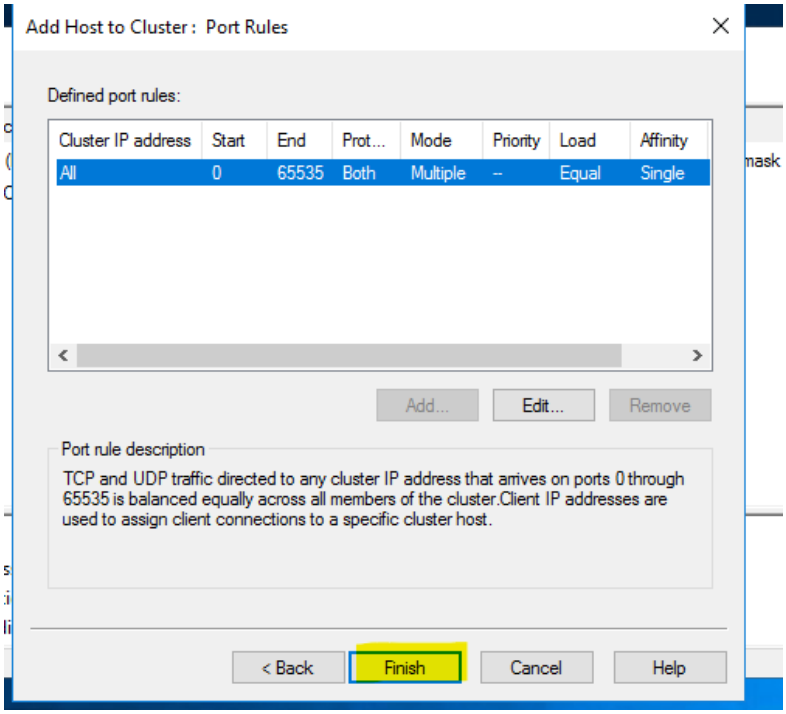
And type the IP address of another Node (node02 – 192.168.10.12)



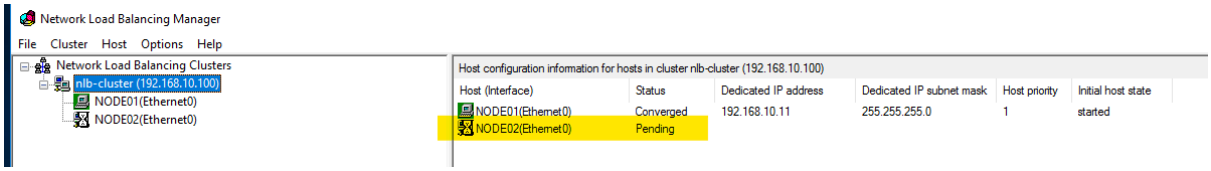
Leave all as default and click Next.



Verify and click on Finish



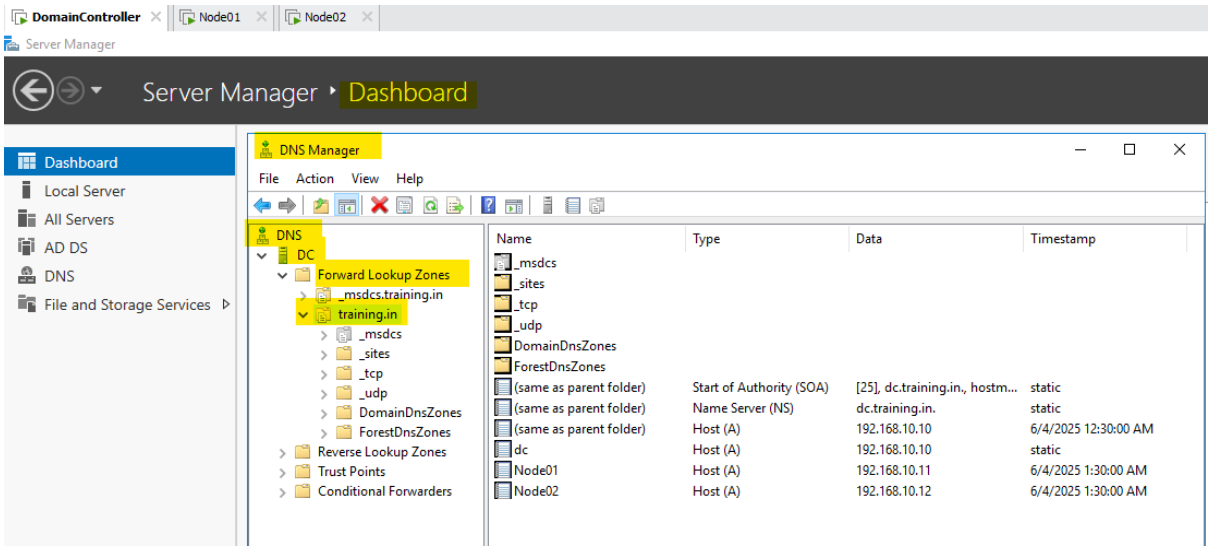
Wait until the status changes to “Converged”



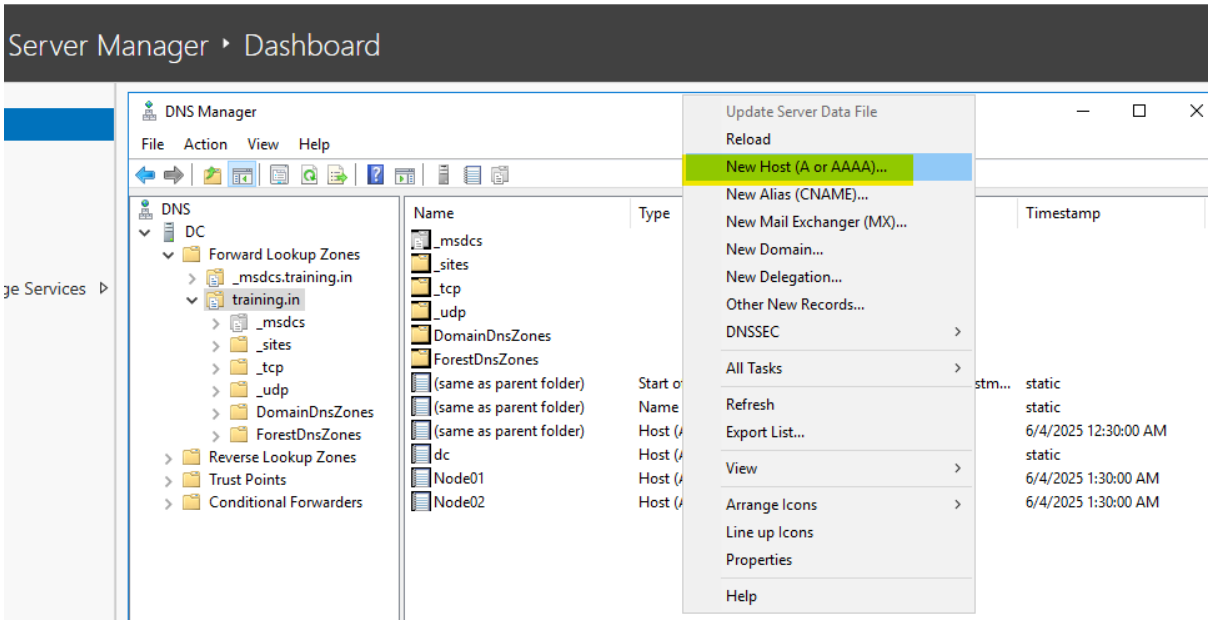
Congratulations, both Node01 and Node02 are part of nlb-cluster.

Now add this NLB-Cluster (with IP as 192.168.10.100) to the DNS on DC so that client can access this cluster using name (instead of IP address).

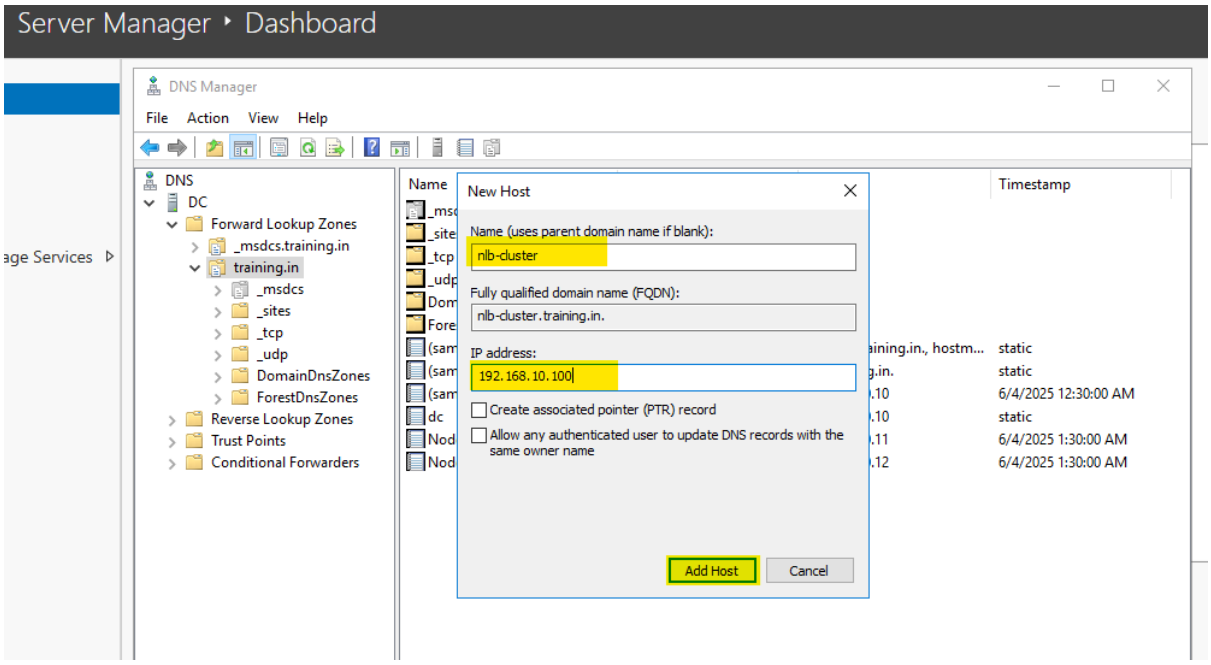
DC → Dashboard → Tools → DNS



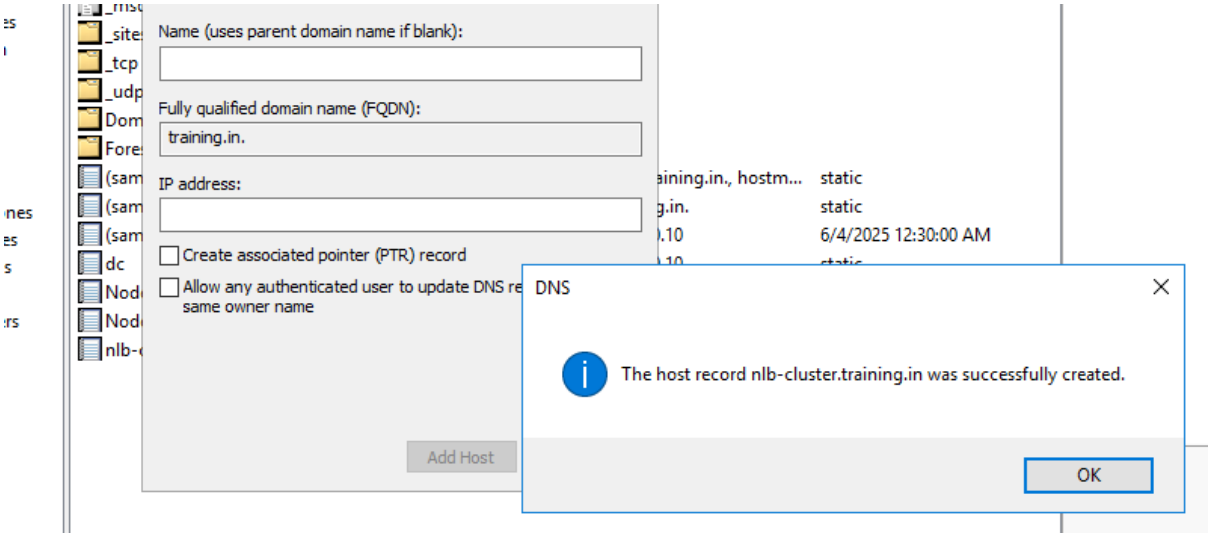
Now create an “A” record here by right-clicking on white area.



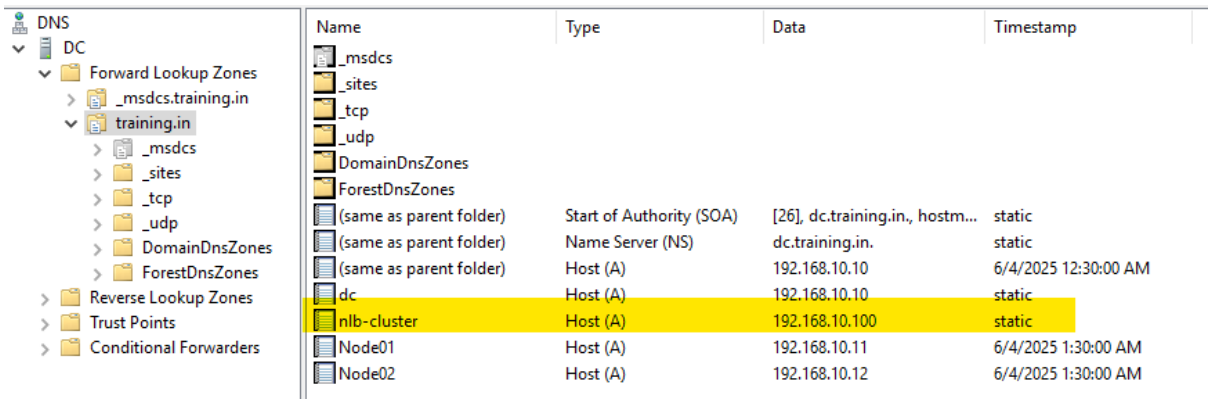
Provide the same hostname and IP address, given at the time of NLB configuration.



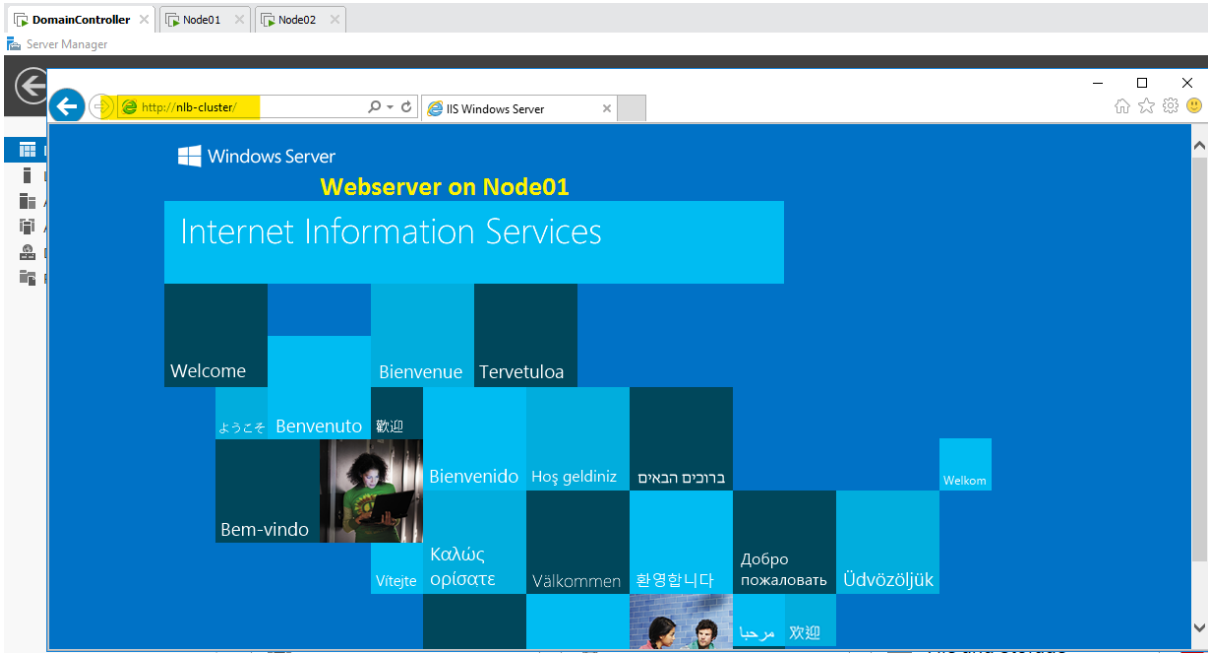
And click on “Done”



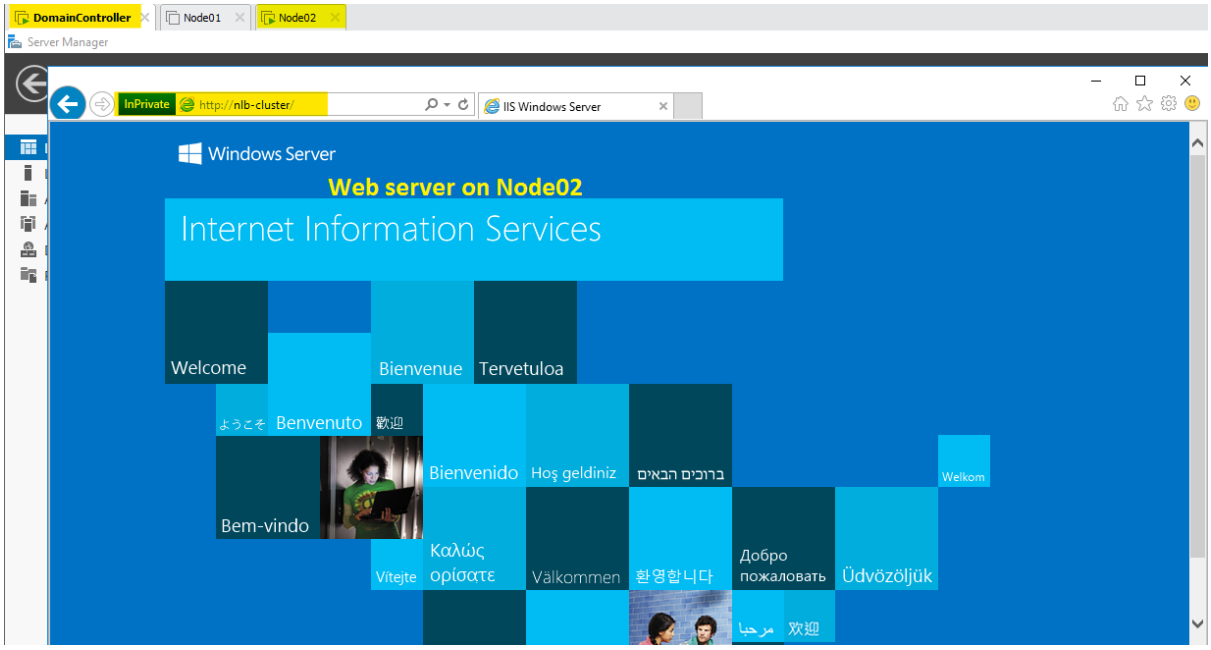
Verify:



To verify, go to “Internet Explorer” on DC and access the URL http://nlb-cluster



Now to check the cluster, turn off Node01 and then refresh the browser (you can also use incognito mode to verify).



Note – NLB cluster successfully configured.

<u>Note – To configure Failover cluster, NLB and IIS webserver must be uninstalled and reboot both Node01 and Node02</u>

Dashboard → Manage → Remove roles and features → select both IIS and NLB and reboot.

Windows Server Update Service (WSUS)

What is WSUS?

- WSUS is a Microsoft technology that enables centralized management and distribution of Microsoft updates (security patches, bug fixes, feature updates) to computers in a corporate or organizational network.
- It allows administrators to approve, schedule, and deploy updates to Windows operating systems and other Microsoft software.
- WSUS reduces bandwidth usage by downloading updates once and distributing them locally.

Purpose of WSUS

- Ensure all managed computers are up-to-date with critical security patches.
- Control which updates are deployed and when.
- Monitor update status and compliance across the organization.
- Reduce Internet bandwidth usage by caching updates locally.

How WSUS Works

- WSUS Server downloads updates from Microsoft Update.
- Updates are stored in the local WSUS database and file storage.
- Client computers connect to the WSUS server at scheduled intervals.
- Clients check for approved updates relevant to their system.
- WSUS server approves or declines updates based on administrator decisions.
- Clients download approved updates from WSUS server.
- WSUS provides reporting on update installation status.

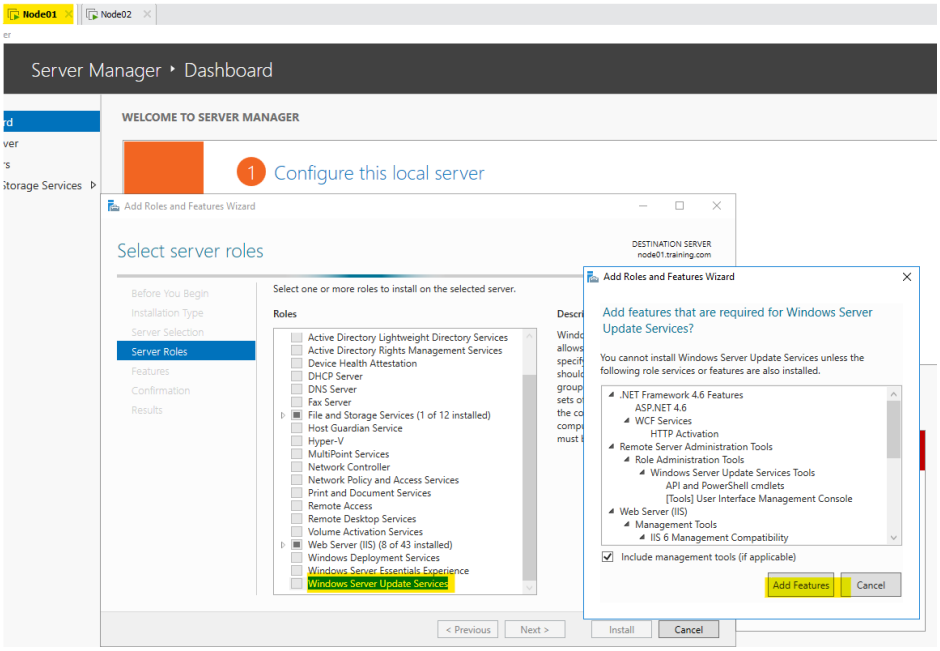
Key Components of WSUS

Component	Description
WSUS Server	The server hosting the WSUS role, managing update synchronization, approvals, and client communications.
WSUS Database	Stores update metadata, approvals, client info, and status. Can be Windows Internal Database (WID) or SQL Server.
Update Repository	File storage on the WSUS server where actual update files are stored.
WSUS Clients	Windows machines configured to receive updates from WSUS instead of Microsoft Update.
Group Policy (GPO)	Used to configure client machines to point to WSUS server and set update policies.
WSUS Console	GUI used by admins to manage updates, approvals, reports, and synchronization.
Reporting Services	Optional integration for advanced reporting via SQL Server Reporting Services (SSRS).

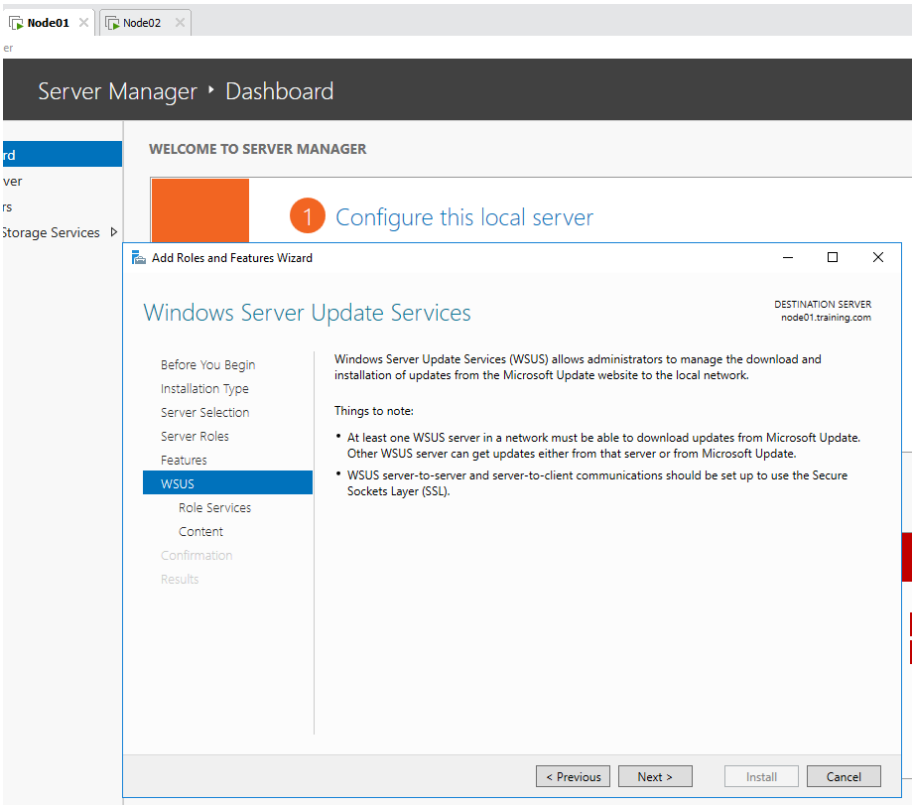
Installing and configuring Windows Server Update Service (WSUS)

Information – To install and configure WSUS I have used another domain name called "Training.com". rest everything is same for both the domains. You can continue with your existing domain, no need to create a new domain for this.

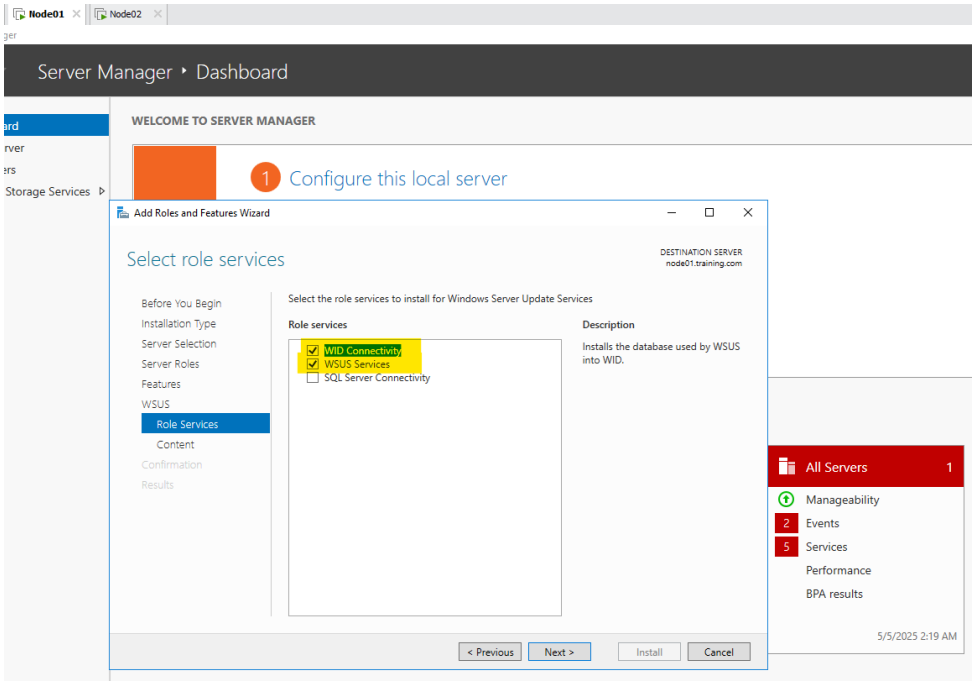
Node01 → Server Manager → Manage → Add roles and features → Role (Windows Server Update Service)



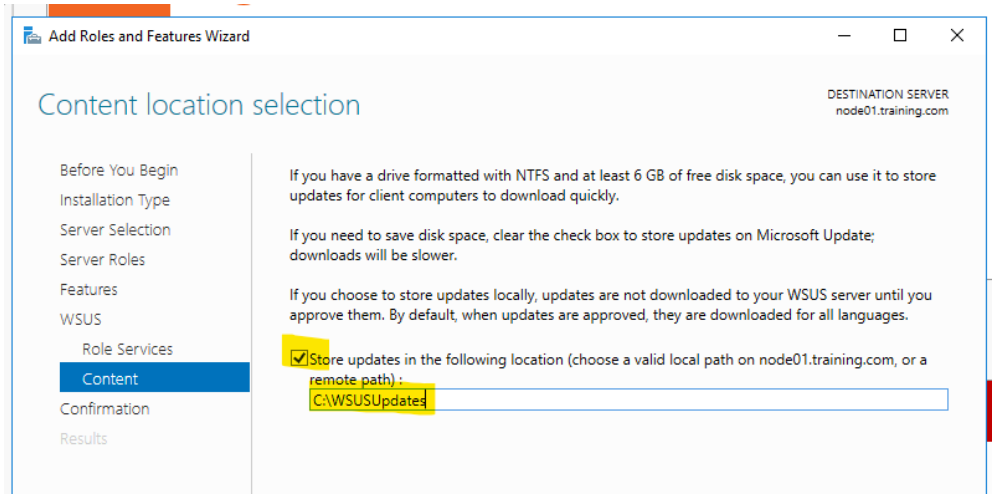
No features to be added:



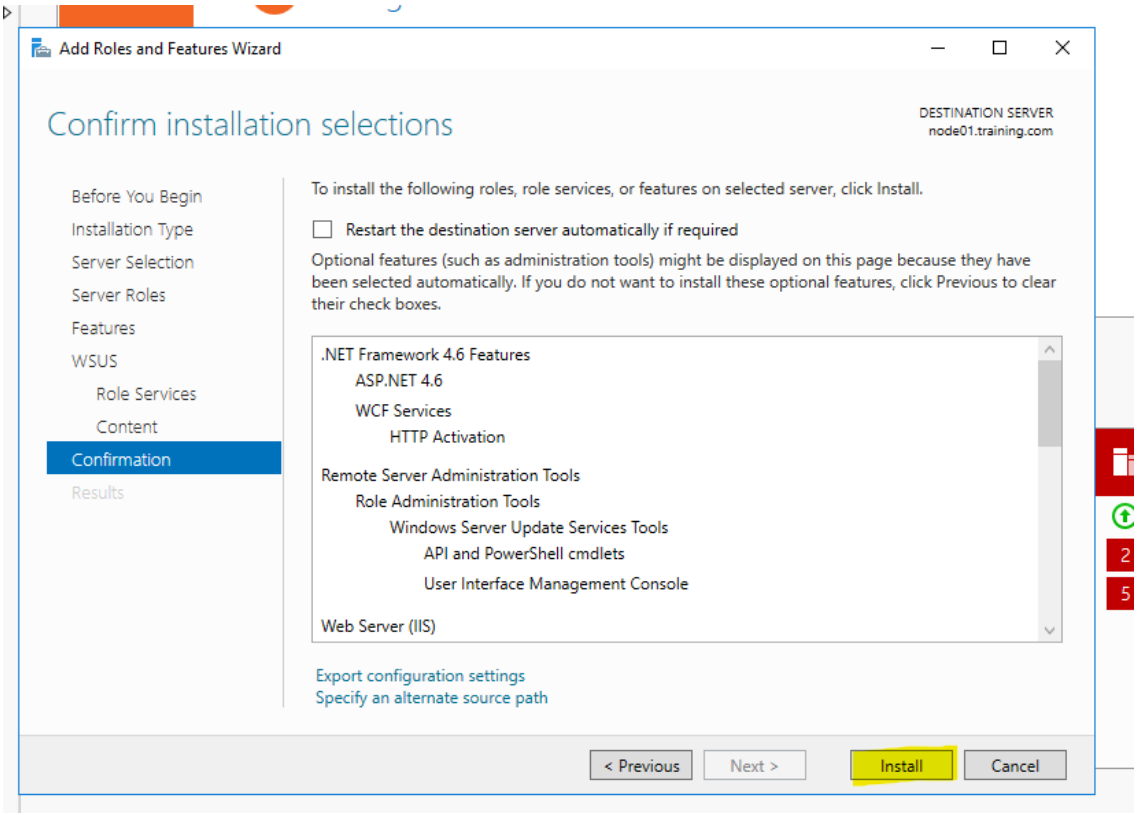
Select required role services:



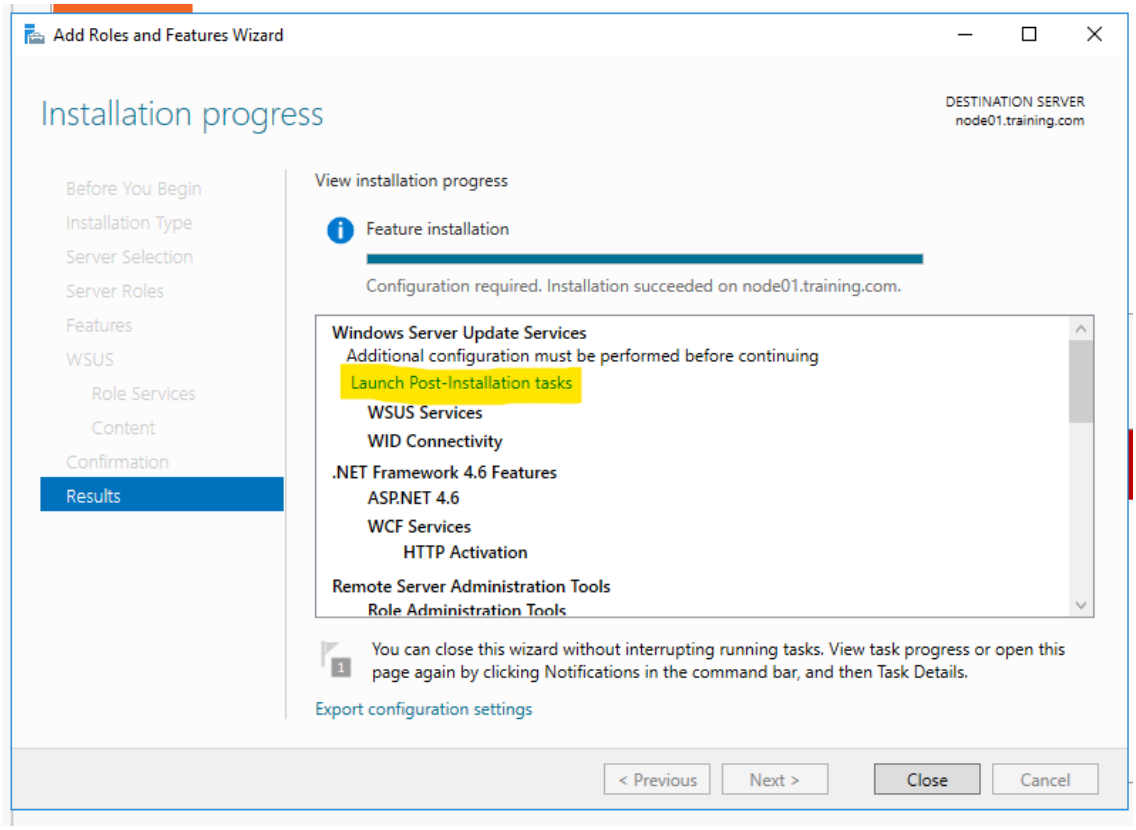
Adding path for storing updates (create new folder):



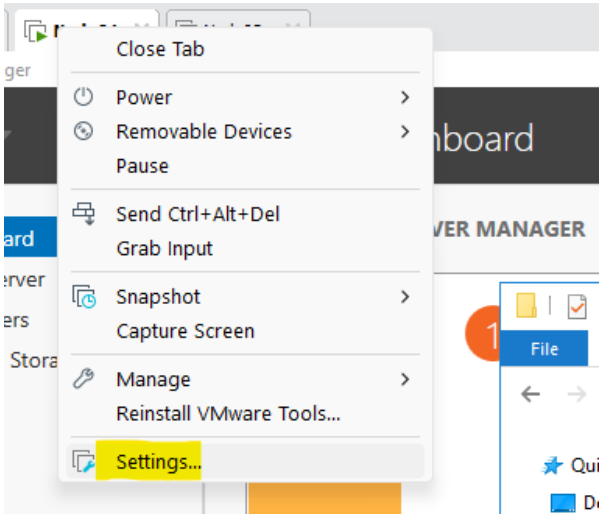
Install:



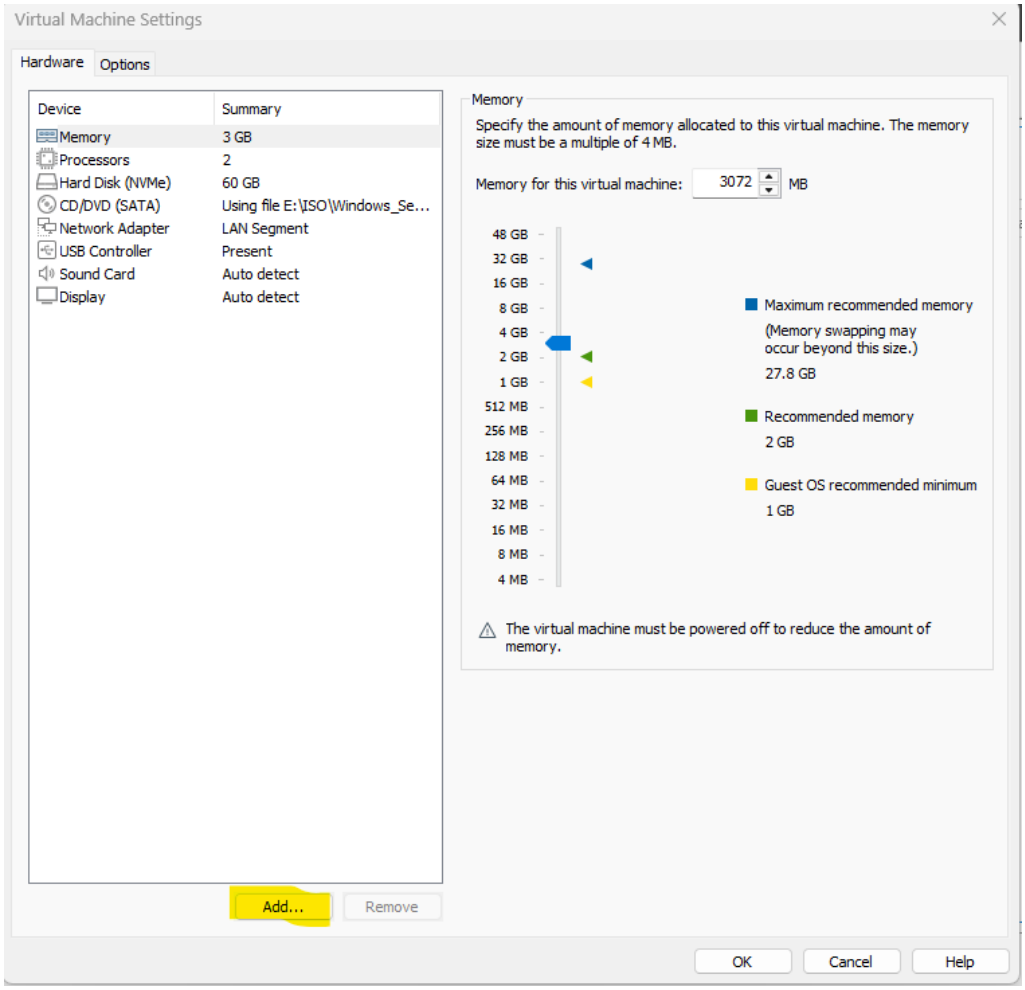
Click on “Launch Post-Installation tasks”



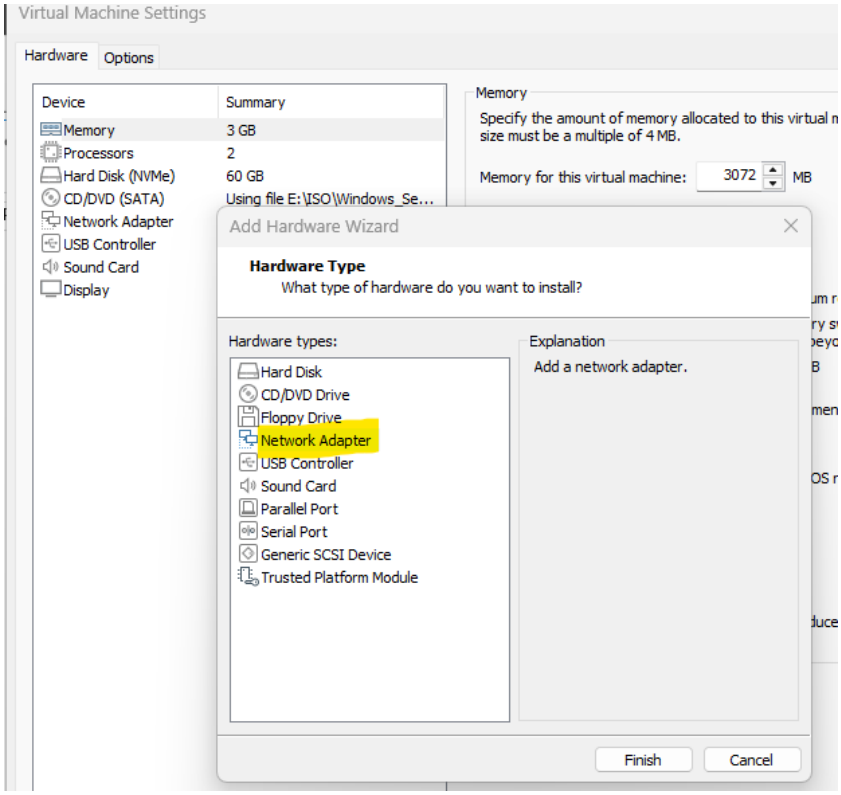
Add a new NIC card to node VM (Node01):



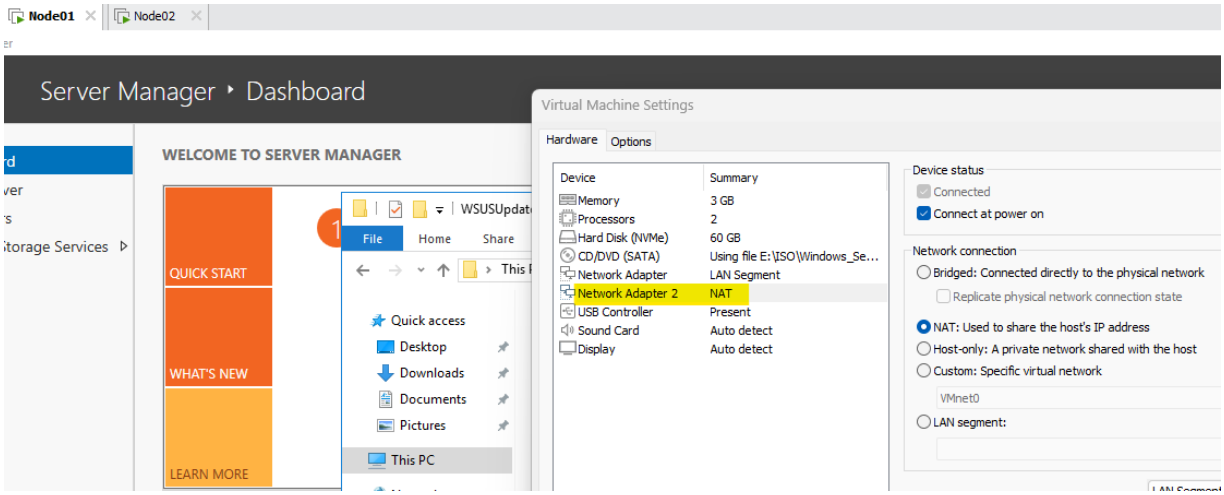
Click on “ADD”:



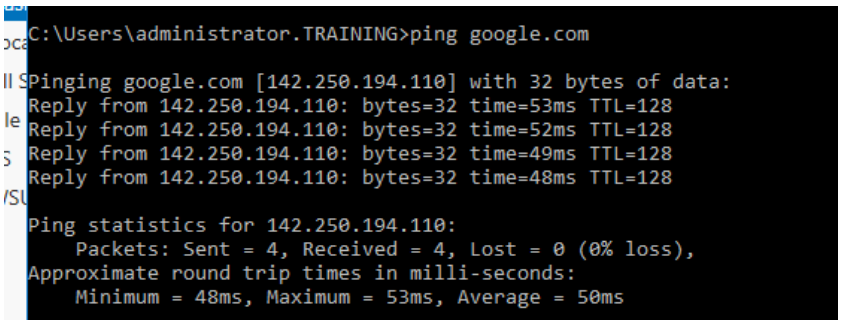
Select “Network Adapter”:



Ensure that new network adapter is on NAT:

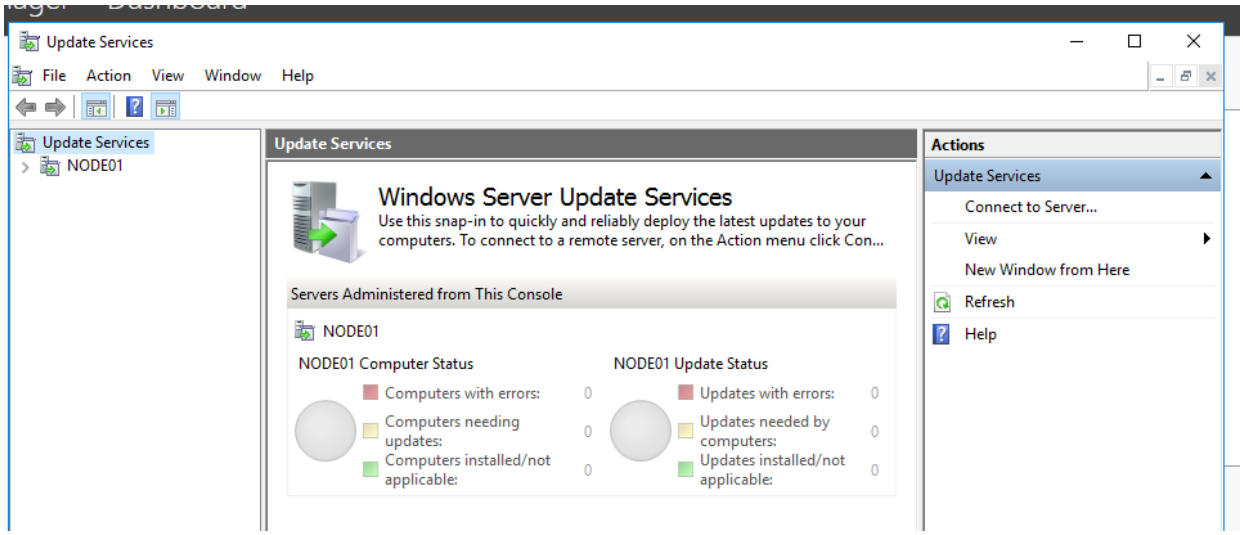


Now ping Google.com to test if internet is working:

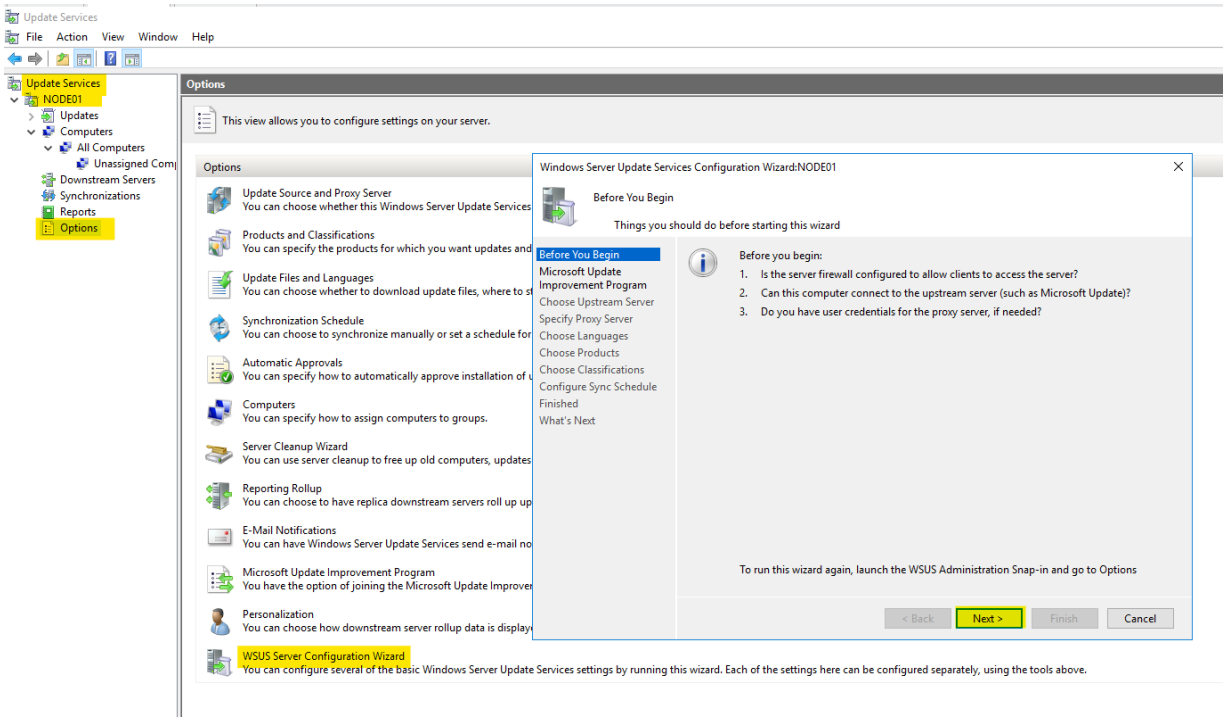


Configuring WSUS on Node01:

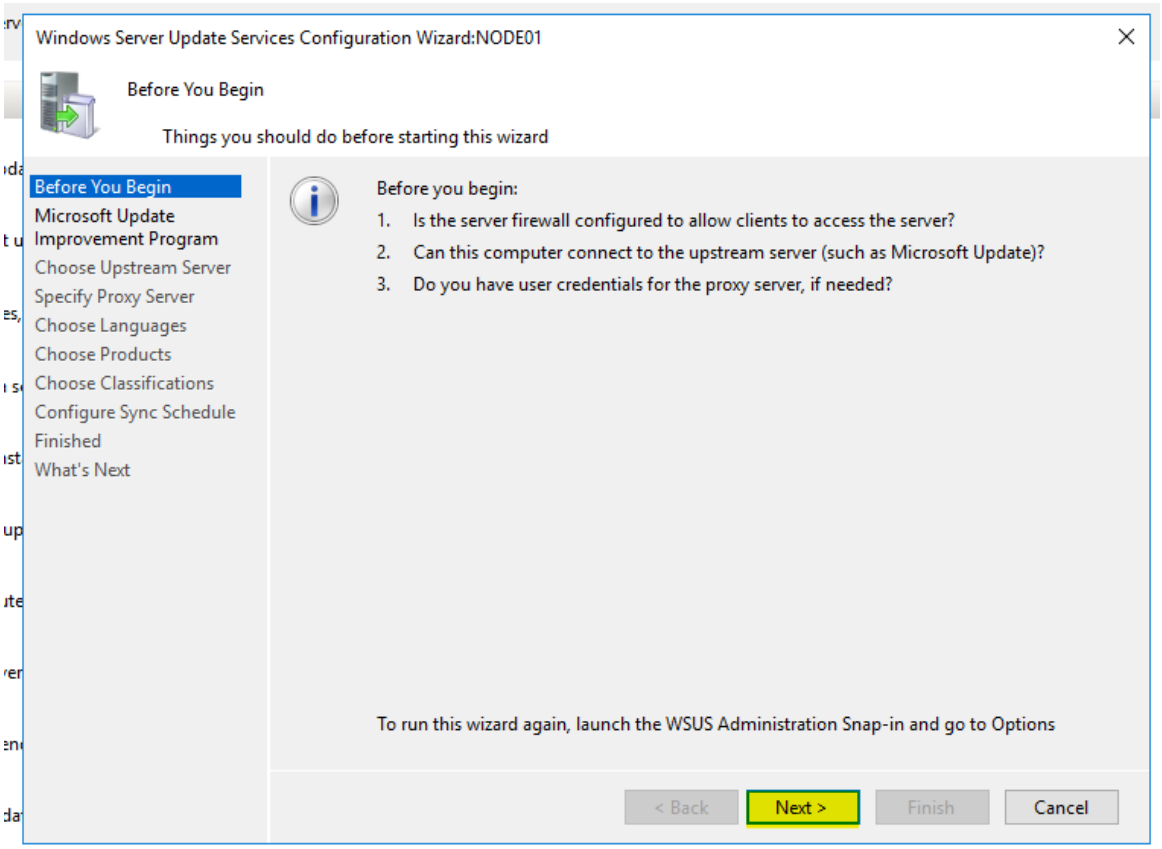
Server Manager Dashboard Page → Tools → Windows Server Update Service



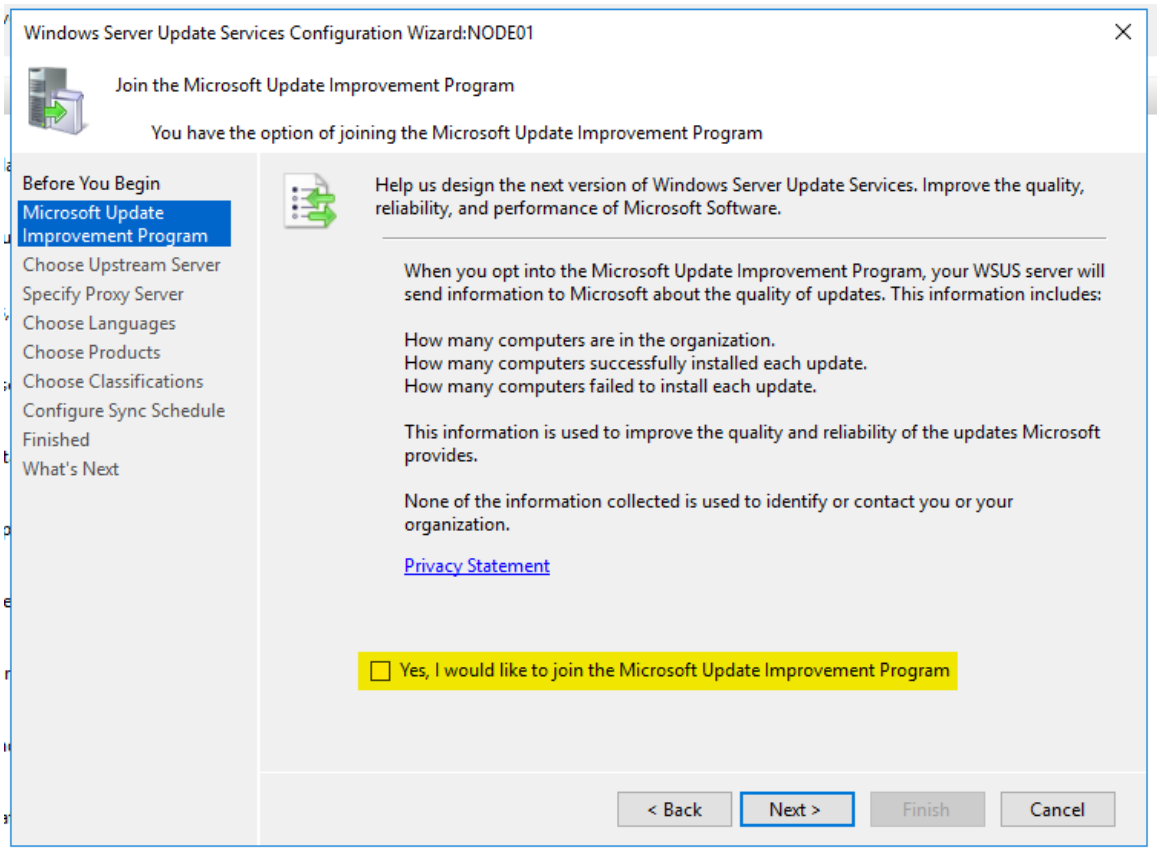
To configure WSUS configuration, Tools → Windows Server Update Service Console (select Options on left side):



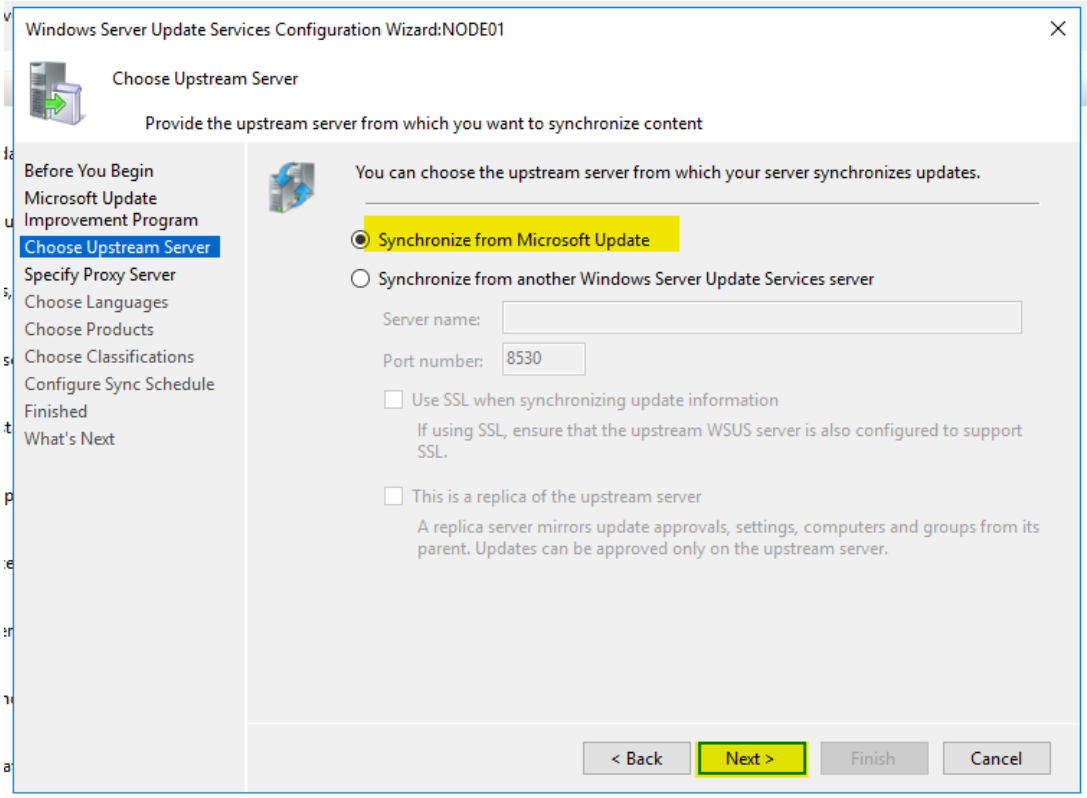
Click Next on “Before You Begin”:



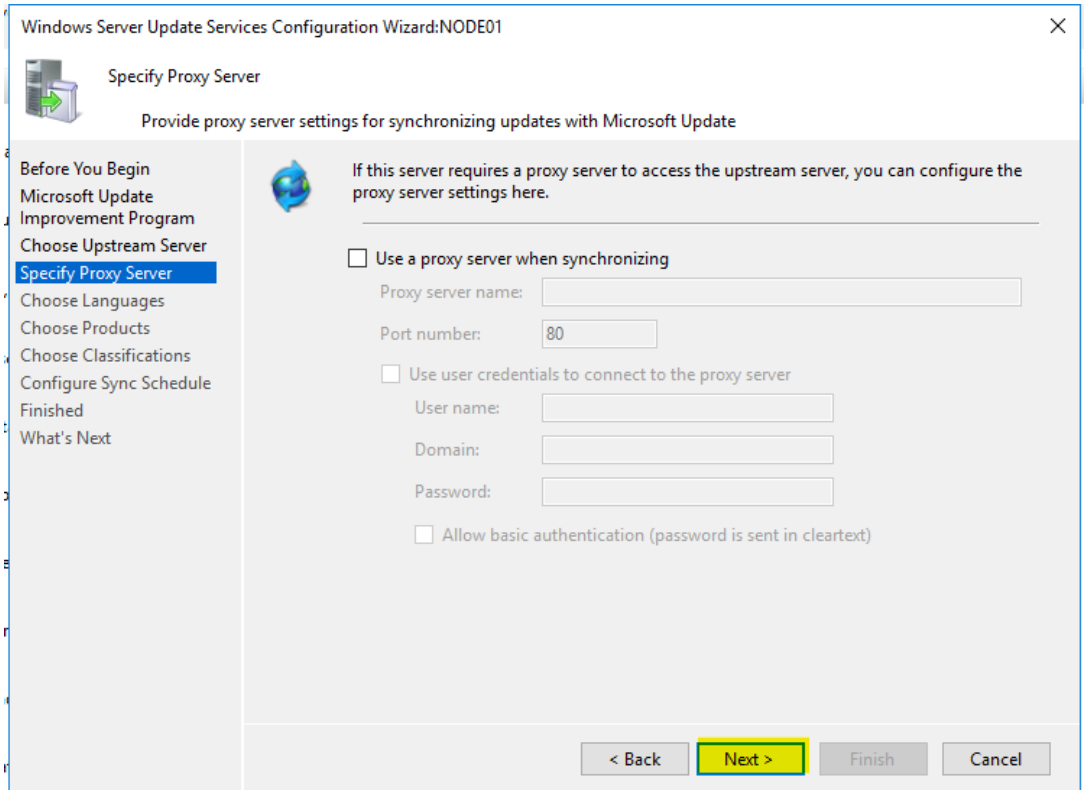
Untick “Yes, I would like to join Microsoft Update improvement program”



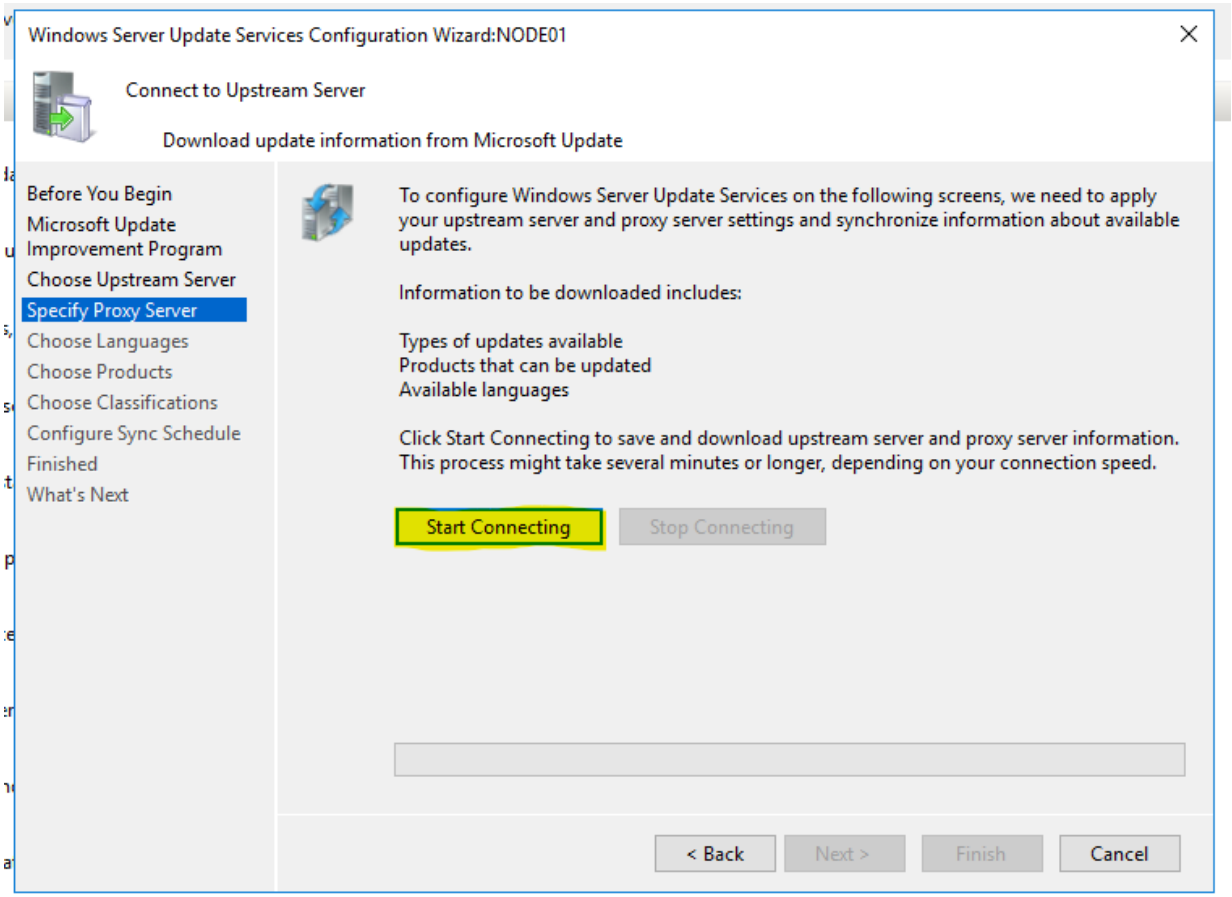
Select “Synchronize from Microsoft Update”, as we are connected to internet:

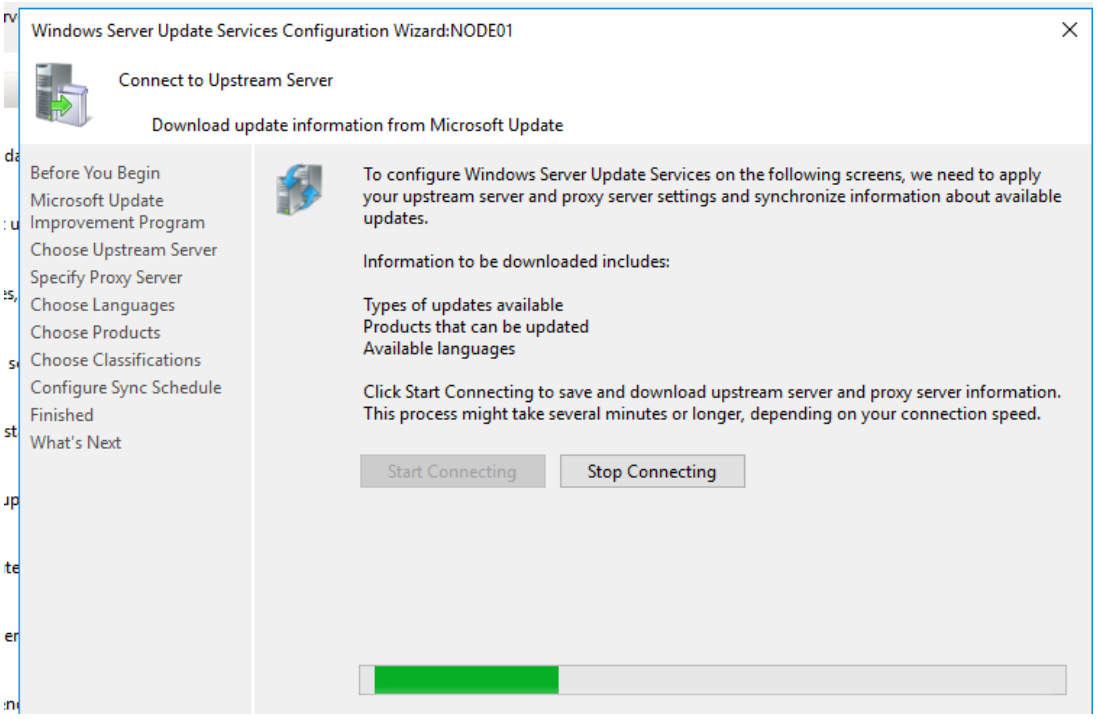


Leave the proxy server page and click Next:

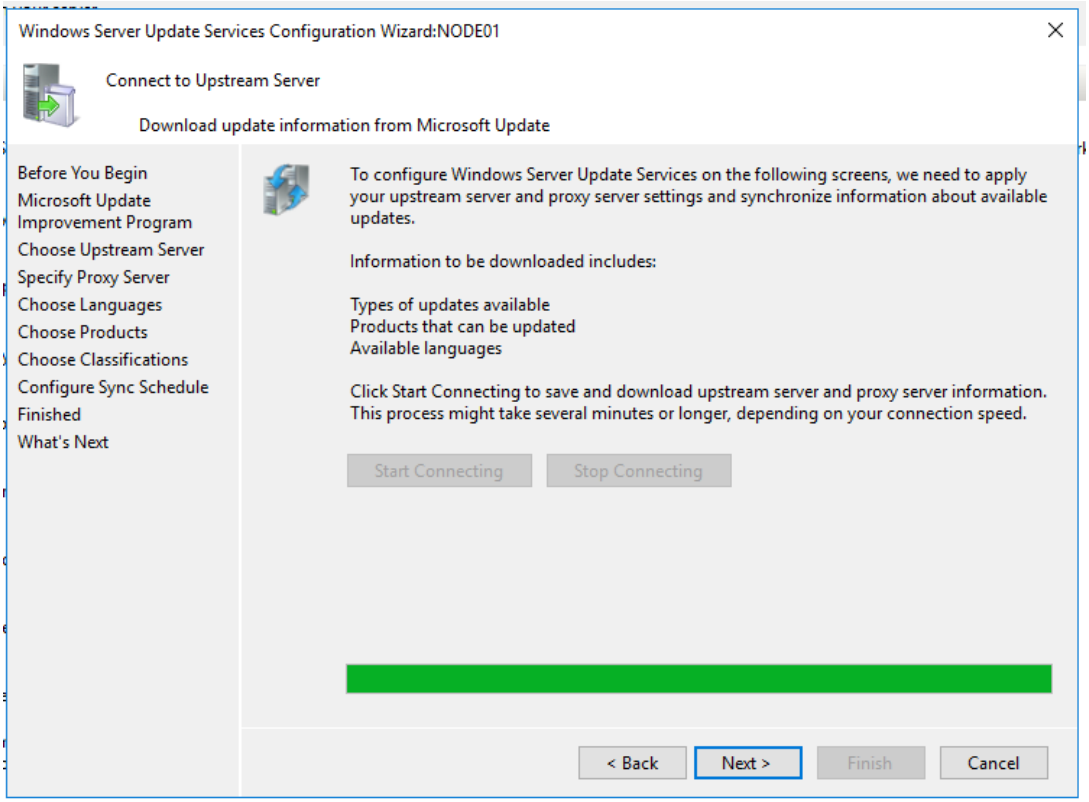


Click on “Start Connecting”:

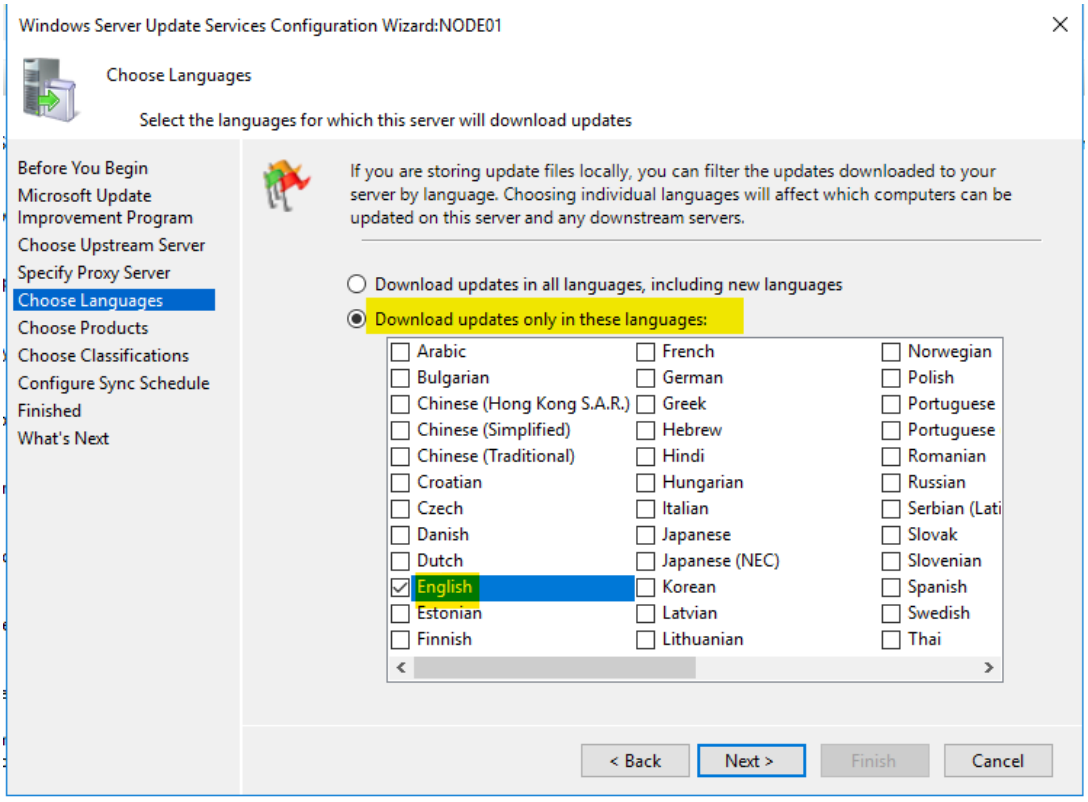




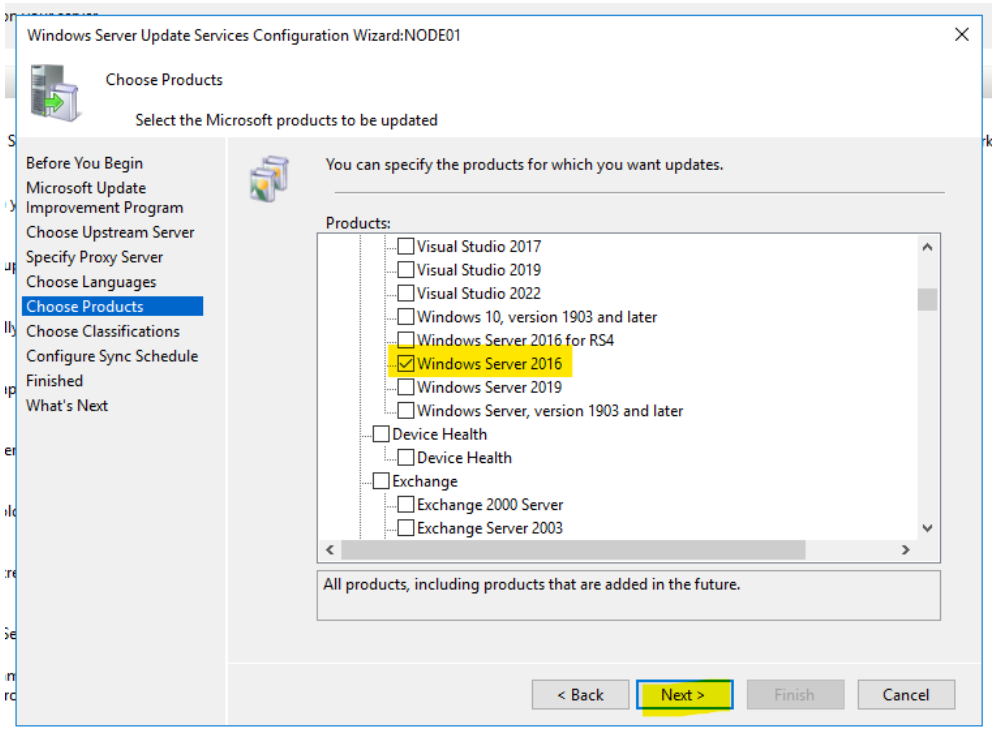
Approx. after 30mins the update was complete. Now click on Next:



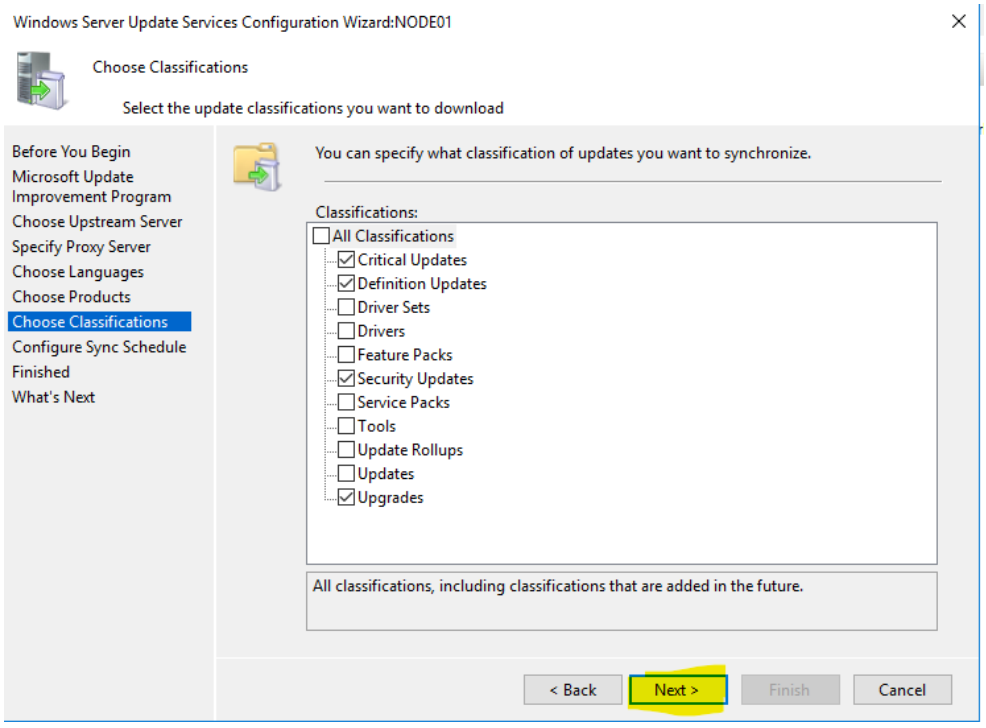
Select English language:



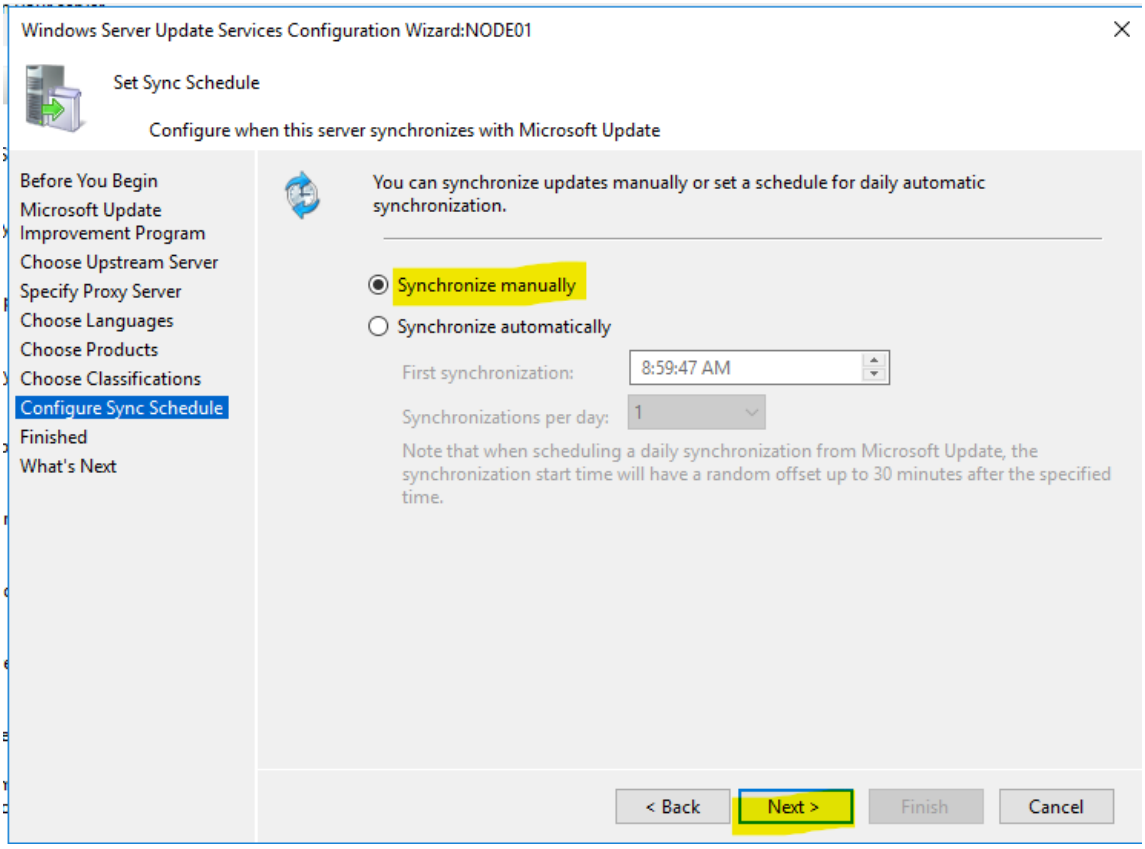
Select appropriate product (depending upon requirement):



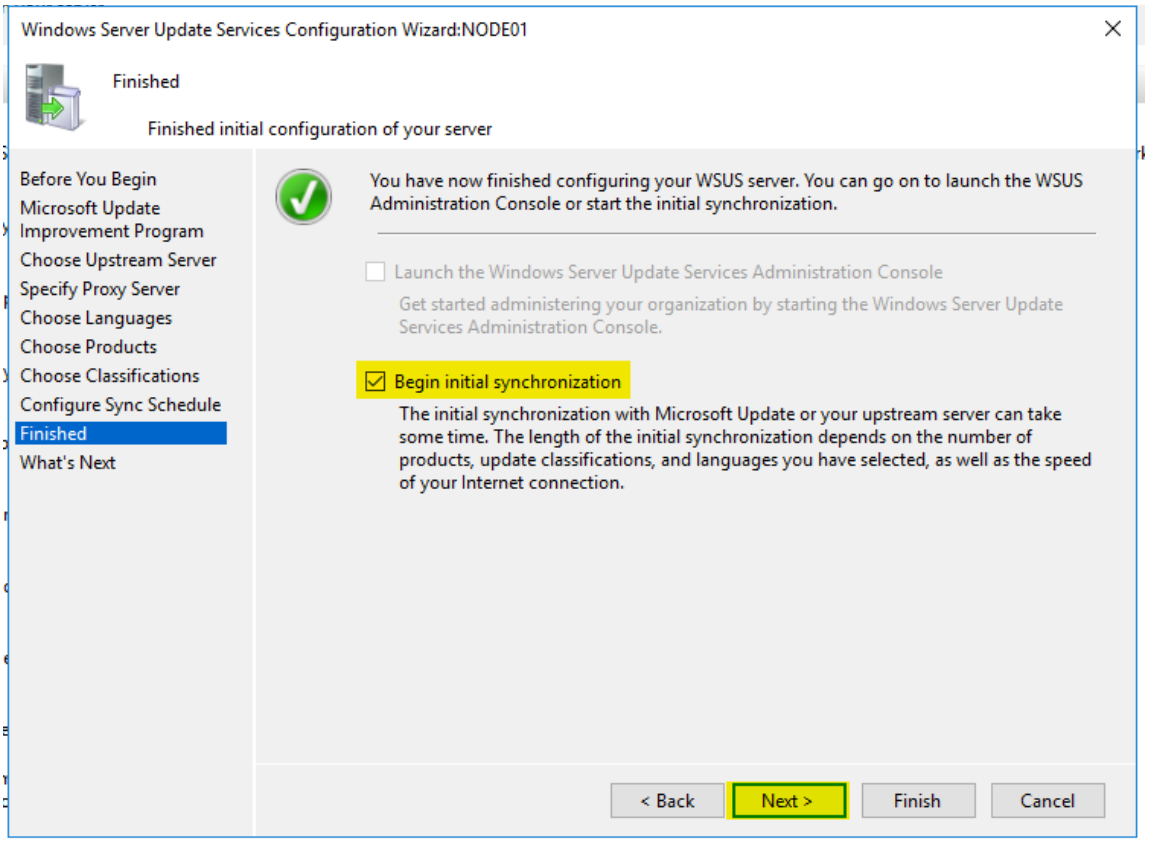
Select the required classification:



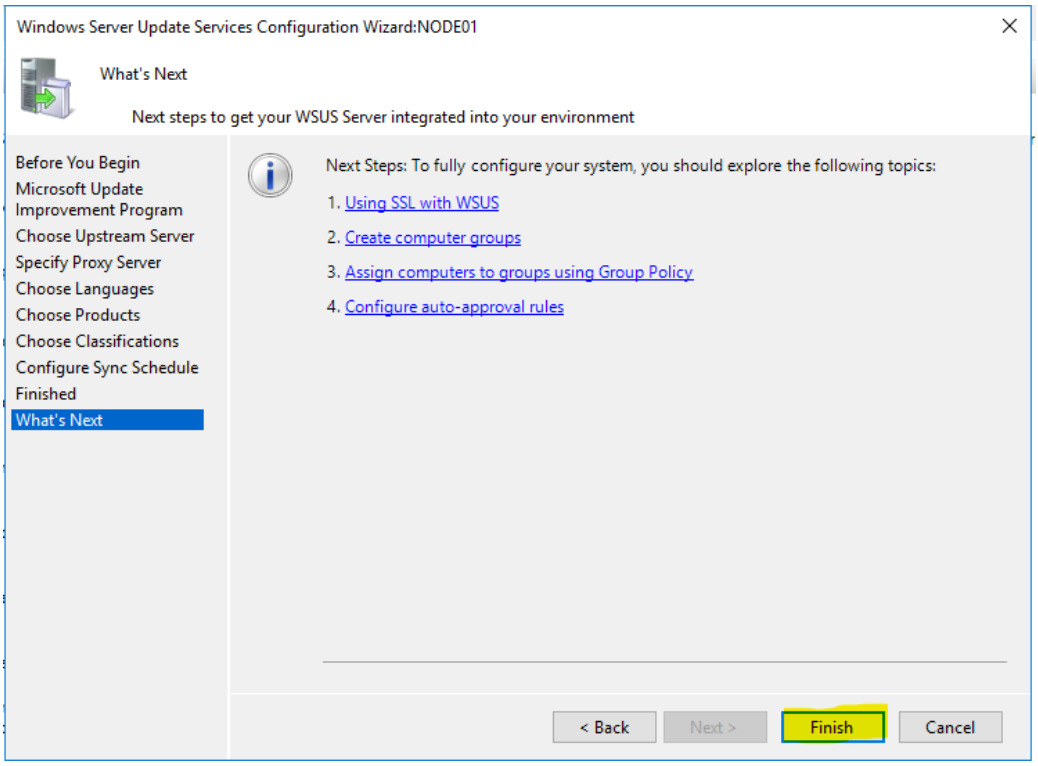
Select the sync time. We will select Manually as we will be using GPO for the updates:



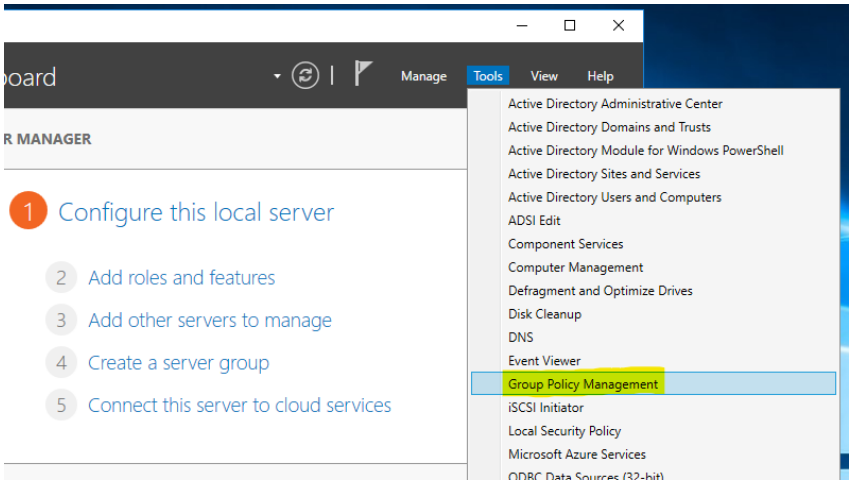
Check “Begin initial sync”:



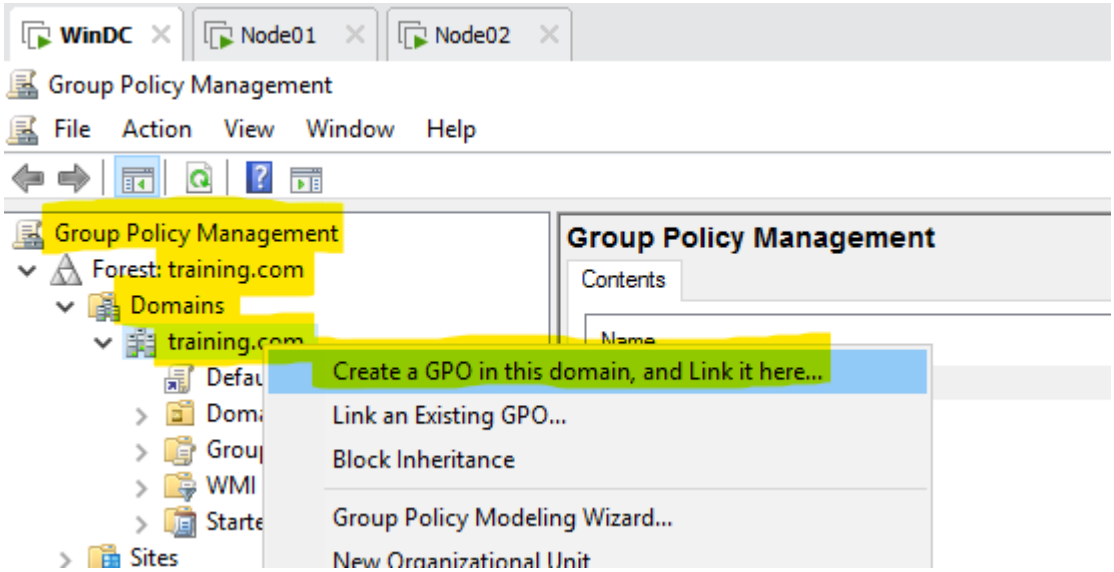
Finish the configuration:



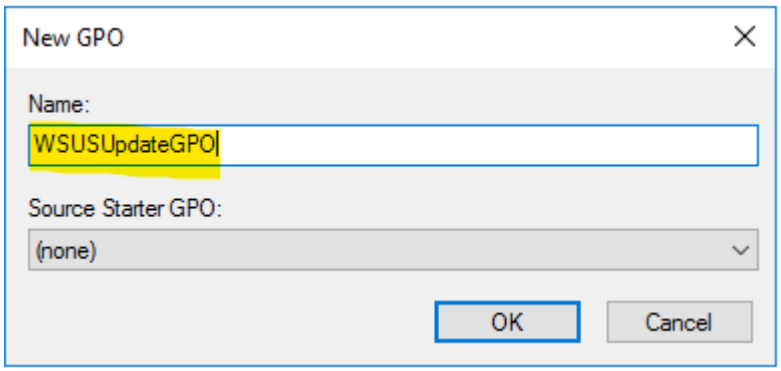
Configuring Group Policy for WSUS on DC machine:



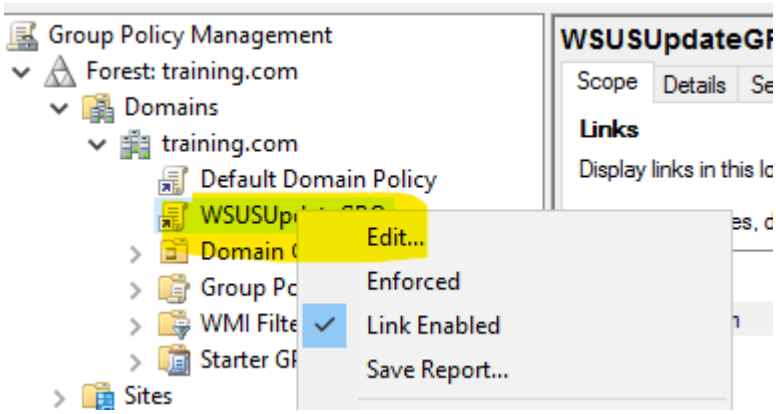
Create a new GPO:



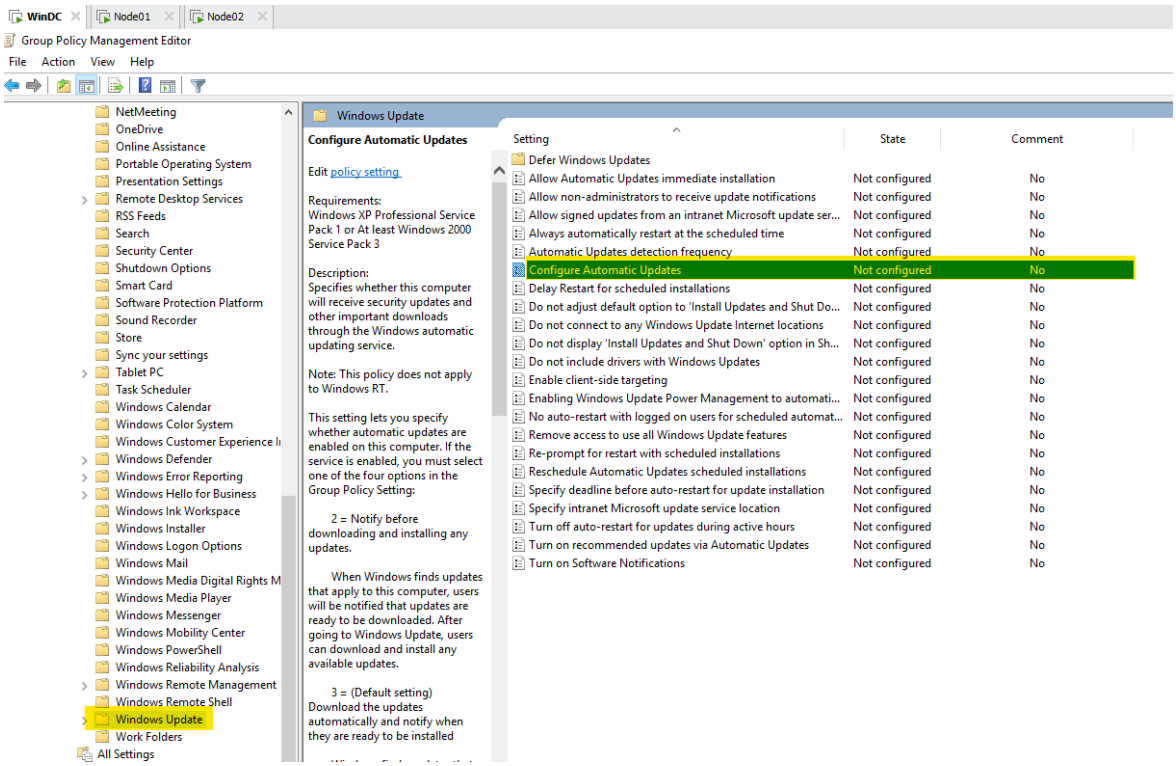
Give any name to it.



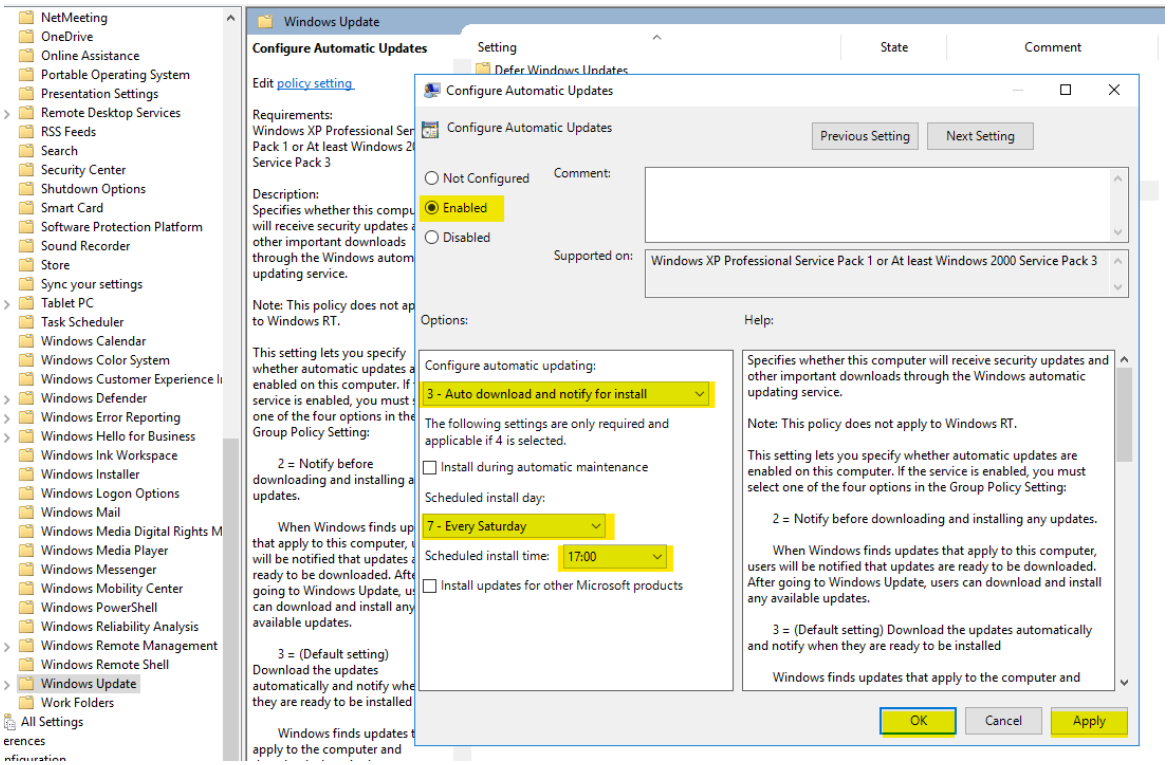
Right click and edit it:



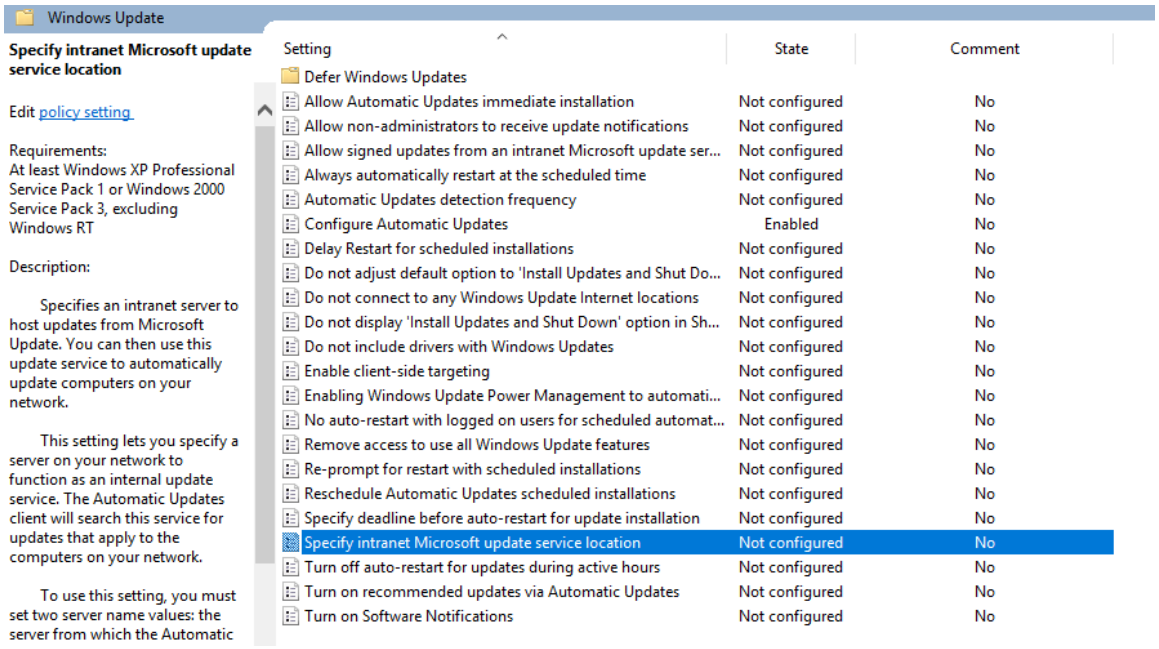
Go to: Computer configuration → Policies → Administrative Templates → Windows Components → Windows updates



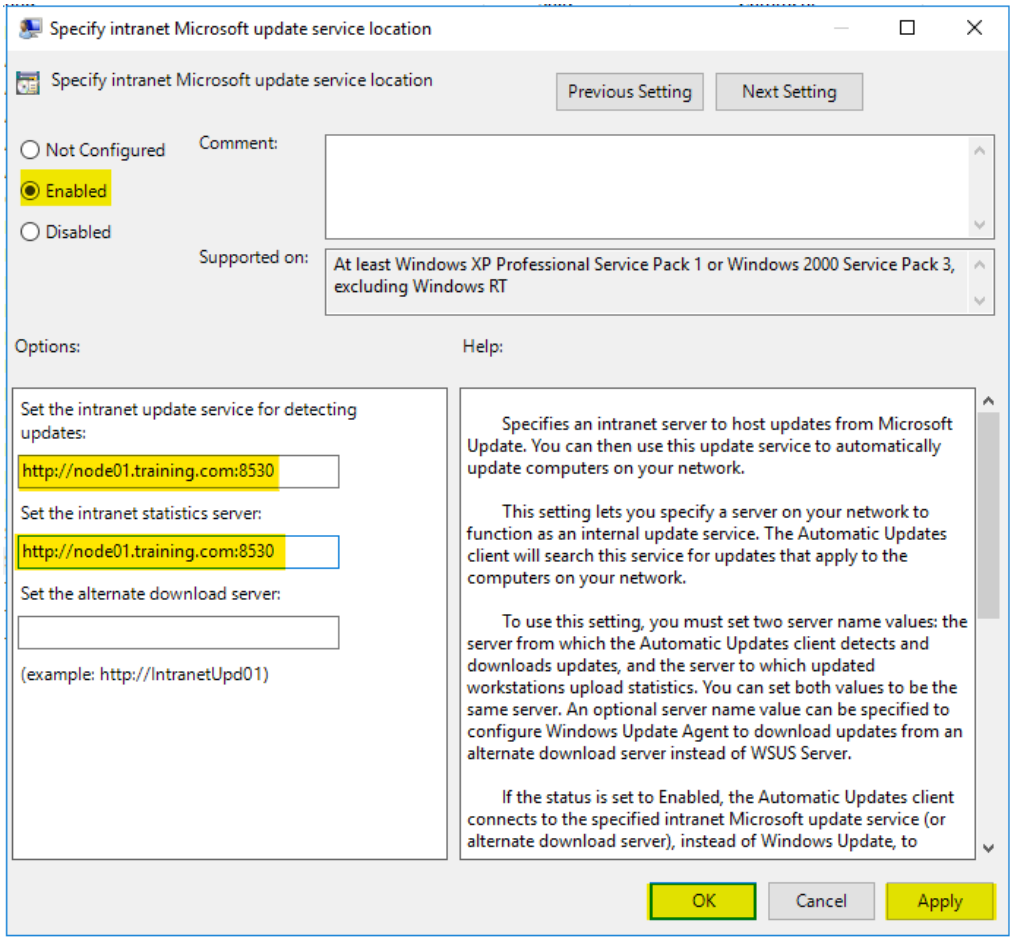
Double-click on the policy & fill details:



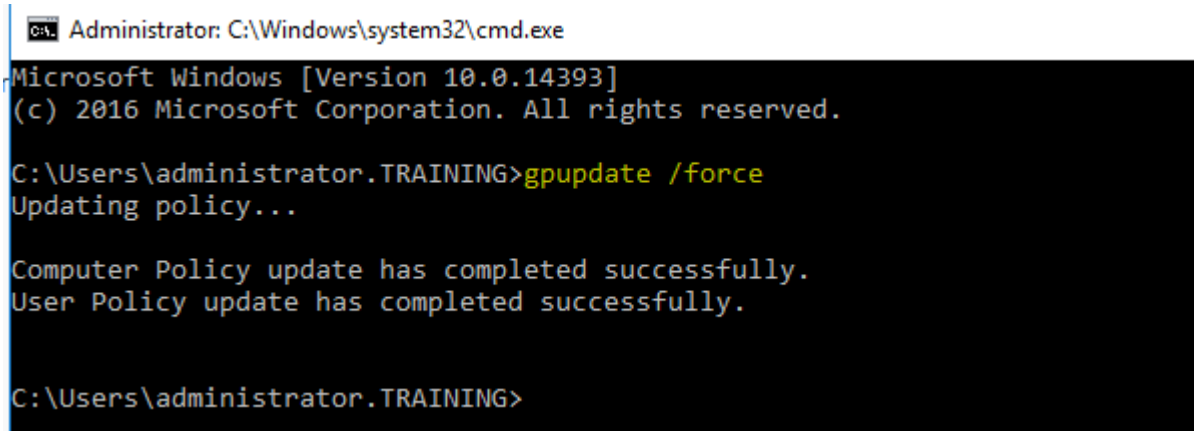
Next Specify Intranet Microsoft Update Service Location (within same GPO):



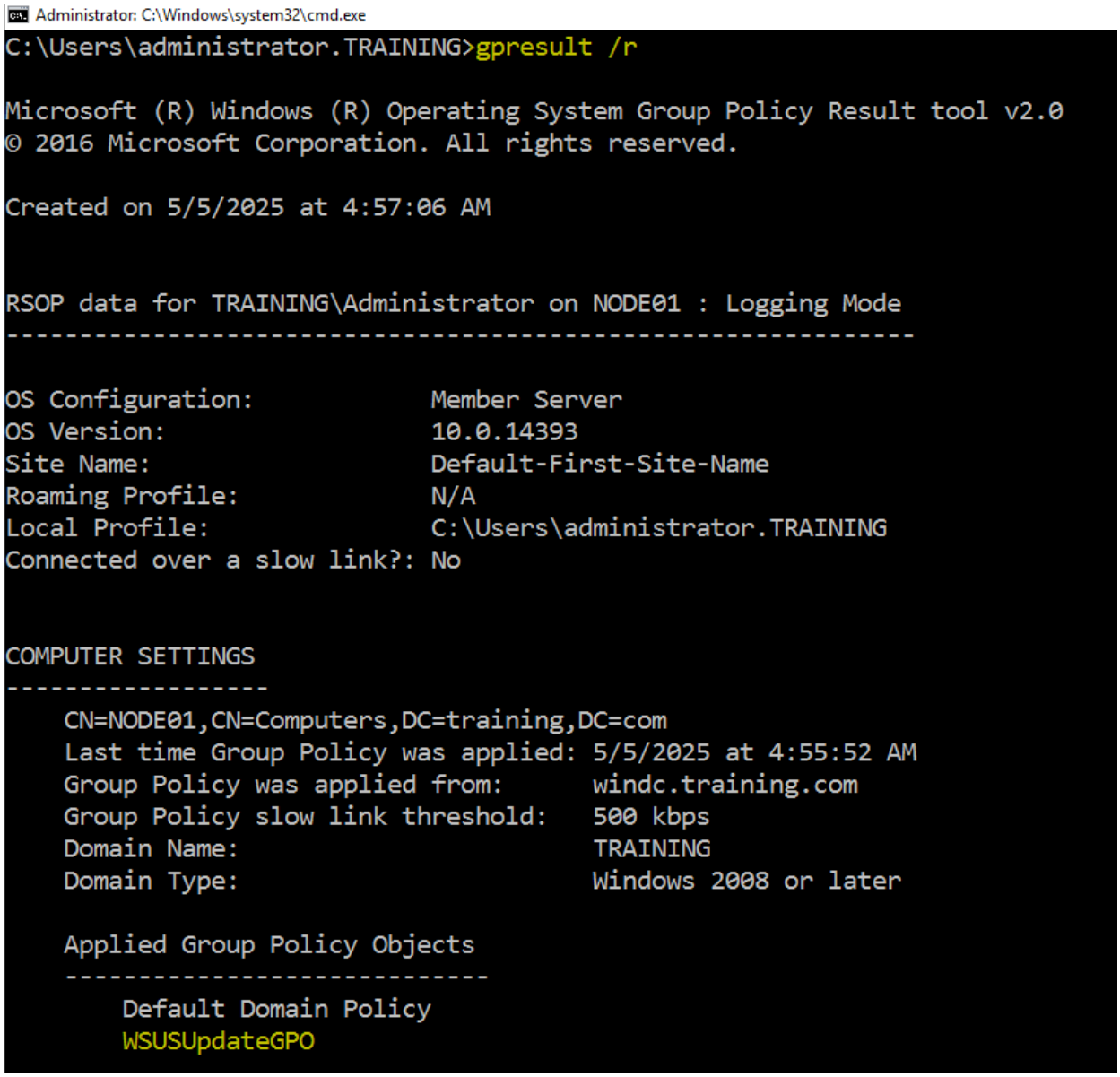
Set URL as http://node01.training.com:8530



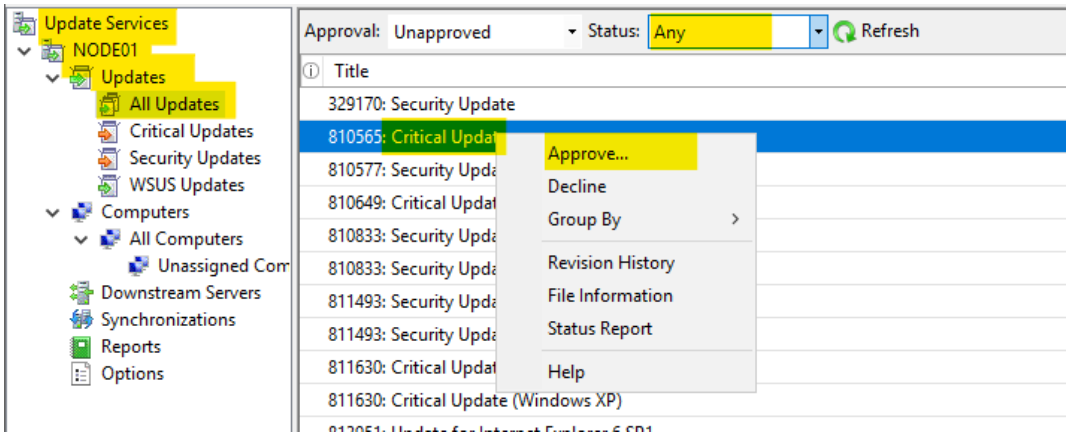
Now on clients, update the group policy:



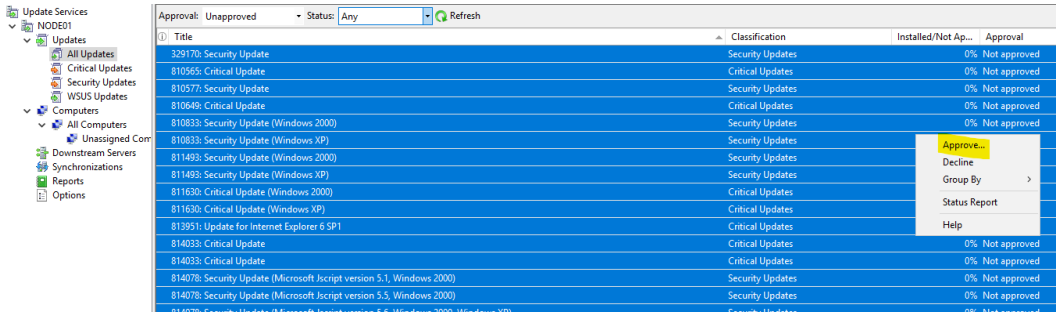
Listing the policy on client side (cmd: gpresult /r):



To approve the updates:



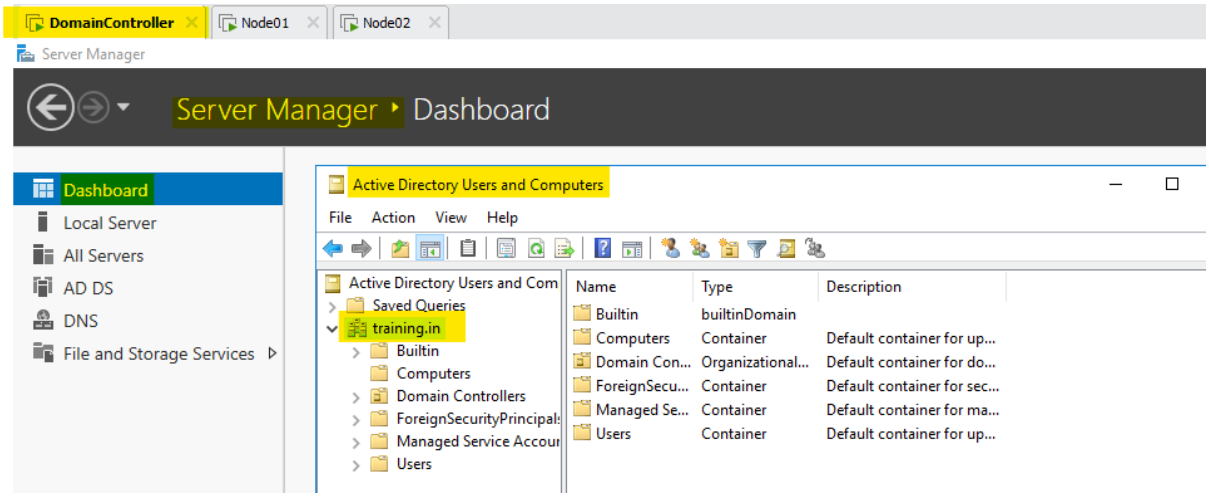
Or you can select All by pressing CTRL+A and right-click to approve them all:



Note – WSUS is now configured and ready to patch/update the nodes/machines within your domain.

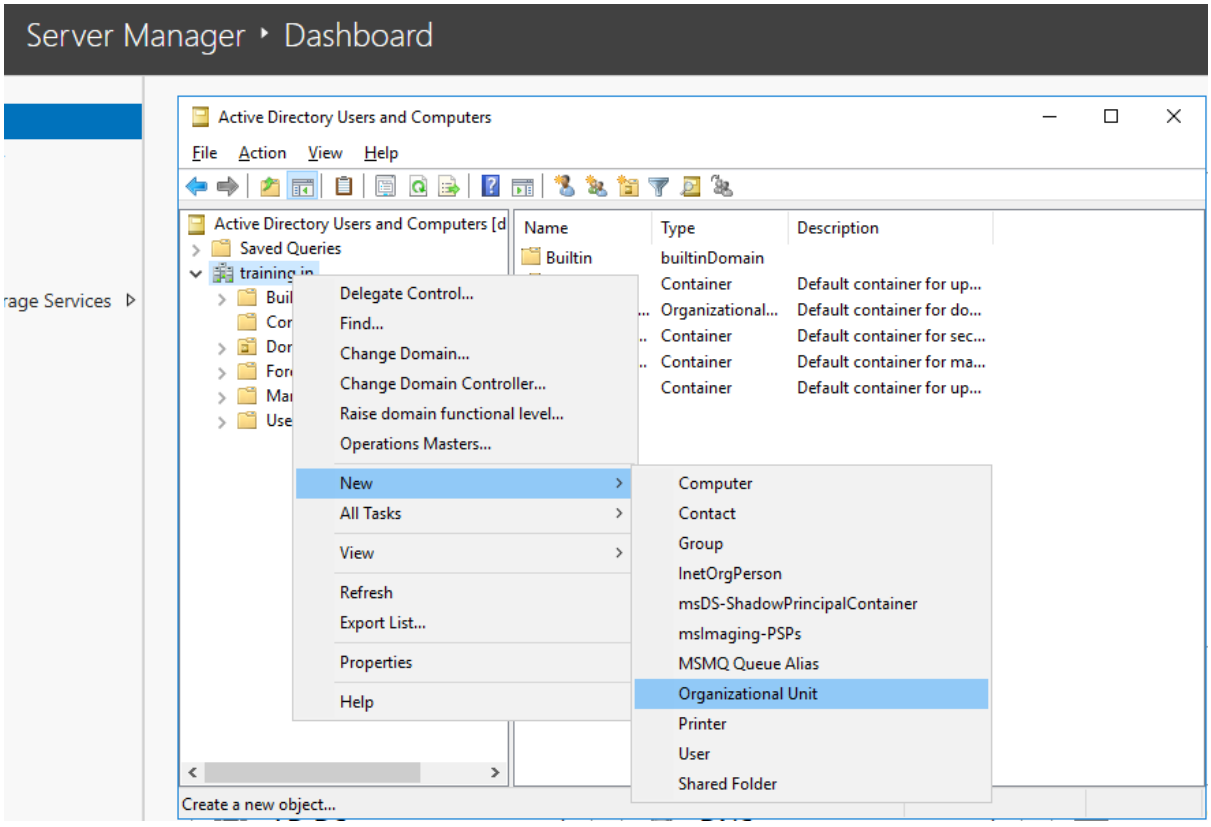
Creating a new user and adding this user to a new OU.

DC → Dashboard → Tools → Active Directory Users and Computers

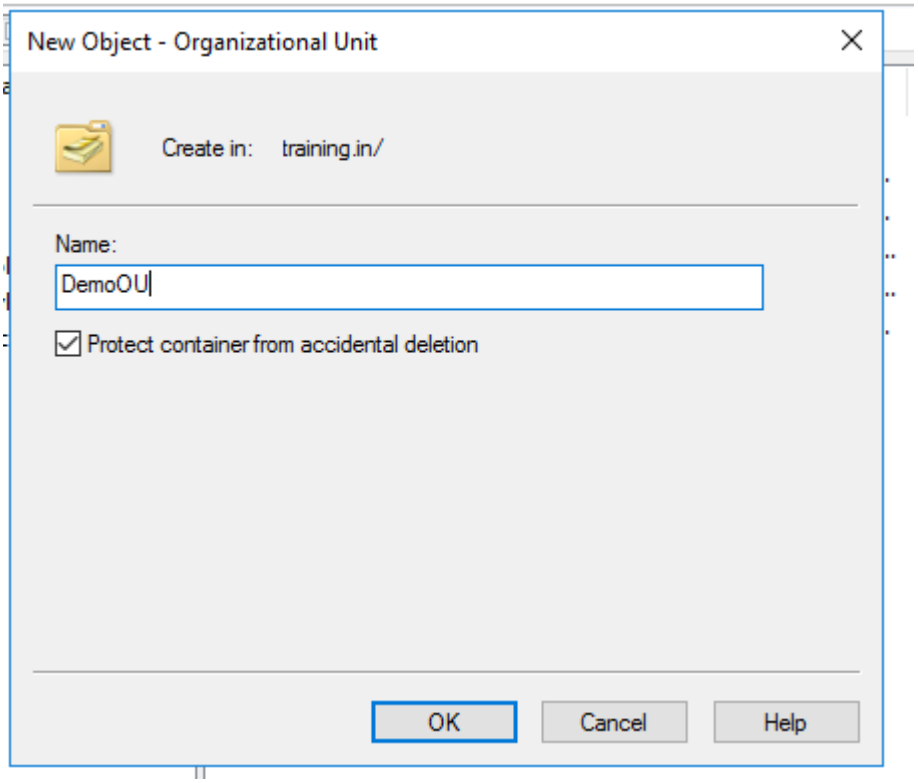


To create a new Organizational Unit (OU)

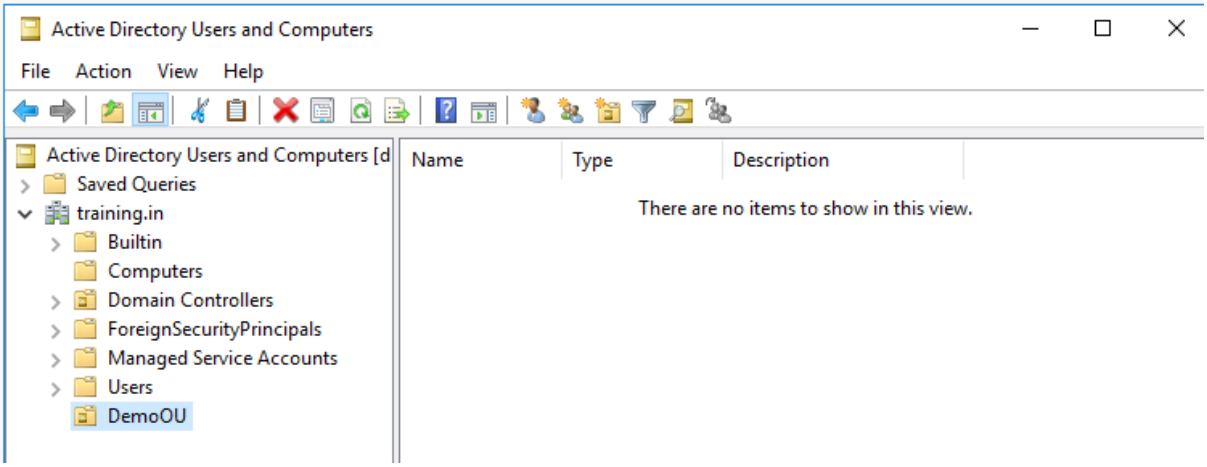
Right-click on the domain (training.in) → New → Organizational Unit (OU)



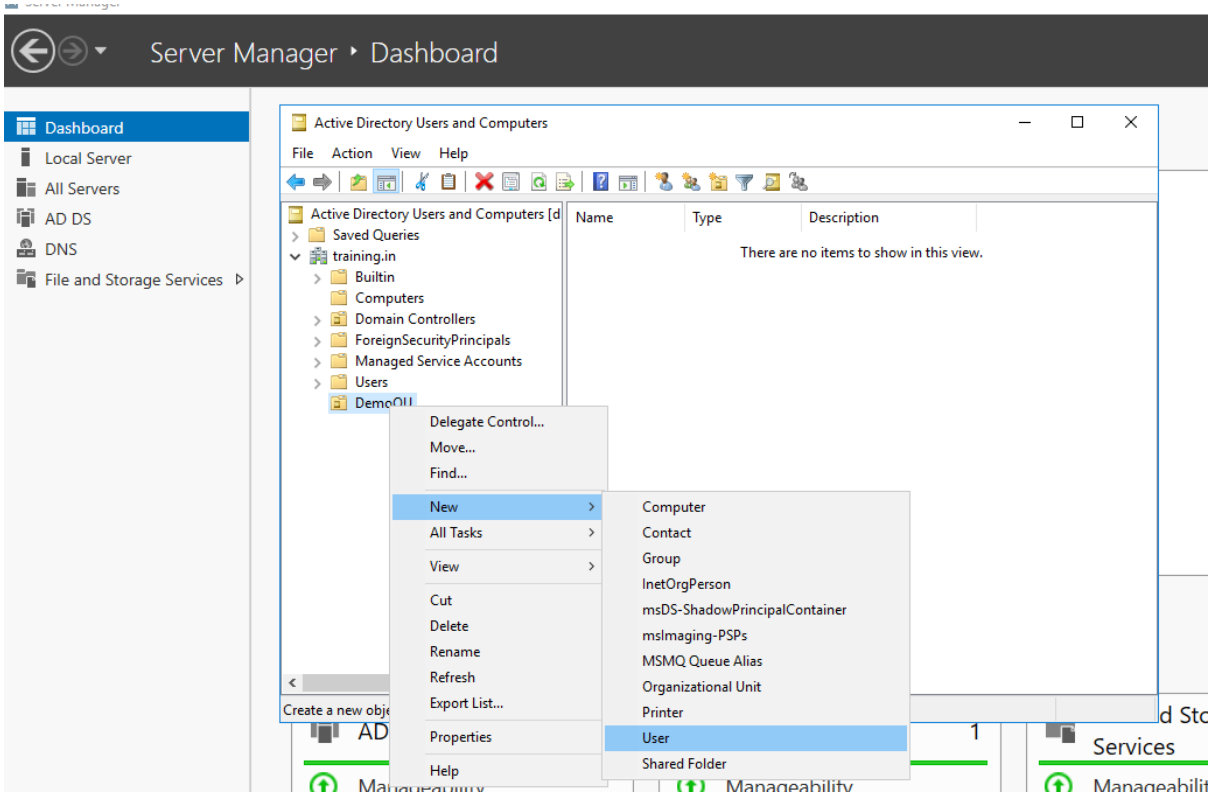
Give a name to this OU and click OK



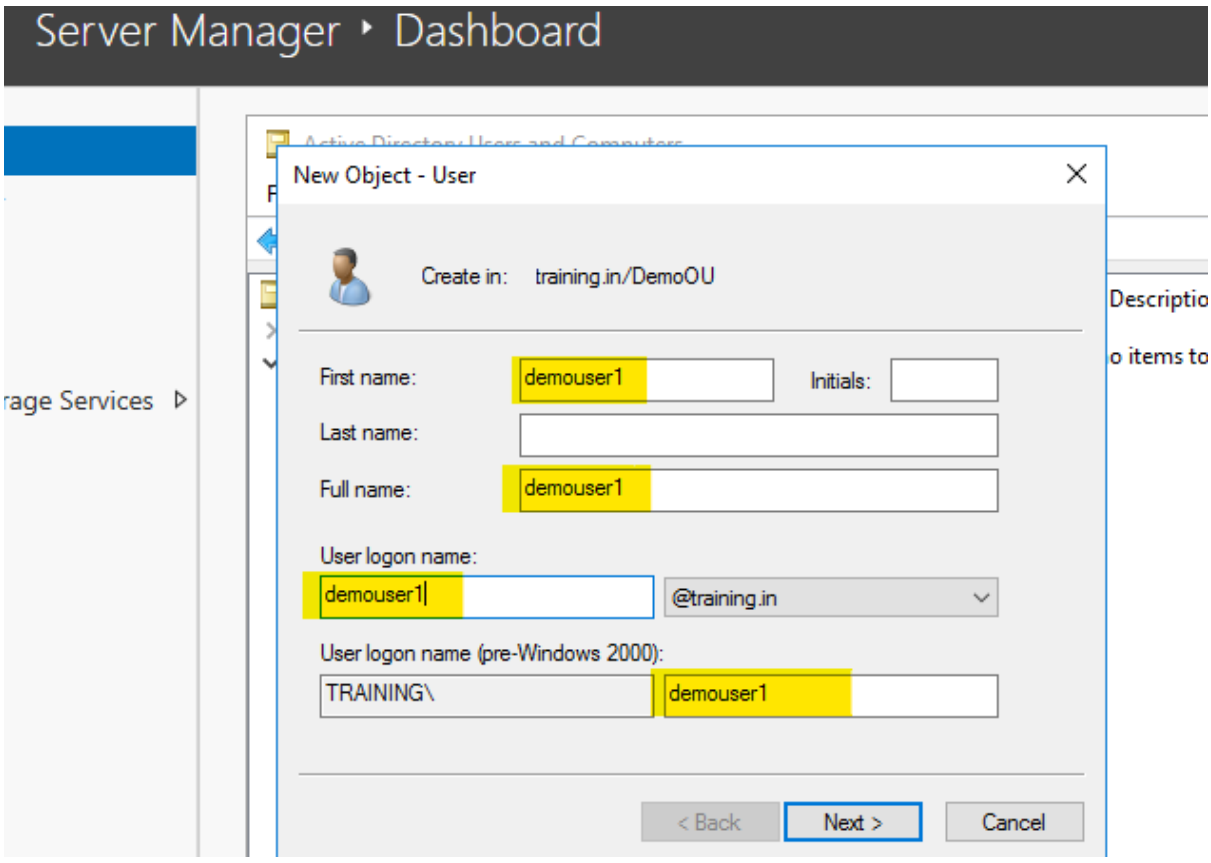
And verify on the console.



Now creating a user within this OU.

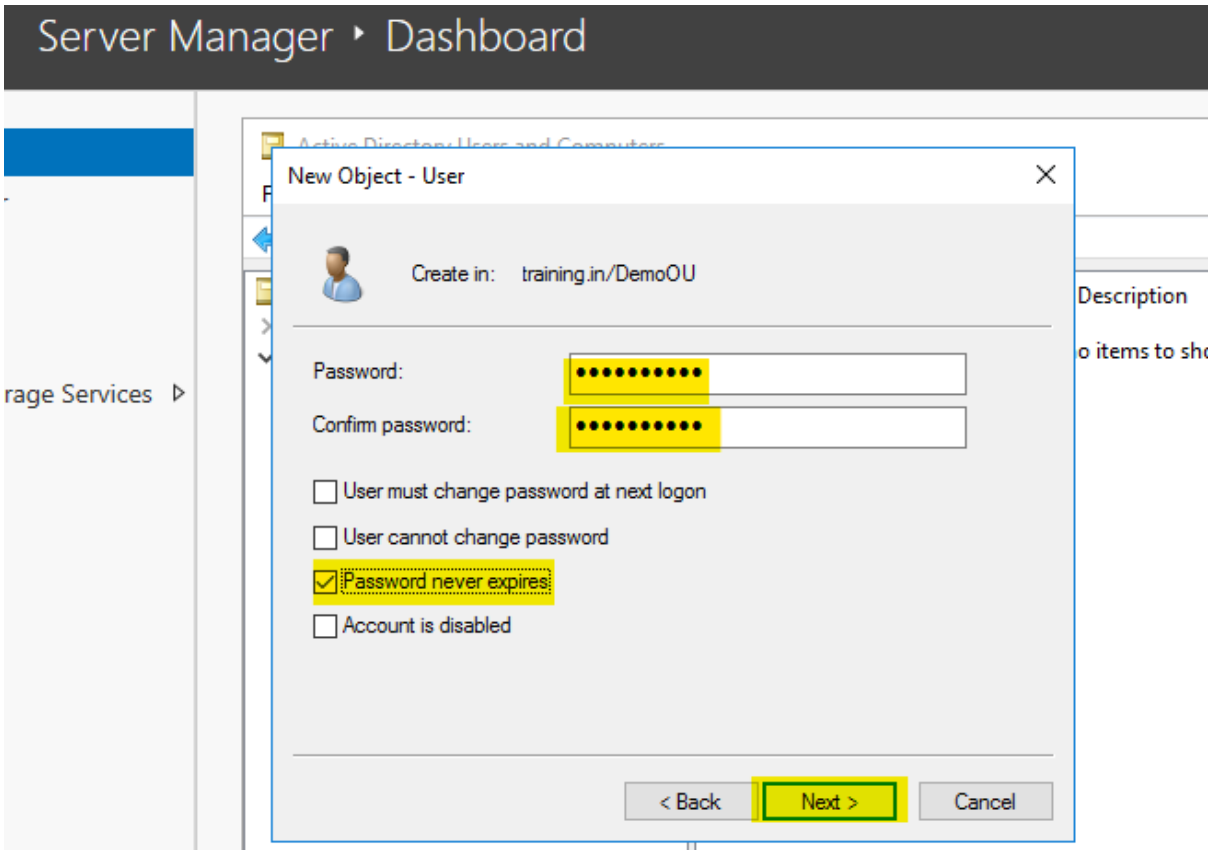


Provide a username (demouser1 in my case)

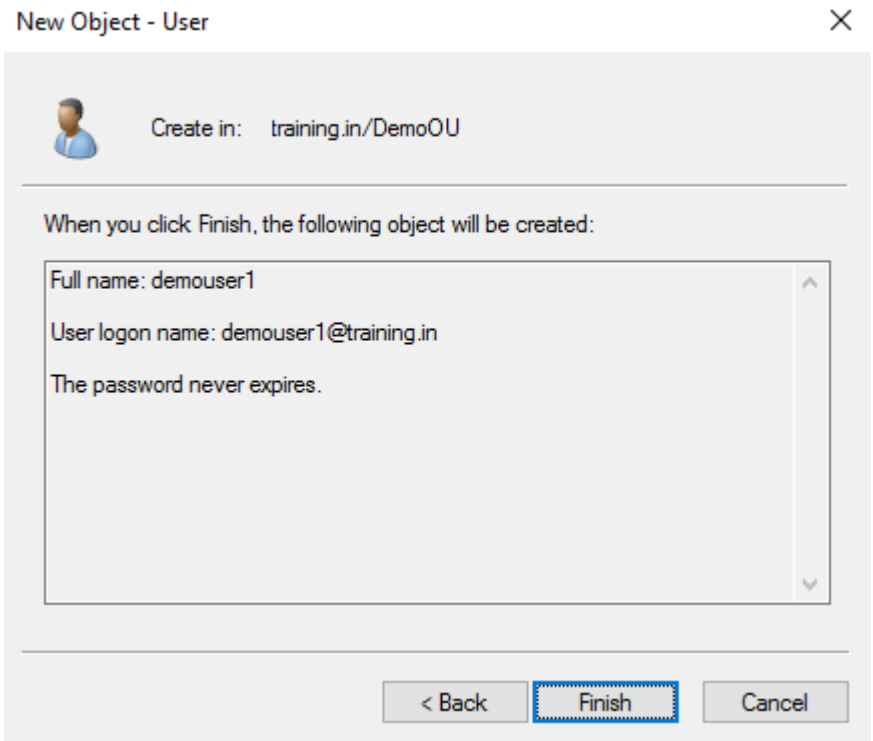


Click on Next.

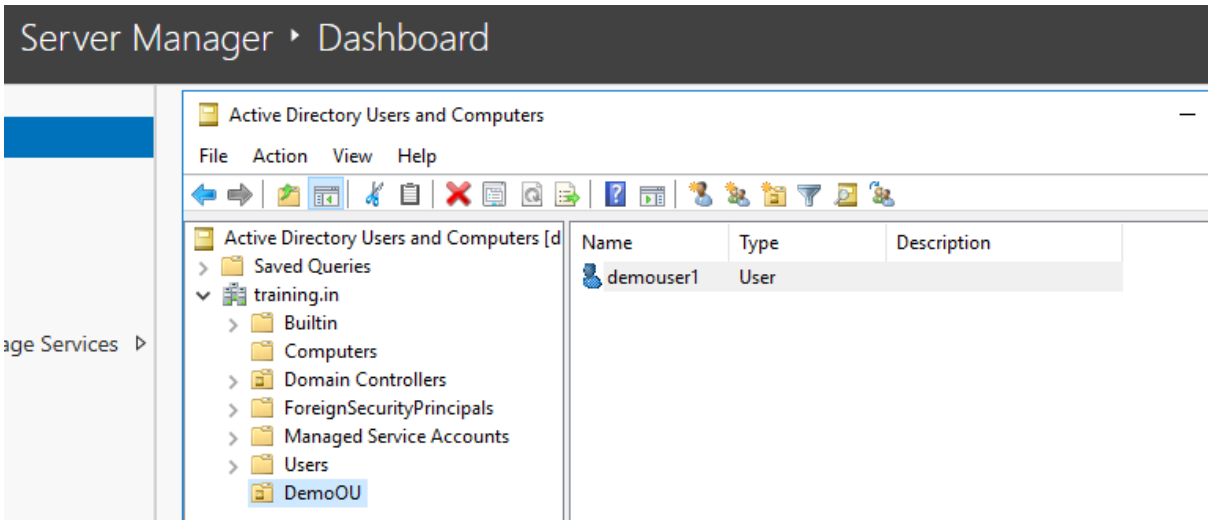
Provide a strong password and click Next:



Verify & click Finish

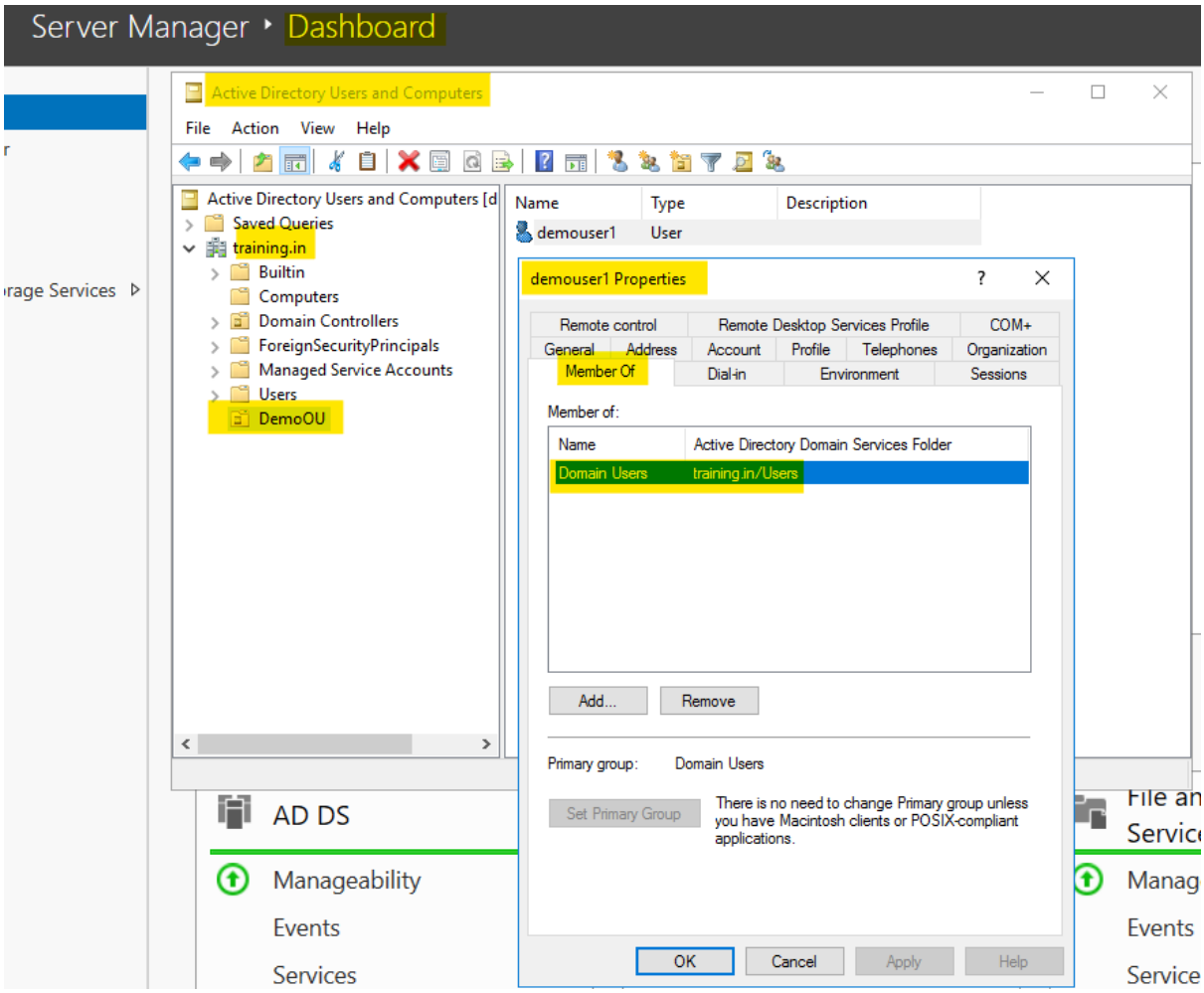


Verify:

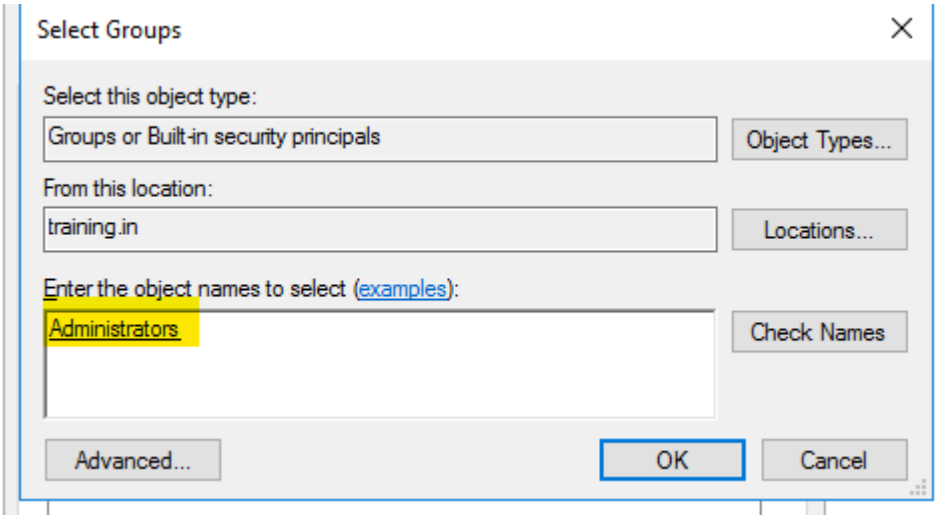

Server Manager ‣ Dashboard
Active Directory Users and Computers
File Action View Help
Active Directory Users and Computers [d
Saved Queries
training.in
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accounts
Users
DemoOU
Name
Type
Description
demouser1
User

Providing “Administrator” access to this new user.

DC → Dashboard → Tools → Active Directory Users and Computers → training.in → DemoOU → demouser1 → Right-click → Properties → Member Of

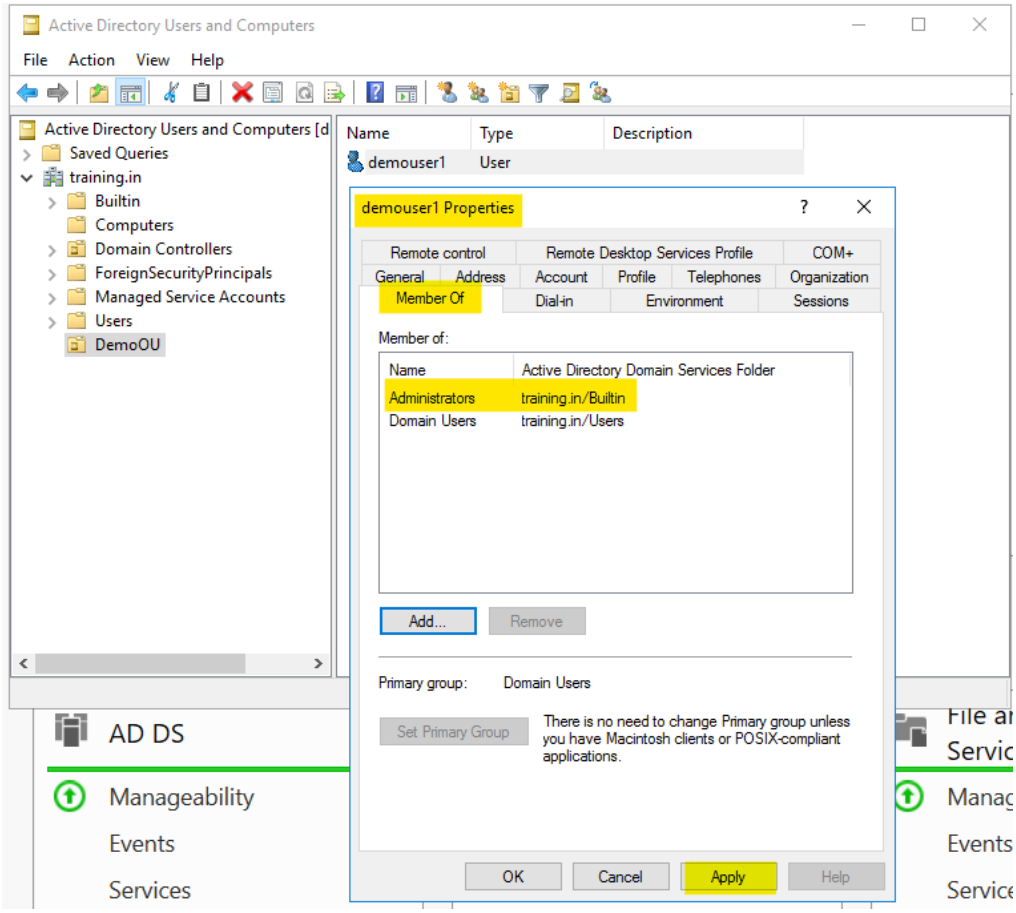


Click on Add button and search for keyword “Admin” → Check Names



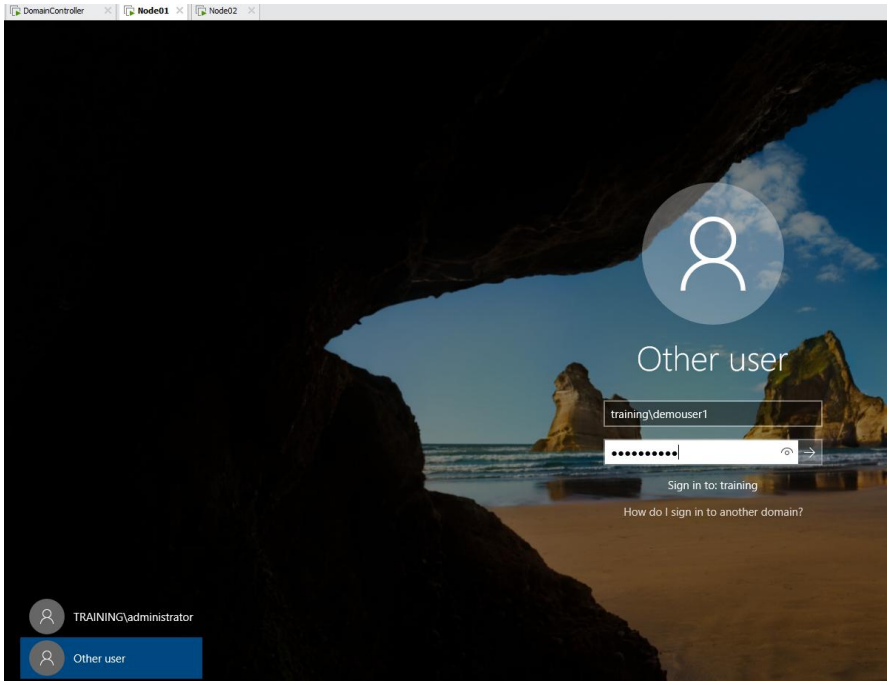
Once “administrators” appears, click OK.

And verify:

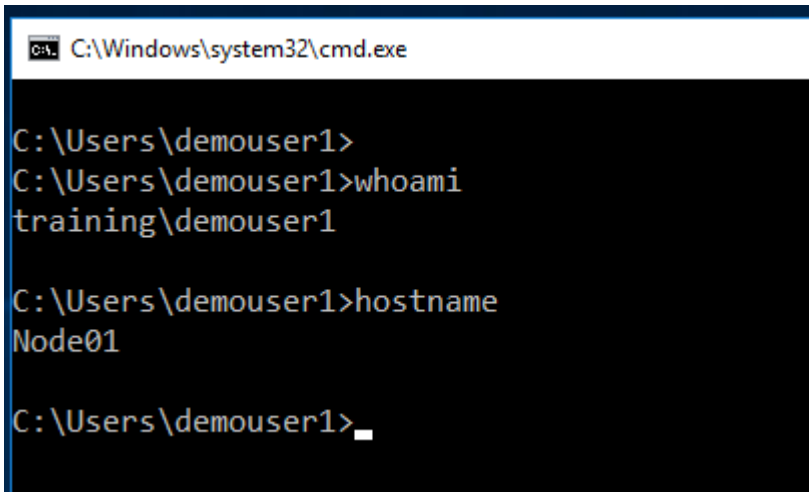


Click on Apply → OK and that's it.

Now logging in with this new user (with admin) privileges on Node01/Node02 (any). First sign-out from any existing user and login again using "Other User"



Verify:


C:\Windows\system32\cmd.exe
C:\Users\demouser1>
C:\Users\demouser1>whoami
training\demouser1
C:\Users\demouser1>hostname
Node01
C:\Users\demouser1>

Creating users in bulk using PowerShell script with “Domain Users” permissions.

PowerShell Code:

```
cls
$Users = Import-csv "C:\Users\Administrator\Desktop\BulkUserCreation\user-details.csv"
foreach ($User in $Users)
{
        $Username = $User.username
        $Firstname = $User.firstname
        $Lastname = $User.lastname
        $OU = $User.ou
        $Password = $User.Password
        $email = $User.email
  $groupname = "OU=DemoOU,DC=training,DC=in"

        if (Get-ADUser -F {SamAccountName -eq $Username})
        {
                Write-Warning "A user account with username $Username already exist."
        }
        else
        {
        New-ADUser `
        -SamAccountName $Username `
        -UserPrincipalName "$Username@training.in" `
        -Name "$Firstname $Lastname" `
        -GivenName $Firstname `
        -Surname $Lastname `
        -Enabled $True `
        -DisplayName "$Lastname, $Firstname" `
        -Path $OU `
        -EmailAddress $email `
        -AccountPassword (convertto-securestring $Password -AsPlainText -Force) -
ChangePasswordAtLogon $True

  # Add-ADGroupMember -Identity $groupname -Members $Username

  Write-Host "$username " -ForegroundColor Cyan -NoNewline
  write-host "is created"

        }
}
Add-ADGroupMember -Identity "Domain Users" -Members $groupname
```

CSV file data:

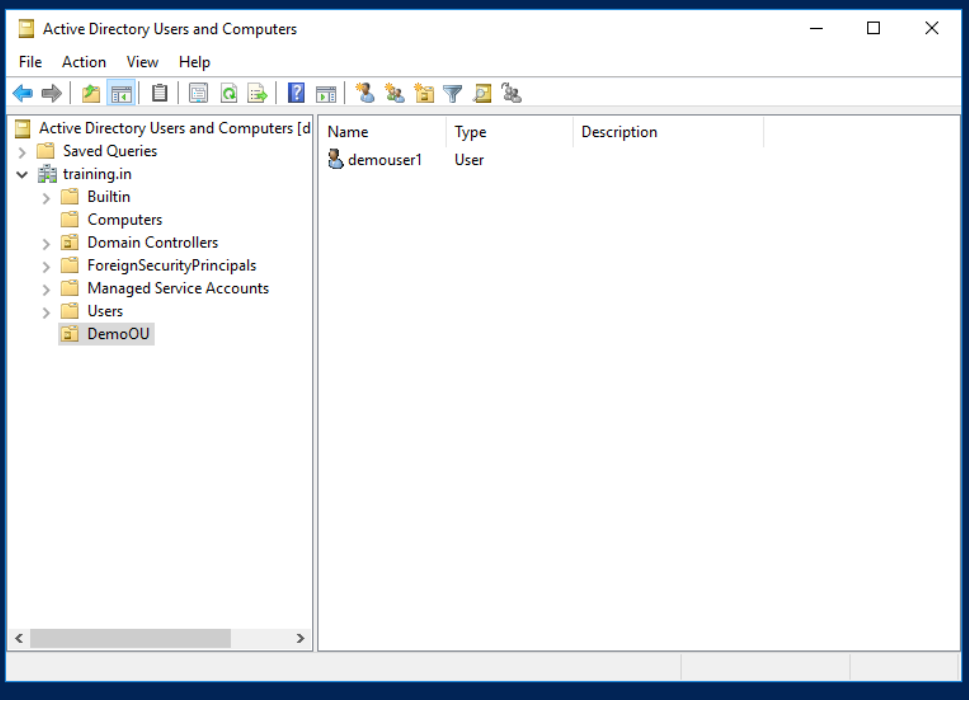
```
Username,Firstname,Lastname,OU,Password,Email
devasenapathy,K,Devasenapathy,"OU=DemoOU,DC=training,DC=in",pass@word1,devasenapathy@training.in
sasikumar,S,Sasikumar,"OU=DemoOU,DC=training,DC=in",pass@word1,sasikumar@training.in
hemaambiha,A,Hema Ambiha,"OU=DemoOU,DC=training,DC=in",pass@word1,hemaambiha@training.in
rutravigneshwaran,P,Rutravigneshwaran,"OU=DemoOU,DC=training,DC=in",pass@word1,rutravigneshwaran@training.in
krishnaveni,A,Krishnaveni,"OU=DemoOU,DC=training,DC=in",pass@word1,krishnaveni@training.in
nivashini,G,Nivashini,"OU=DemoOU,DC=training,DC=in",pass@word1,nivashini@training.in
sathiyapriya,Sathiya ,Priya,"OU=DemoOU,DC=training,DC=in",pass@word1,sathiyapriya@training.in
nalini, K,Nalini,"OU=DemoOU,DC=training,DC=in",pass@word1,nalini@training.in
bhuvaneswari, K ,Bhuvaneswari,"OU=DemoOU,DC=training,DC=in",pass@word1,bhuvaneswari@training.in
kavitha,K,KAVITHA,"OU=DemoOU,DC=training,DC=in",pass@word1,kavitha@training.in
prince,Prince,Jeyaseelan,"OU=DemoOU,DC=training,DC=in",pass@word1,prince@training.in
sreepriya, S,Sreepriya,"OU=DemoOU,DC=training,DC=in",pass@word1,sreepriya@training.in
sujatha, H,Sujatha,"OU=DemoOU,DC=training,DC=in",pass@word1,sujatha@training.in
sripradha, SriPradha,,"OU=DemoOU,DC=training,DC=in",pass@word1,sripradha@training.in
nilkanteshwar, Nilkanteshwar,Dnyandeo,"OU=DemoOU,DC=training,DC=in",pass@word1,nilkanteshwar@training.in
nitish, Nitish ,Shankar,"OU=DemoOU,DC=training,DC=in",pass@word1,nitish@training.in
ramrao,Datta,Ramrao,"OU=DemoOU,DC=training,DC=in",pass@word1,ramrao@training.in
tanaji,Tanaji,Shivaji,"OU=DemoOU,DC=training,DC=in",pass@word1,tanaji@training.in
sambhaji,Sambhaji,Vamanrao,"OU=DemoOU,DC=training,DC=in",pass@word1,sambhaji@training.in
balaji,Balaji,Madhavrao,"OU=DemoOU,DC=training,DC=in",pass@word1,balaji@training.in
nagnath,Nagnath,Atmaram,"OU=DemoOU,DC=training,DC=in",pass@word1,nagnath@training.in
geetha,GEETHA,DHANALAKSHMI,"OU=DemoOU,DC=training,DC=in",pass@word1,geetha@training.in
jereil,David,Jereil,"OU=DemoOU,DC=training,DC=in",pass@word1,jereil@training.in
joseph,Joseph,Paramasivam,"OU=DemoOU,DC=training,DC=in",pass@word1,joseph@training.in
monica,CYNTHIA,MONICA,"OU=DemoOU,DC=training,DC=in",pass@word1,monica@training.in
eliahim,Eliahim,Jeevarj,"OU=DemoOU,DC=training,DC=in",pass@word1,eliahim@training.in
gayathri,B,GAYATHRI,"OU=DemoOU,DC=training,DC=in",pass@word1,gayathri@training.in
james,James,Manoharan,"OU=DemoOU,DC=training,DC=in",pass@word1,james@training.in
sriram,N,Sriram,"OU=DemoOU,DC=training,DC=in",pass@word1,sriram@training.in
maharasan,S,Maharasan,"OU=DemoOU,DC=training,DC=in",pass@word1,maharasan@training.in
rajesh,Rajesh,,"OU=DemoOU,DC=training,DC=in",pass@word1,rajesh@training.in
surendar,Surendar,,"OU=DemoOU,DC=training,DC=in",pass@word1,surendar@training.in
aravind, B, Aravind,"OU=DemoOU,DC=training,DC=in",pass@word1,aravind@training.in
dhileeban, A, Dhileeban,"OU=DemoOU,DC=training,DC=in",pass@word1,dhileeban@training.in
dharaneesh, S, Dharaneesh,"OU=DemoOU,DC=training,DC=in",pass@word1,dharaneesh@training.in
```

Store these two files in any location and execute them using PowerShell ISE.

Before executing the script:

```
Import Bulk Users.ps1
  1   cls
  2   $Users = Import-csv "C:\Users\Administrator\Desktop\BulkUserCreation\user-details.csv"
  3   foreach ($User in $Users)
  4   {...}
 38   Add-ADGroupMember -Identity "Domain Users" -Members $groupname
```

```
PS C:\Users\Administrator\Desktop\BulkUserCreation>
```

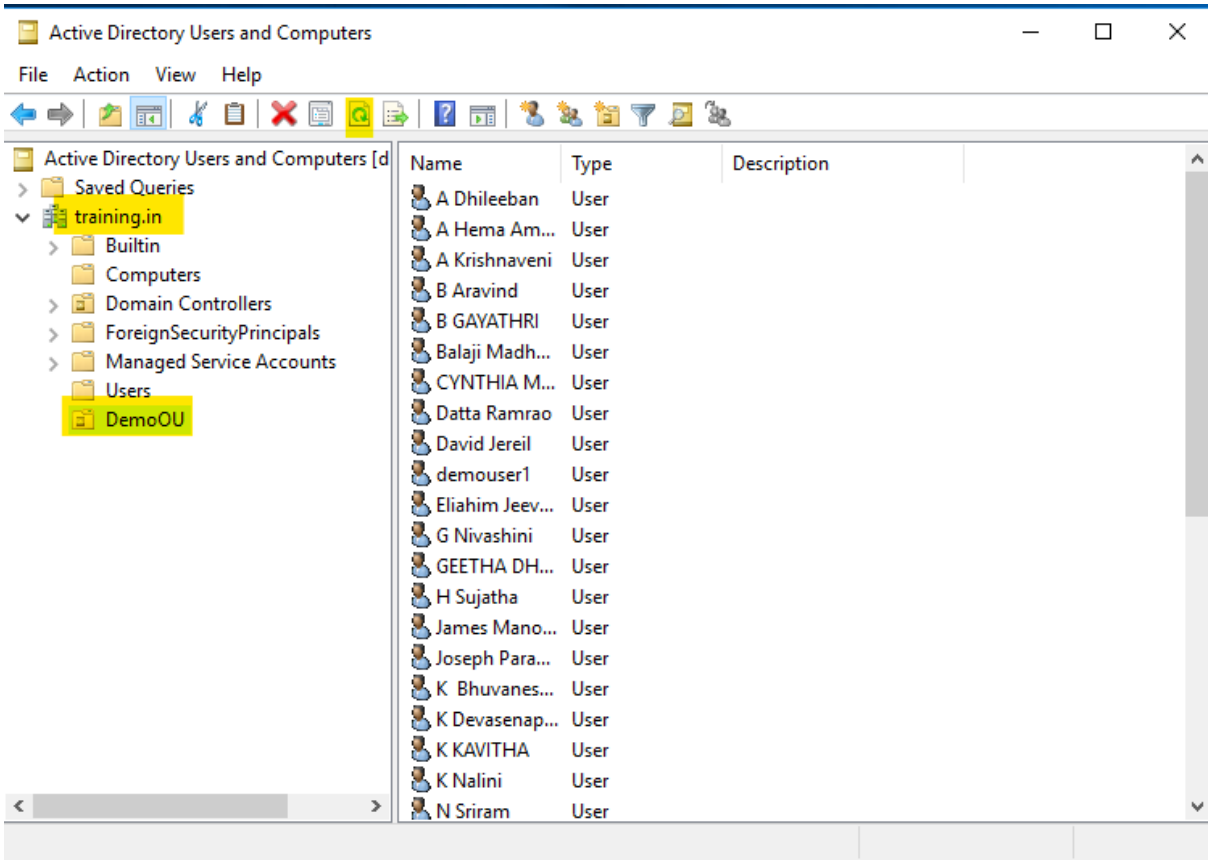


After:

```
devasenapathy is created
sasikumar is created
hemaambiha is created
rutravigneshwaran is created
krishnaveni is created
nivashini is created
sathiyapriya is created
nalini is created
bhuvaneswari is created
kavitha is created
prince is created
sreepriya is created
sujatha is created
sripradha is created
nilkanteshwar is created
nitish is created
ramrao is created
tanaji is created
sambhaji is created
balaji is created
nagnath is created
geetha is created
jereil is created
joseph is created
monica is created
eliahim is created
gayathri is created
james is created
sriram is created
maharasan is created
rajesh is created
surendar is created
aravind is created
dhileeban is created
dharaneesh is created
Add-ADGroupMember : Cannot find an obj
At C:\Users\Administrator\Desktop\Bulk
+ Add-ADGroupMember -Identity "Domain
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNo
    + FullyQualifiedErrorId : SetADGro
```

```
Import Bulk Users.ps1
  1   cls
  2   $Users = Import-csv "C:\Users\Administrator\Desktop\BulkUserCreation\user-details.csv"
  3   foreach ($User in $Users)
  4   {
  5       $Username = $User.username
  6       $Firstname = $User.firstname
  7       $Lastname = $User.lastname
  8       $OU = $User.ou
  9       $Password = $User.Password
 10       $email = $User.email
 11       $groupname = "OU=DemoOU,DC=training,DC=in"
 12
 13       if (Get-ADUser -F {SamAccountName -eq $Username})
 14       {
 15           Write-Warning "A user account with username $Username already exist."
 16       }
 17       else
 18       {
 19       New-ADUser `
 20       -SamAccountName $Username `
 21       -UserPrincipalName "$Username@training.in" `
 22       -Name "$Firstname $Lastname" `
 23       -GivenName $Firstname `
 24       -Surname $Lastname `
 25       -Enabled $True `
 26       -DisplayName "$Lastname, $Firstname" `
 27       -Path $OU `
 28       -EmailAddress $email `
 29       -AccountPassword (convertto-securestring $Password -AsPlainText -Force) -ChangePasswordAtLogon $True
 30
 31       # Add-ADGroupMember -Identity $groupname -Members $Username
 32
 33       Write-Host "$username " -ForegroundColor Cyan -NoNewline
 34       write-host "is created"
 35
 36       }
 37   }
 38   Add-ADGroupMember -Identity "Domain Users" -Members $groupname
```

Just refresh the new OU and verify.



What is Failover Clustering?

What is Failover Clustering?

Failover Clustering in Windows Server is a high-availability solution that allows multiple servers (called nodes) to work together to provide continuous access to applications and services. If one node fails, another takes over automatically — this is called failover.

Objective of Failover Clustering

- Minimize downtime for critical applications/services.
- Provide automatic recovery from hardware/software failures.
- Ensure continuous availability of services like file servers, VMs, databases, and applications.

Key Components of a Failover Cluster

Component	Description
Nodes	Physical or virtual servers that are part of the cluster. Each node runs Windows Server.
Cluster Network	Networks used for communication between nodes (heartbeat, replication, client access).
Shared Storage	A common storage accessible by all nodes, used for storing clustered resources (e.g., SAN, iSCSI).
Quorum	A configuration to determine the majority for cluster decisions, prevents split-brain scenarios.
Cluster Resources	Applications, services, or virtual machines managed by the cluster.
Cluster Group/Role	A logical group of resources that failover together (e.g., VM, file server role).
Witness	A tie-breaker vote in the quorum (can be a disk witness, file share witness, or cloud witness).
Cluster Name Object (CNO)	A computer object in Active Directory representing the cluster.

How Does Failover Clustering Work?

1) Multiple nodes are connected to a shared storage system and cluster network.
2) One node actively runs the clustered service (active node).
3) Other nodes are on standby (passive).
4) Health of nodes is monitored via heartbeat signals.
5) If the active node fails, a passive node takes over and brings the resource online — this is called failover.
6) Once the failed node is back online, it can rejoin the cluster.

Cluster Quorum Models

Quorum Type	Description
Node Majority	Used when odd number of nodes. Majority of nodes must be online.
Node and Disk Majority	Even number of nodes. A disk (witness) adds a vote.
Node and File Share Majority	A file share acts as a witness. Useful for multi-site clusters.
Cloud Witness	Azure-based witness for hybrid/cloud-connected clusters.

Common Workloads for Failover Clustering

- Hyper-V Virtual Machines (High Availability VMs)
- SQL Server Failover Cluster Instances (FCI)
- File Server (Scale-Out File Server or General Purpose)
- Distributed Transaction Coordinator (DTC)
- iSCSI Target Server
- Print Services

Steps to Set Up Failover Clustering

1) Install Failover Clustering feature on all nodes:
    a. Install-WindowsFeature -Name Failover-Clustering -IncludeManagementTools
2) Validate the cluster configuration:
    a. Test-Cluster
3) Create the cluster:
    a. New-Cluster -Name MyCluster -Node Node1,Node2 -StaticAddress 192.168.1.100
4) Add Cluster Roles (VM, File Server, SQL, etc.)
5) Configure Quorum and Witness as per your design.
6) Test failover to verify high availability.

Cluster Storage Types

- Shared Disk (Fibre Channel, SAS, iSCSI)
- Cluster Shared Volumes (CSV)
    - Used in Hyper-V clusters for multiple nodes to access a shared volume simultaneously.
- Storage Spaces Direct (S2D)
    - Software-defined storage, removes the need for shared disk arrays.

Monitoring and Maintenance

- PowerShell Cmdlets:
- Get-Cluster
- Get-ClusterNode
- Move-ClusterGroup
- Get-ClusterLog

Failover Cluster vs. NLB

Feature	**Failover Cluster**	**Network Load Balancer (NLB)**
High Availability	Yes	Yes
Load Distribution	No	Yes
Shared Storage	Required	Not required
Application Statefulness	Supported	Not supported
Use Cases	VMs, SQL, file servers	Web apps, stateless services

Install and configure failover cluster role on Node01 and Node02

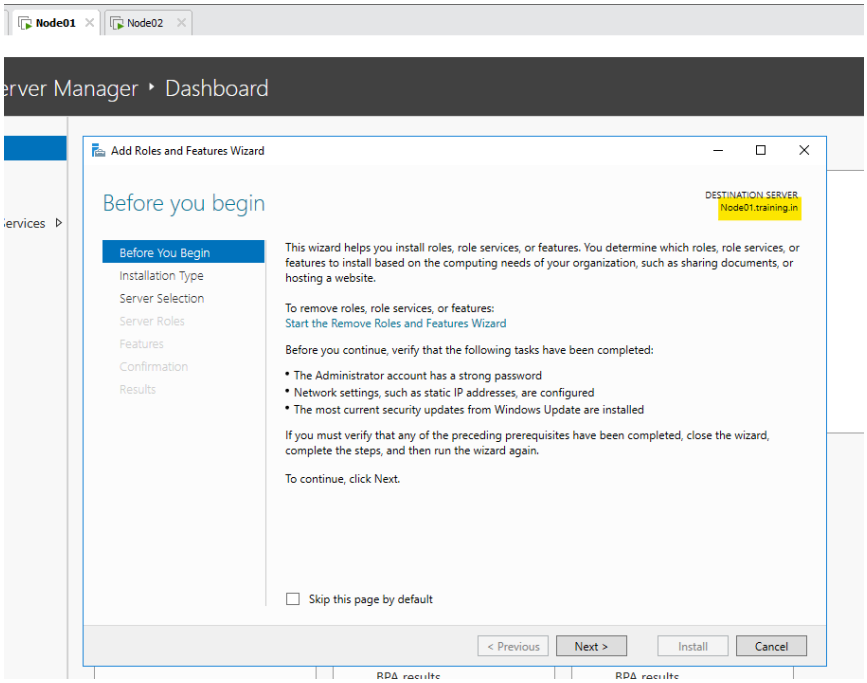
Note – before you proceed further, it's recommended to take the snapshot for all the VMs, in case you need to practise again.

To take snapshot, follow these steps:

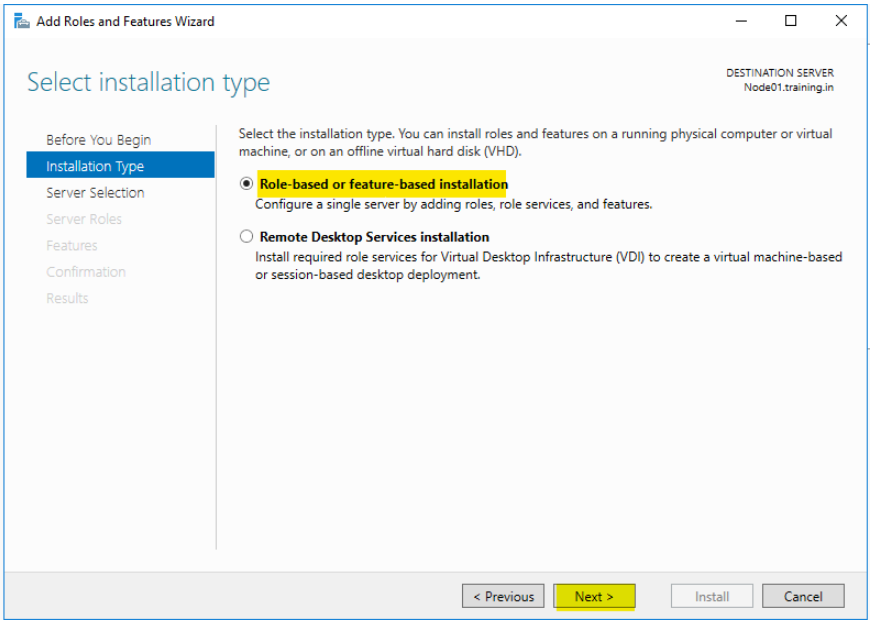
Select the virtual machine (DC) → select VM → Right-click & go to settings → Snapshot → Take Snapshot.

Installing failover cluster feature on both Node01 and Node02, one by one. Ensure that you have 'single' IP address on both nodes.

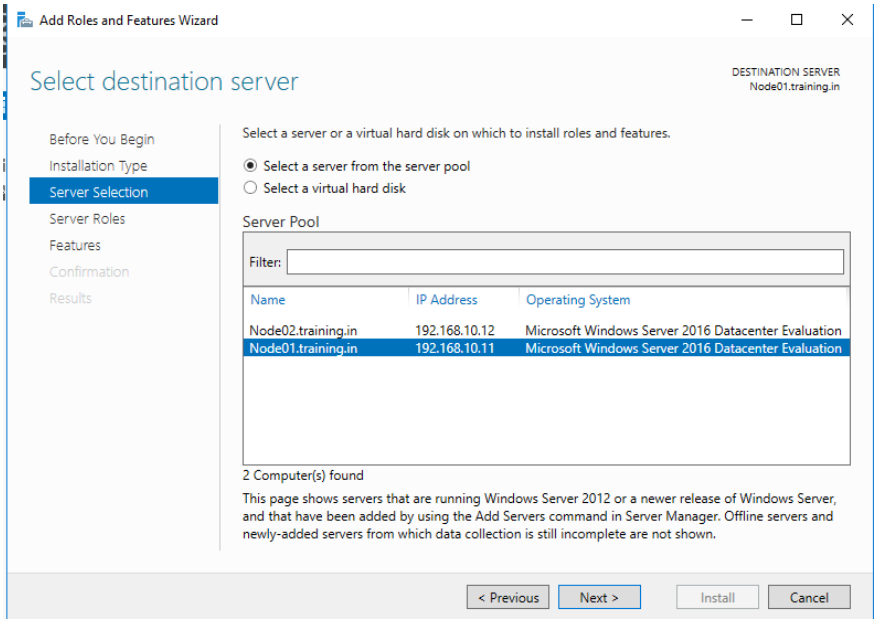
Go to Node01 → Dashboard → Manage → Install roles and features → features → Failover clustering



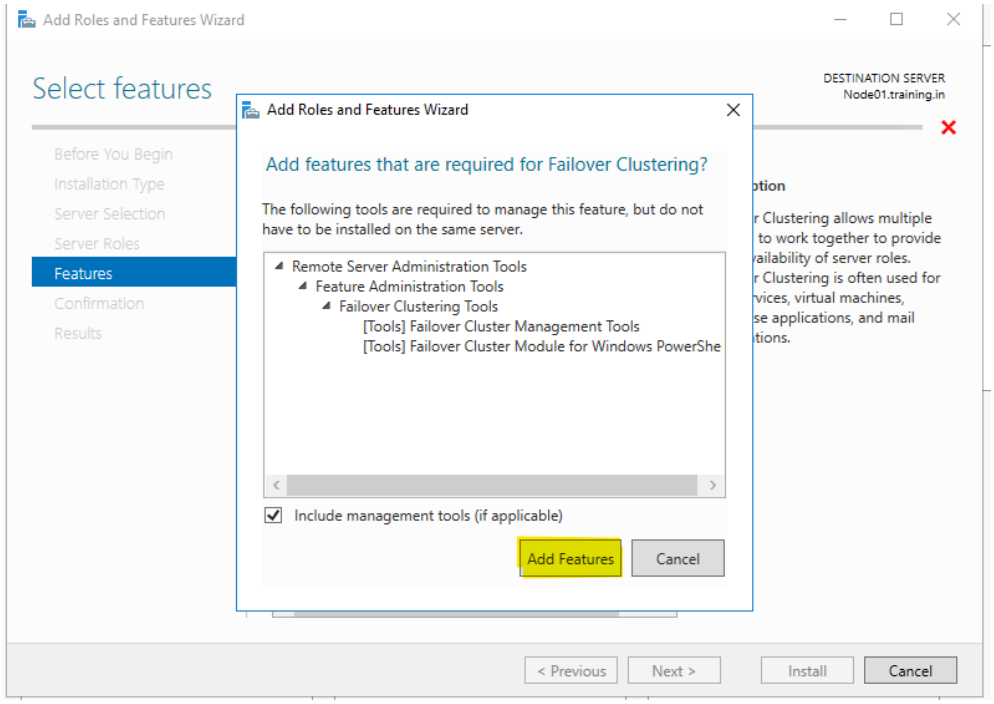
Skip this page and click on Next.

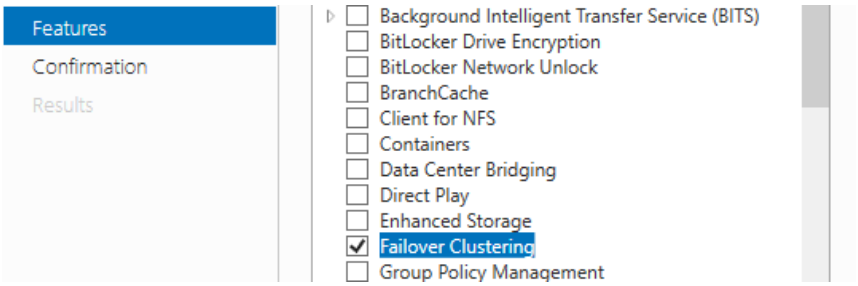


Verify hostname & IP address and click on Next.

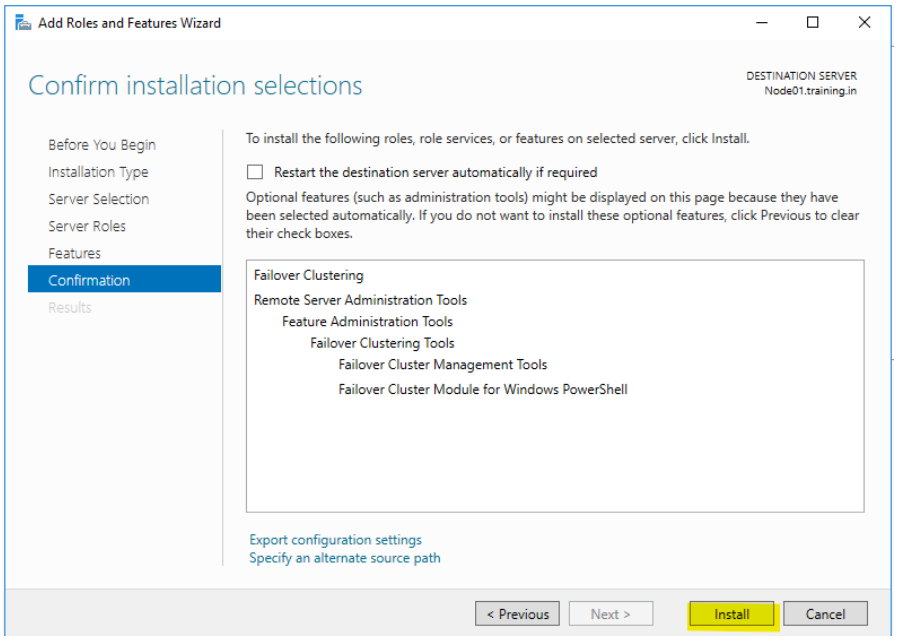


No roles to select, click Next for features and select “Failover Clustering”

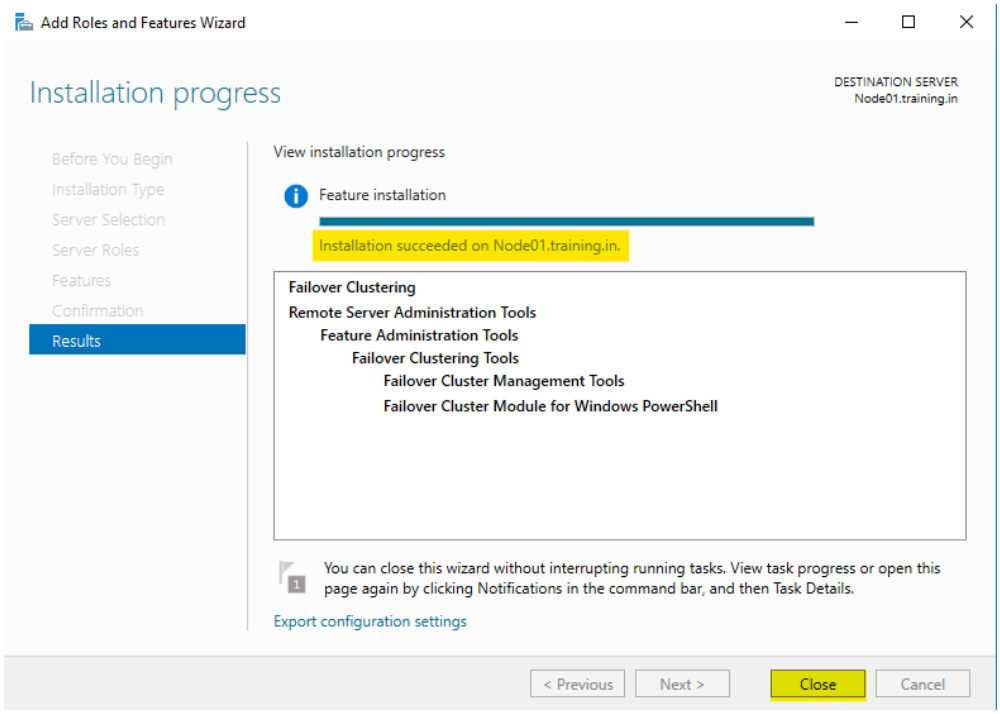




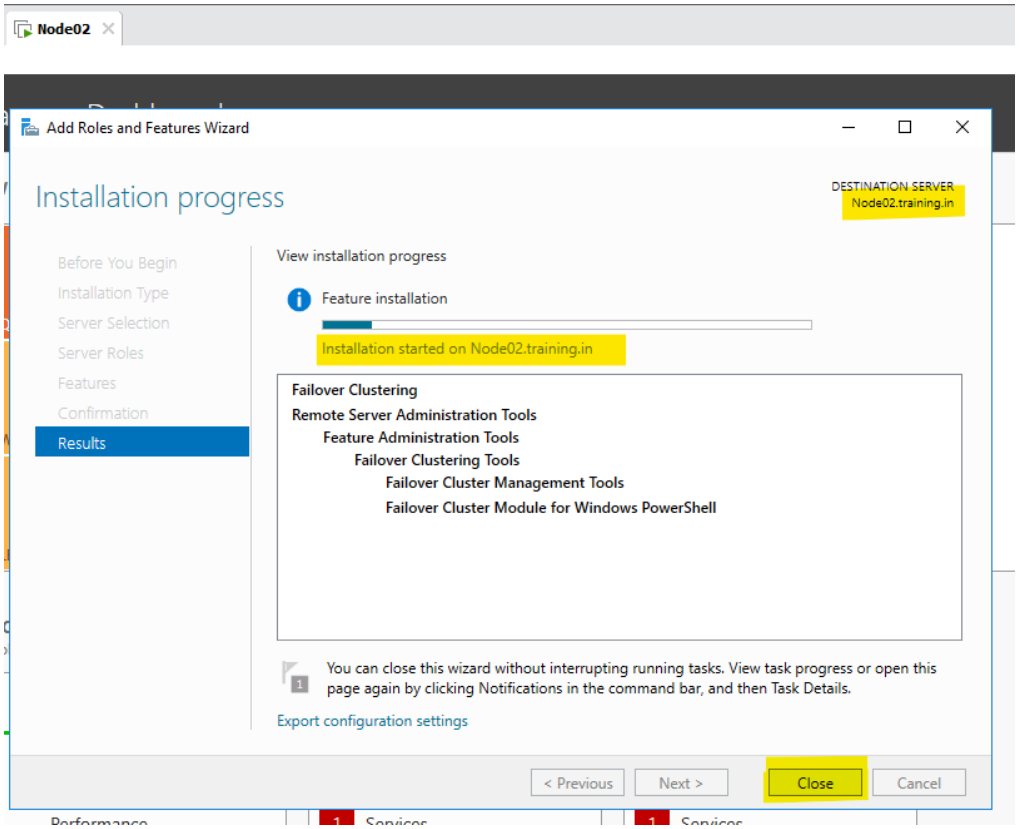
Click on install to finish this:

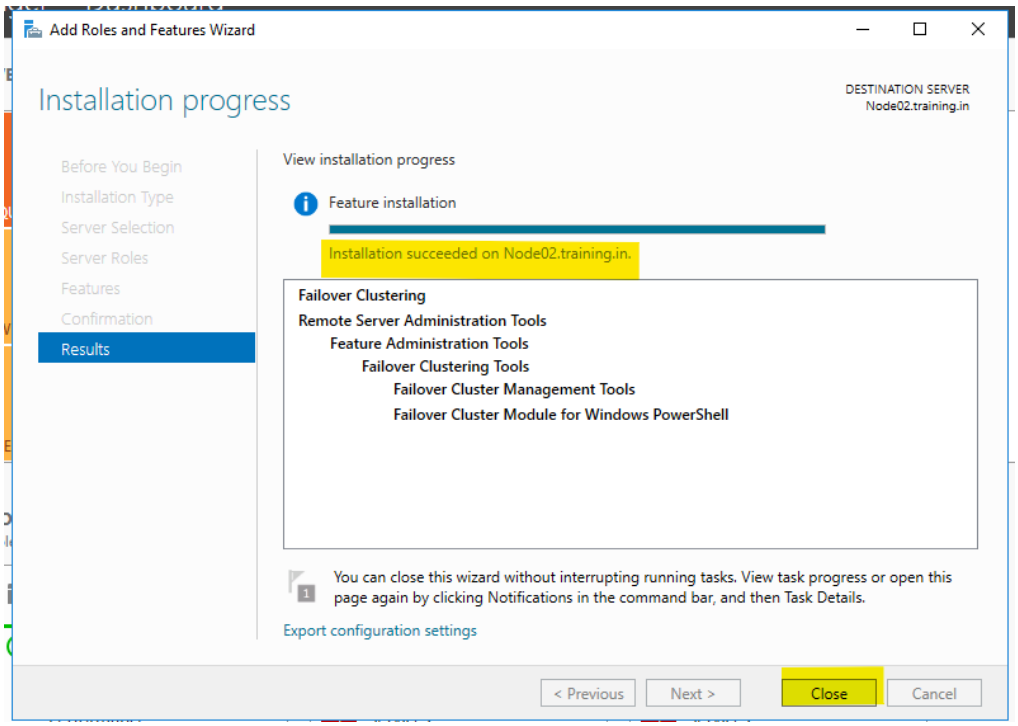


Once installation is succeeded, click on close.



Similarly, installing the Failover cluster on Node02.

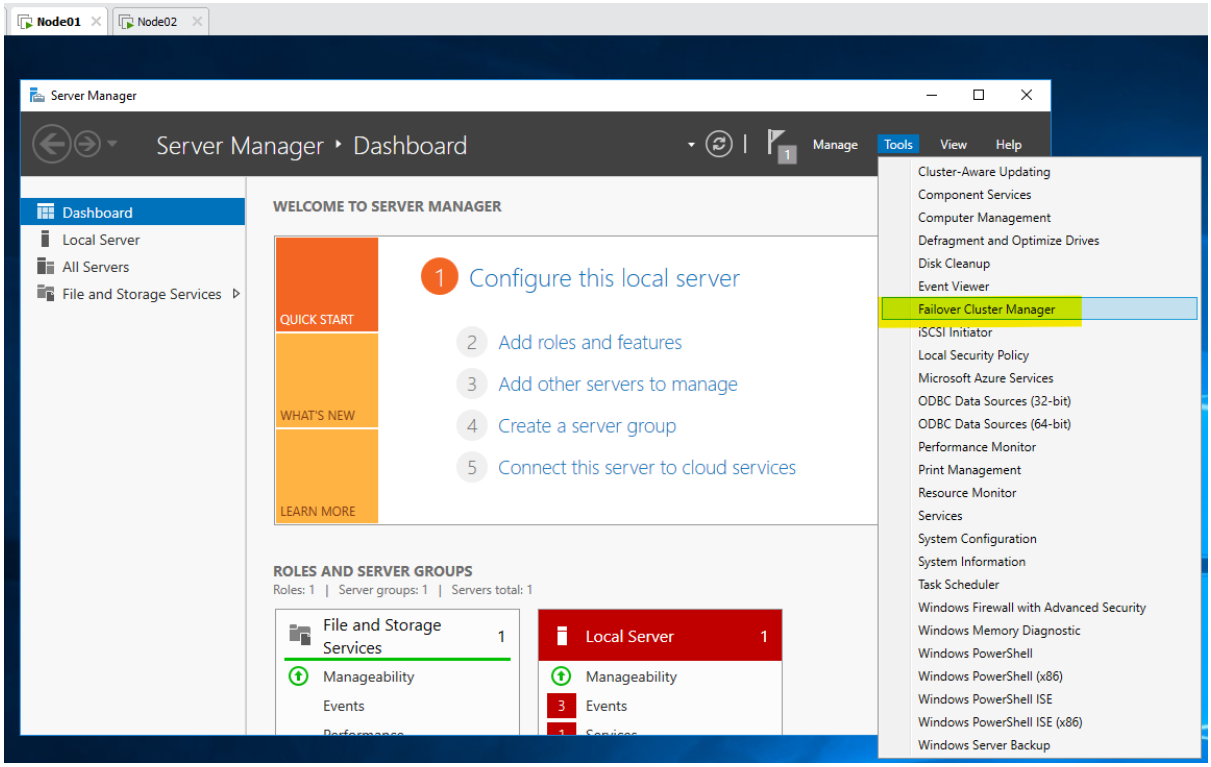




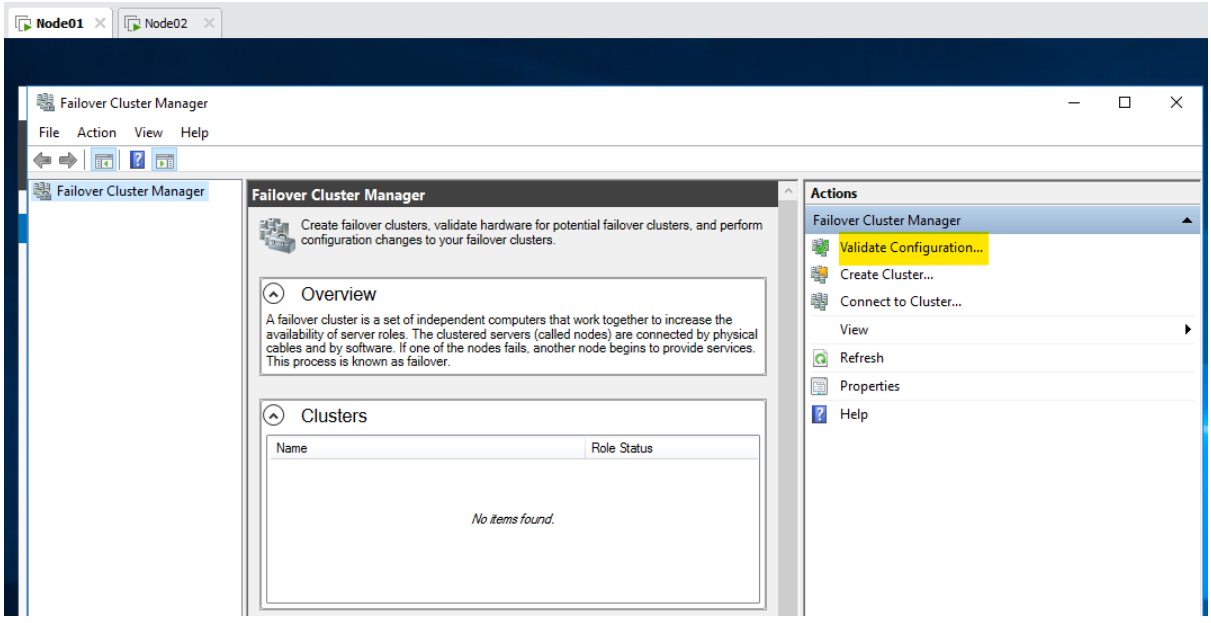
After completion, click on Close.

Now to configure Failover Cluster, go to Node01 and open Failover Cluster Manager.

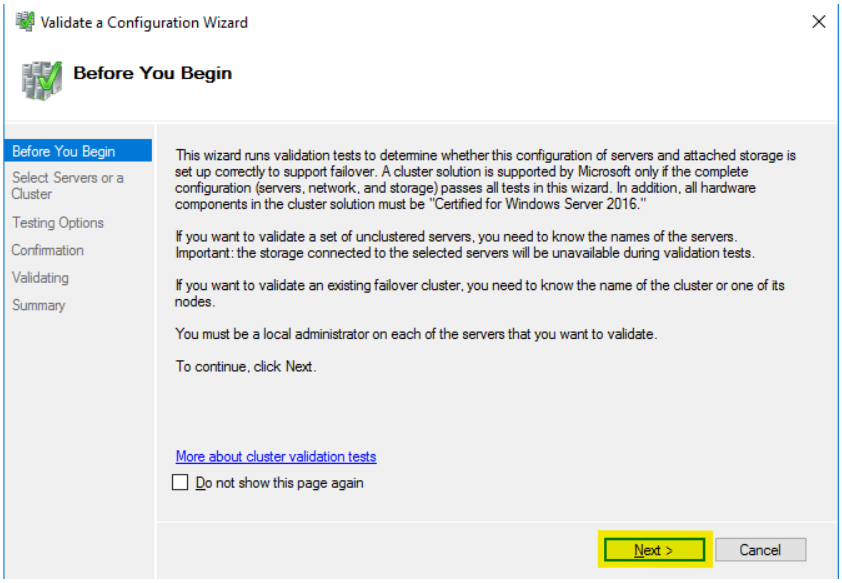
Node01 → Dashboard → Tools → Failover Cluster Manager.



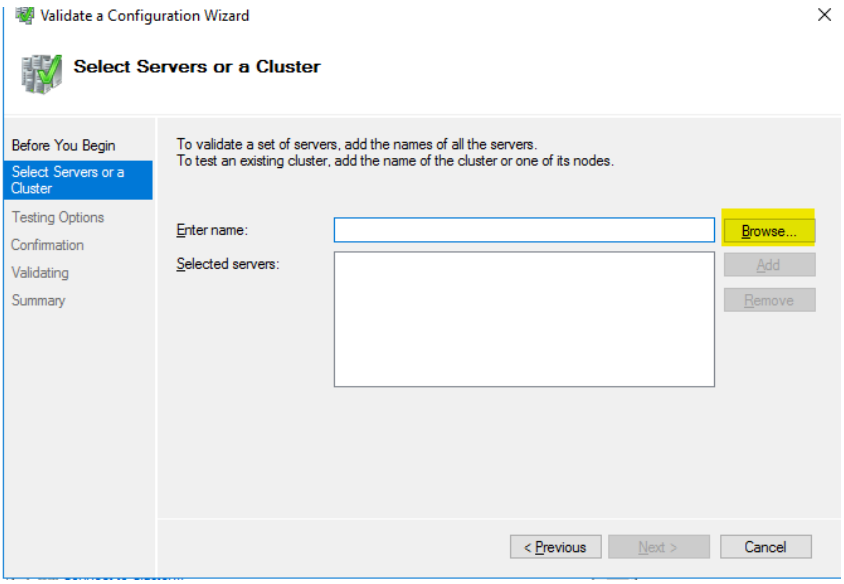
Now before you begin, validate the configuration.



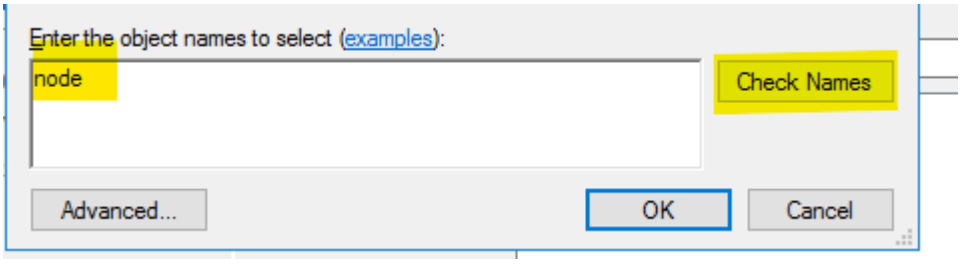
Skip this “before you begin” page:



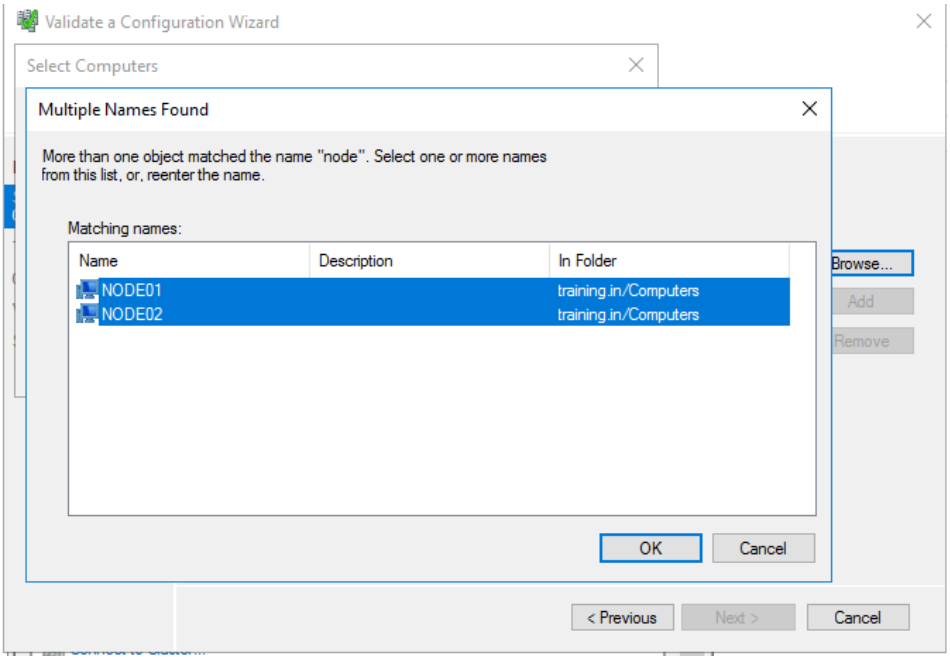
Now click on browse and check for the Nodes.



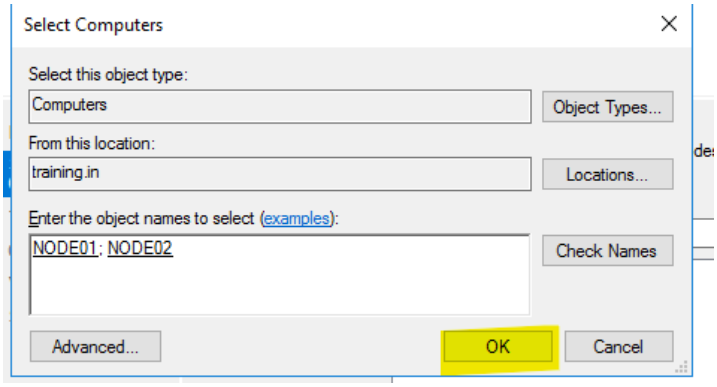
Type ‘node’ and click on ‘check names’



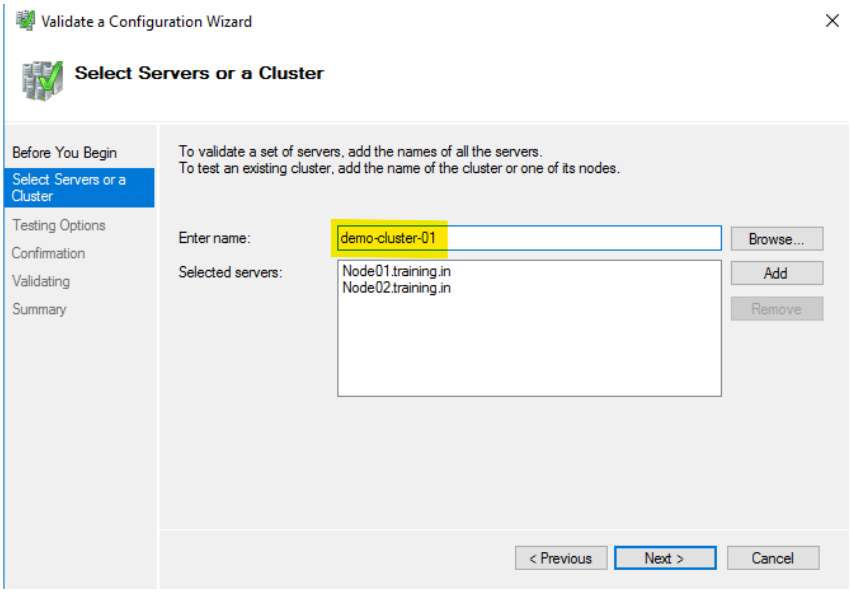
Select both names



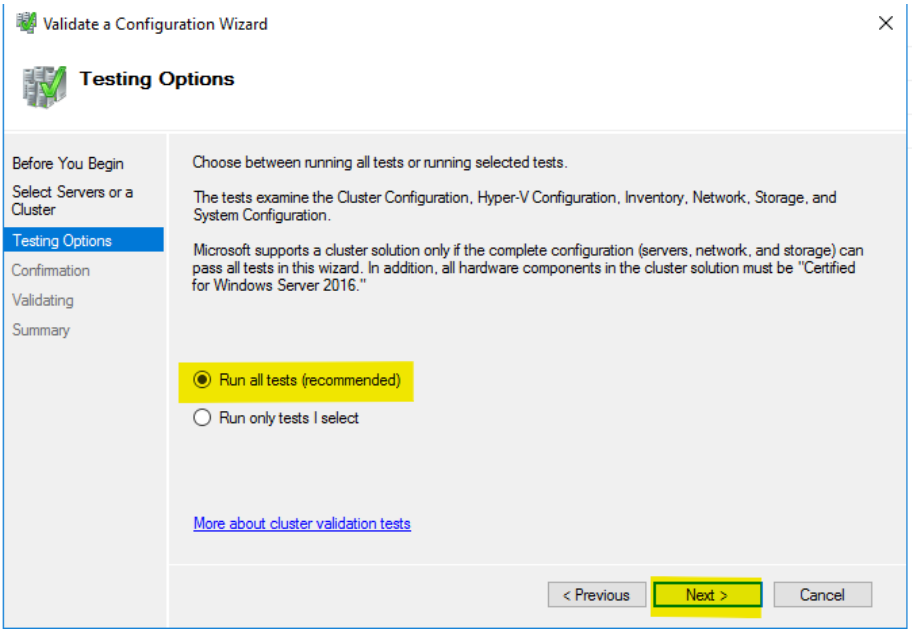
And click on OK.



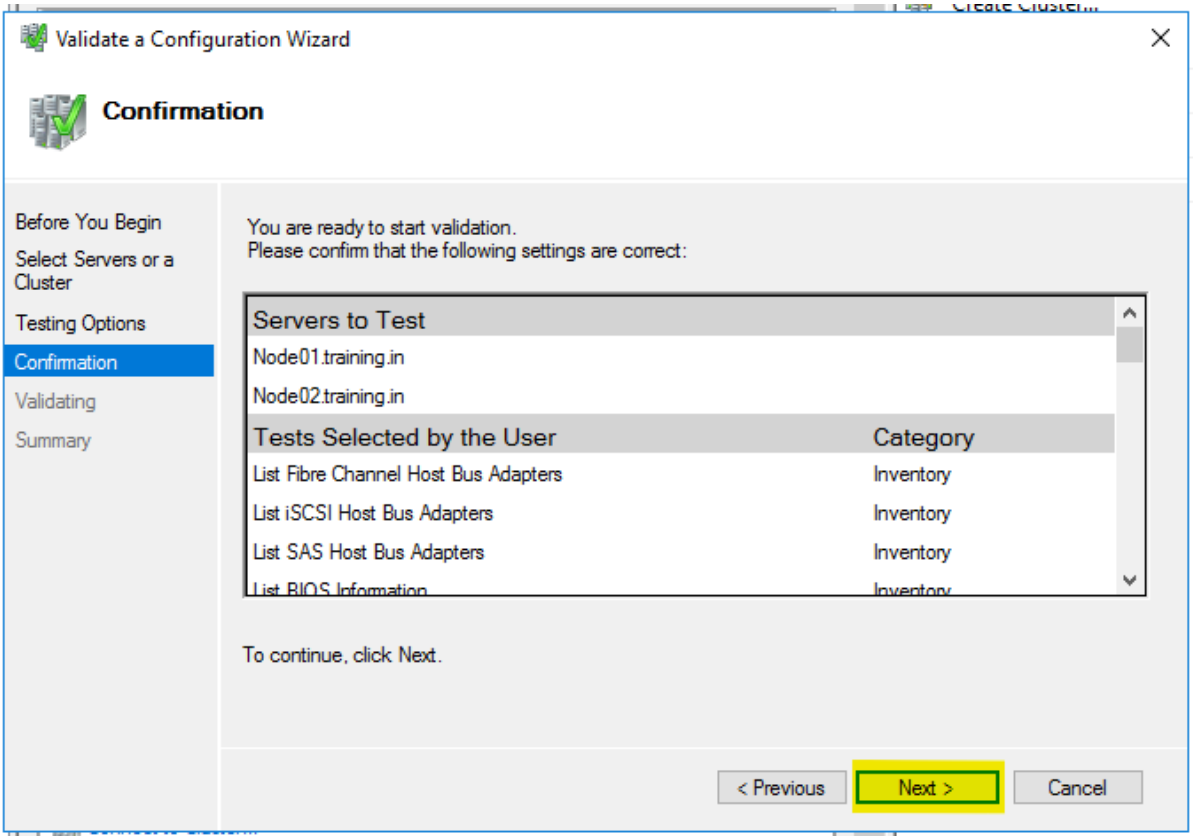
Provide a name for this cluster and click Next:



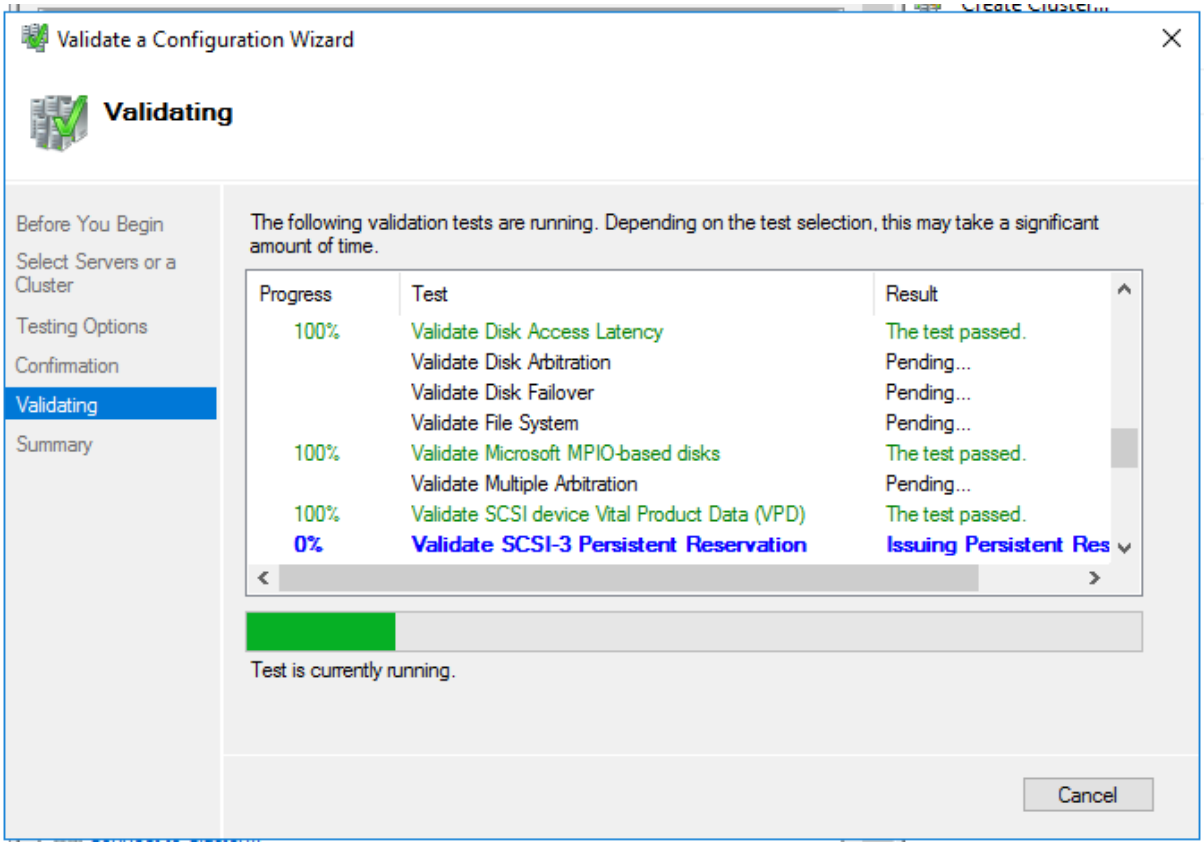
Select “Run all tests” and click Next.



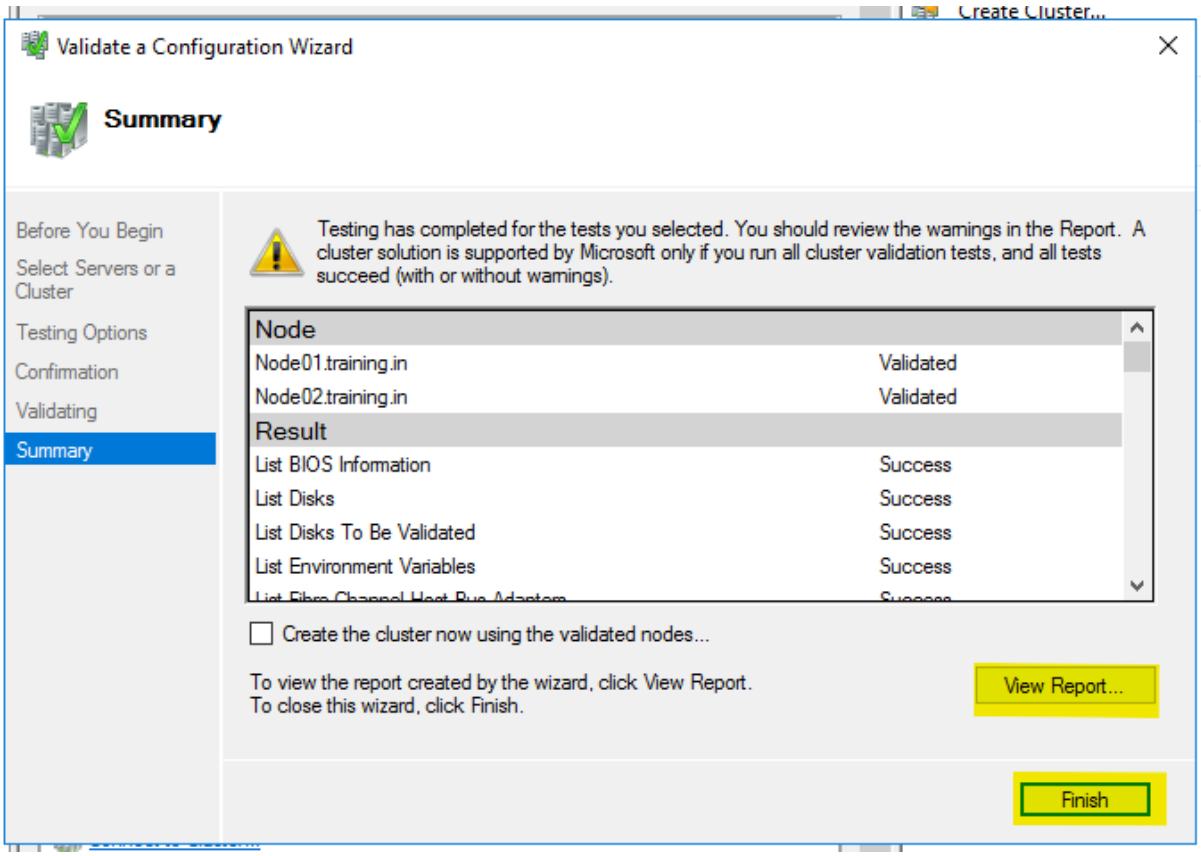
Click next on the confirmation page:



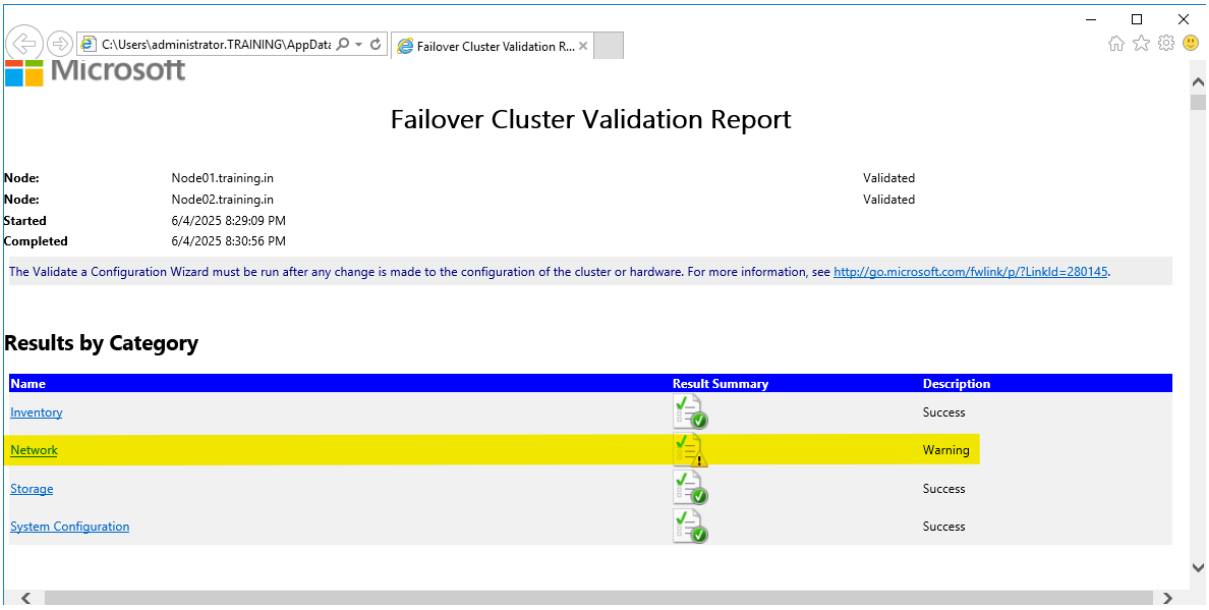
Wait until validation is over.



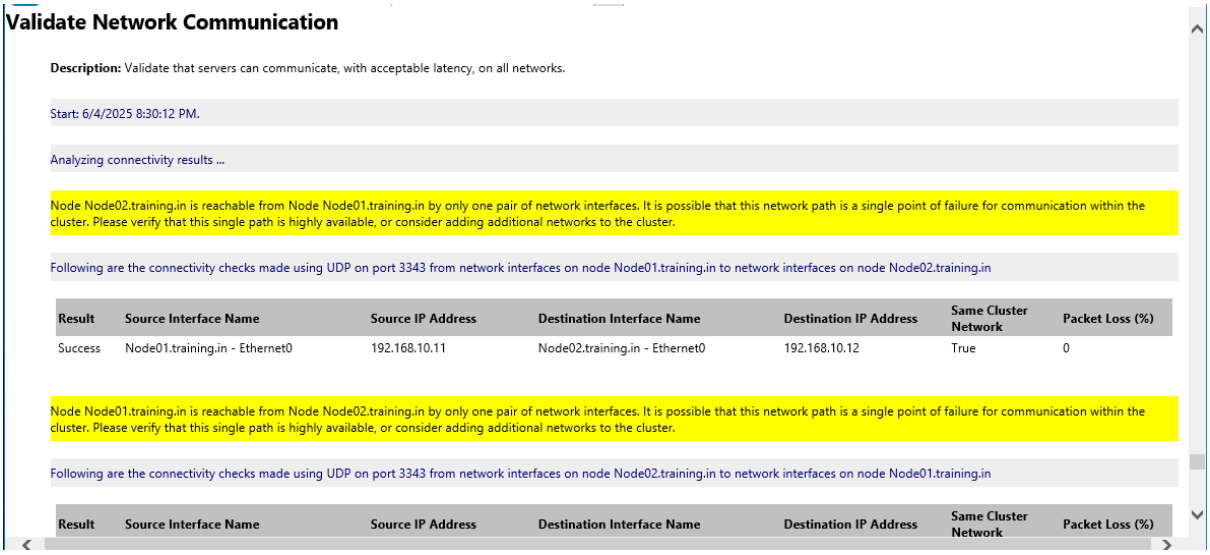
Result succeeded with a warning.



Click on “View Report” to verify.

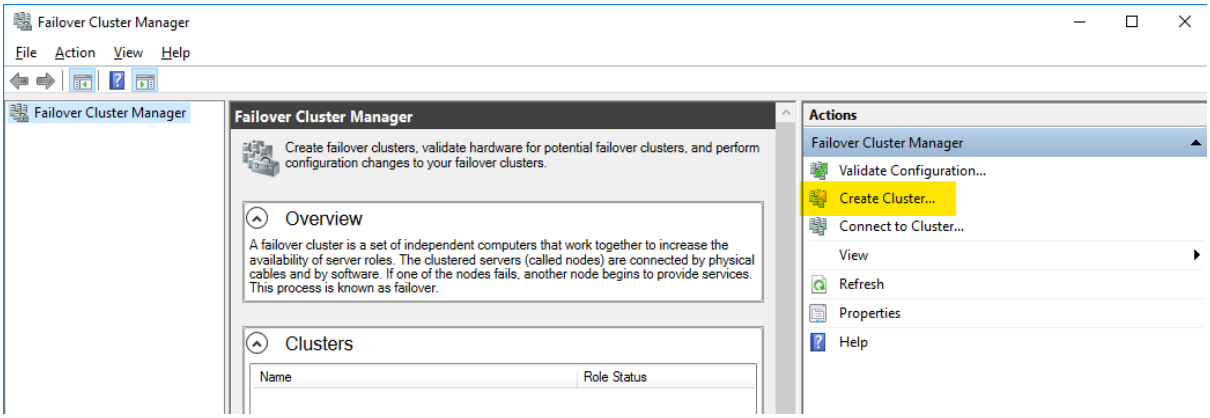


Click on Network to view the warning message.

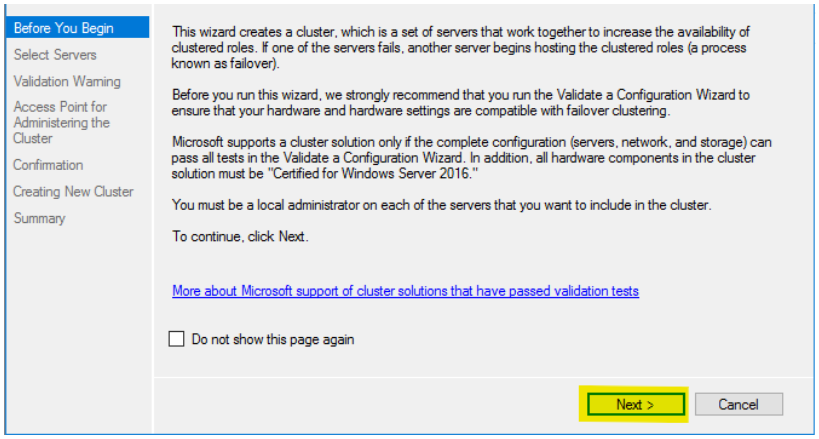


Close this browser and click on finish.

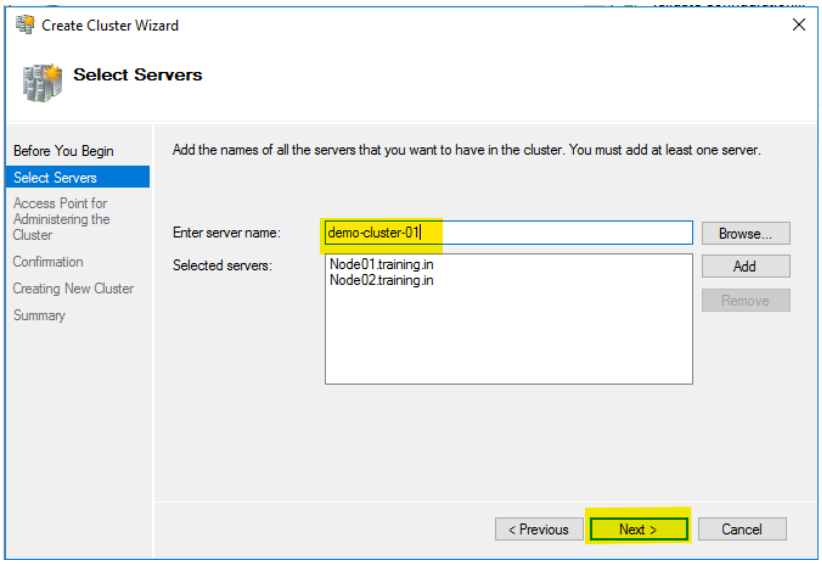
Switch back to Failover cluster wizard and click on “Create Cluster”.



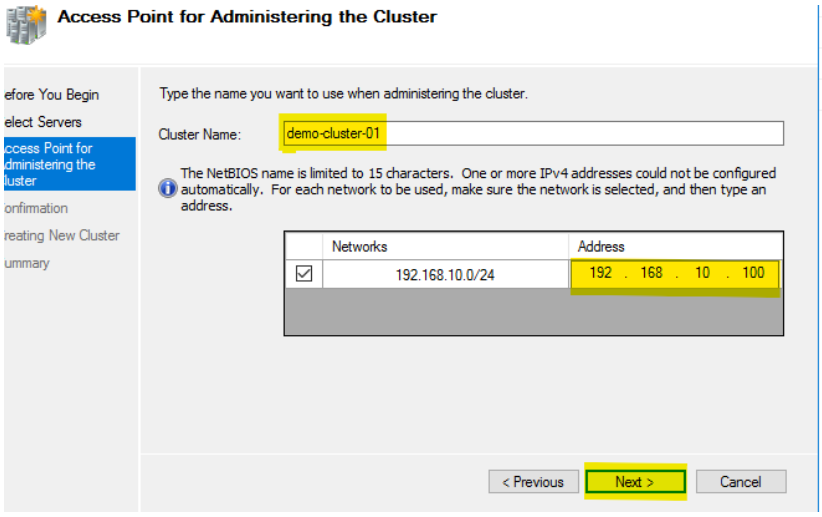
Click on Next.



Browse the nodes and provide a name to it (as done earlier during validation).



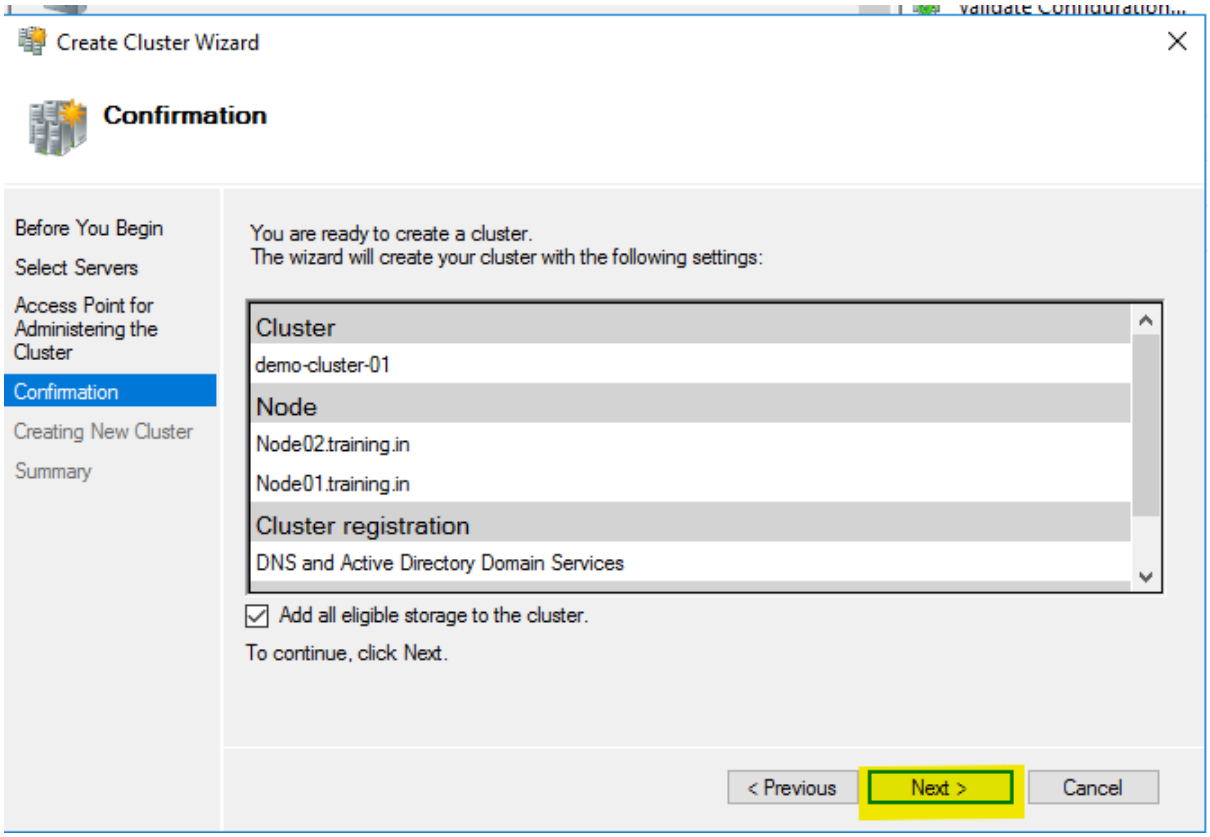
Now, provide a cluster nama and IP address.

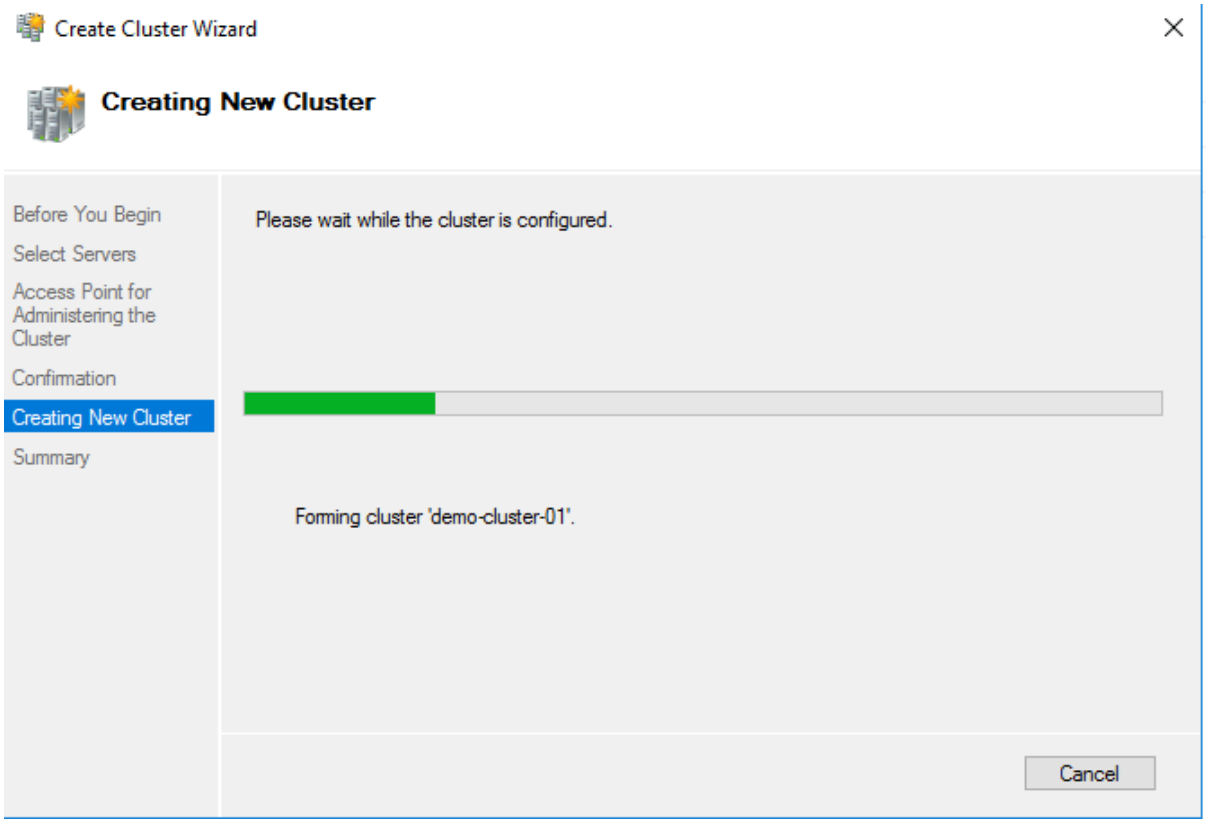


Cluster Name: demo-cluster-01

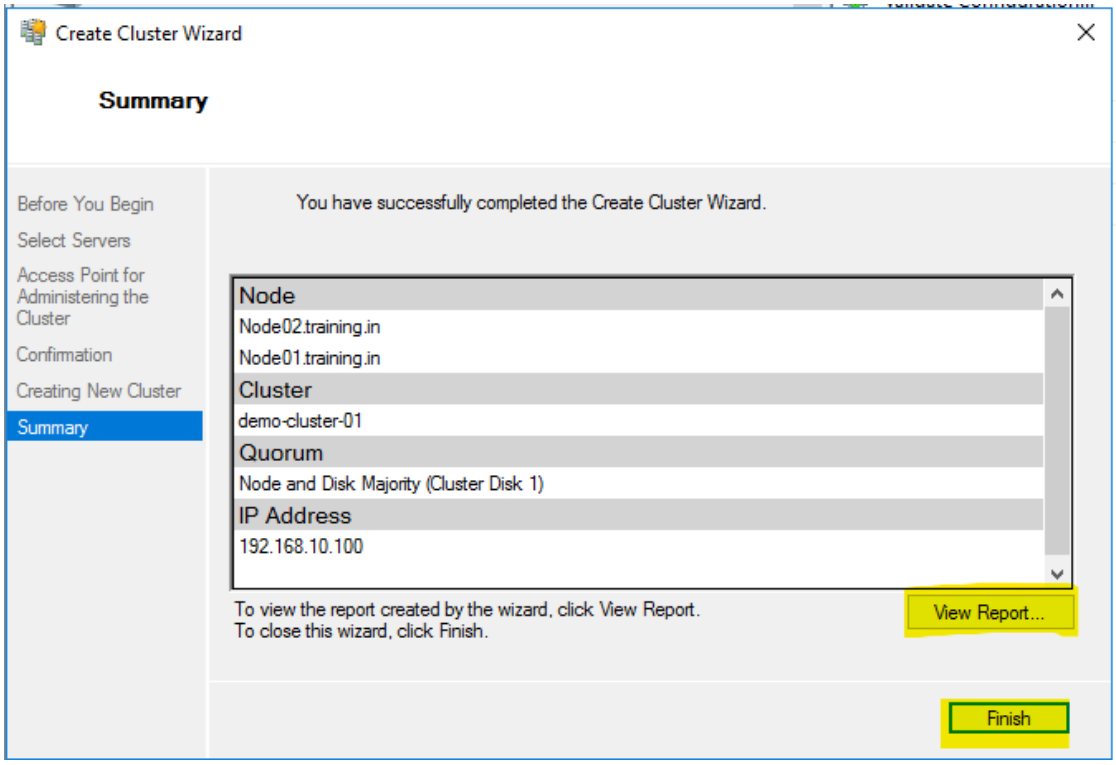
Cluster IP Address: 192.168.10.100

Verify and click Next:

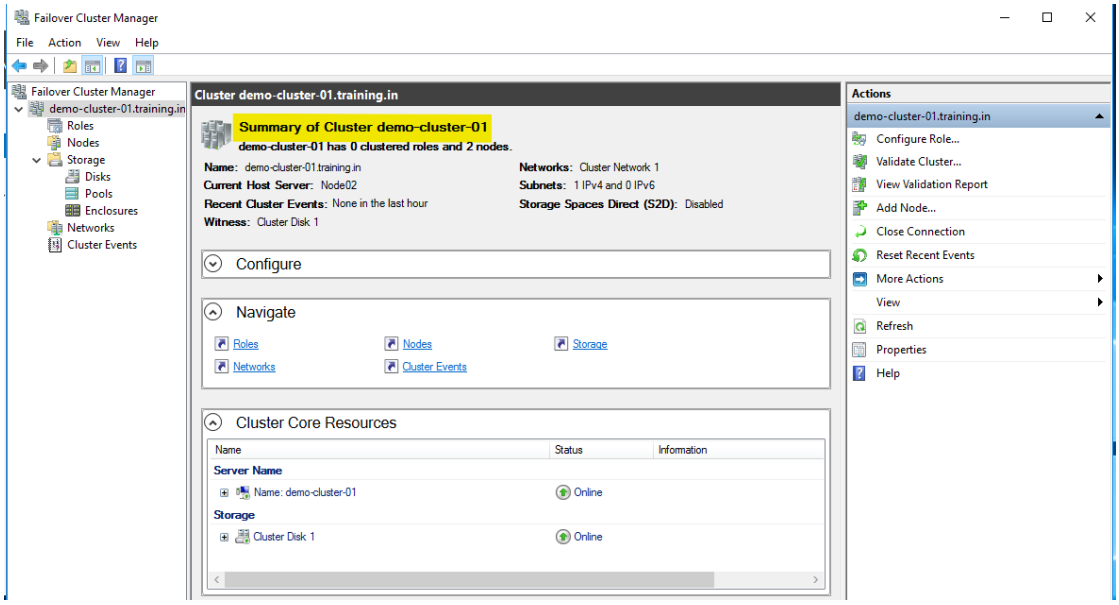




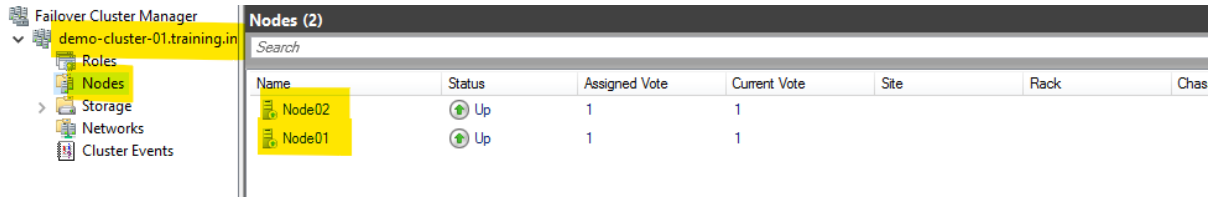
You can view report and then click finish



Validate from the summary:



Open failover cluster wizard and expand cluster → Nodes

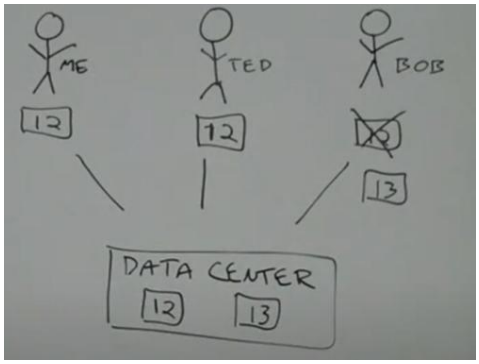


Note – that's all for Failover clustering

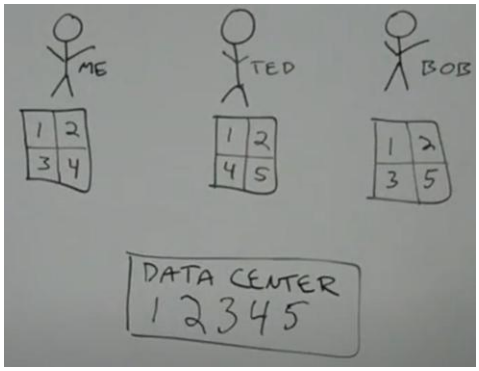
Data Deduplication in Windows Server 2016

Data Deduplication, often called **Dedup.**

- Data Deduplication is a built-in Windows Server feature that helps optimize storage by identifying and removing duplicate chunks of data, storing only one copy to save disk space.
- It got introduced in Win Server 2012
- Best suited for:
    - File server (home directories, shared folders)
    - Backup targets
    - VHDs / VHDX libraries
- Not recommended for database, exchange server or Hyper-V VMs.
- De-Dup is of 2 types:
    - File-level deduplication
        - It maintains only single version.
        - Consumes more space.



    - Block-level deduplication
        - It breaks down the whole data into various blocks and then stores only unique data blocks.
        - Much more efficient and consumes less storage.

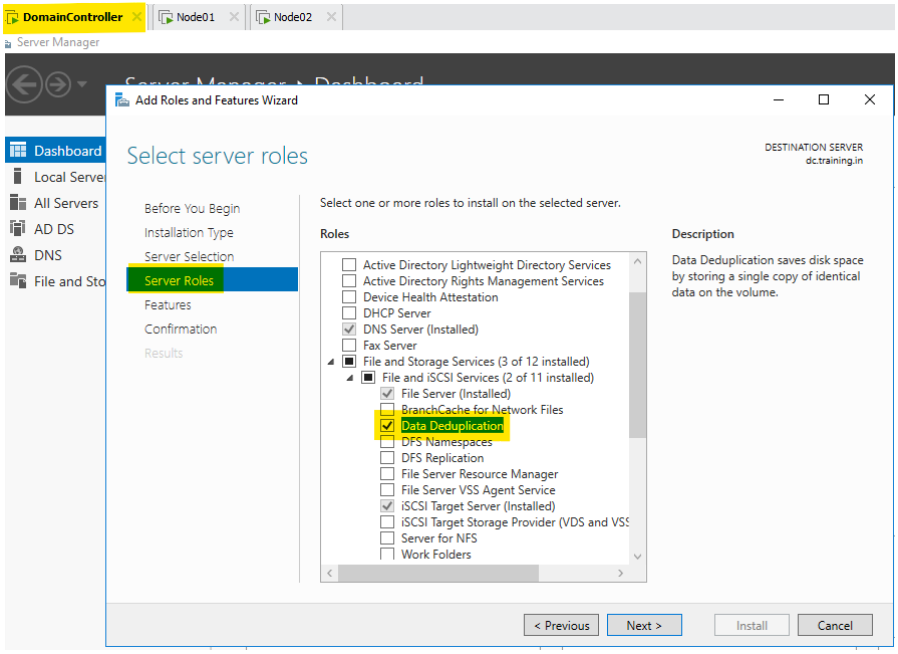


- When can Data Deduplication be used?
    - General purpose
        - Team shares
        - User home folders
        - Work folders
        - Software development shares
    - Virtual Desktop Infrastructure (VDI) deployments
    - Backup targets

Steps to Configure Data Deduplication

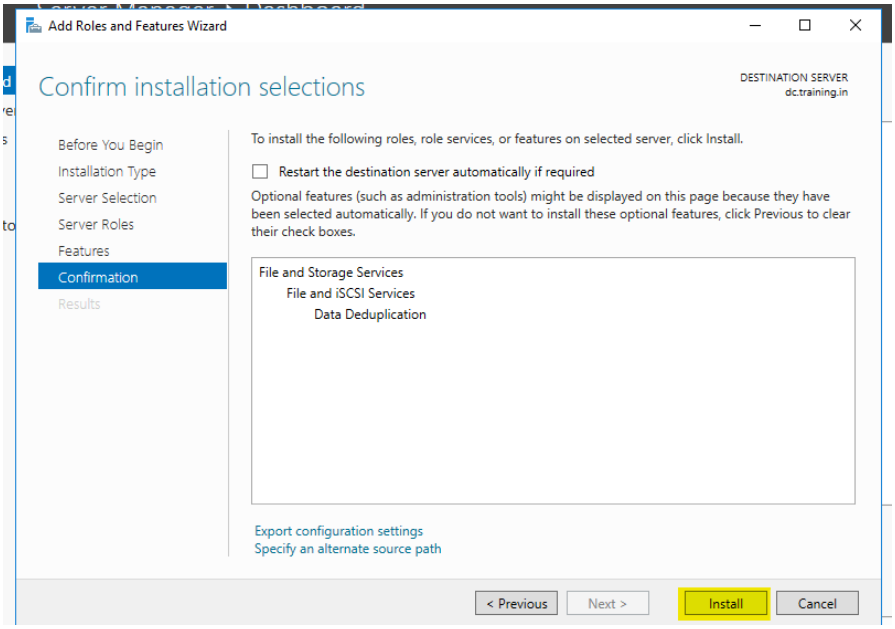
Step 1: Install the Feature

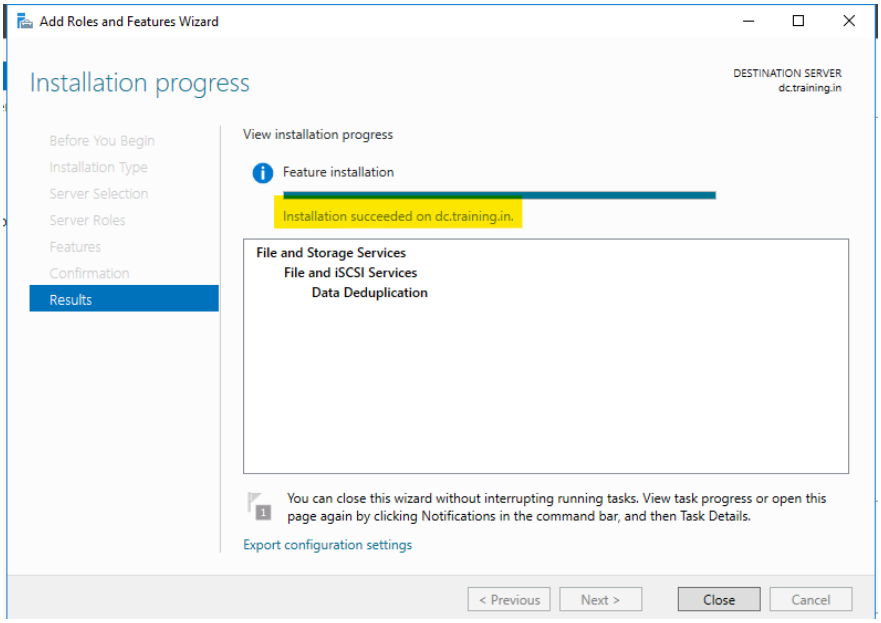
Using Server Manager:
Manage → Add Roles and Features → File and Storage Services → File and iSCSI Services → ✅ Data Deduplication
Using PowerShell:
Install-WindowsFeature -Name FS-Data-Deduplication



No features to be selected, click on Next.

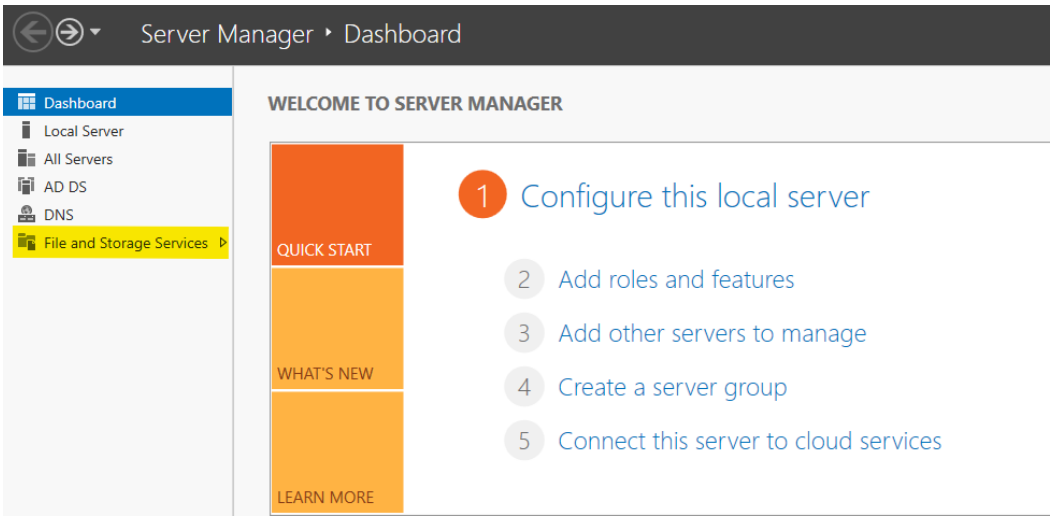
Click on Install.



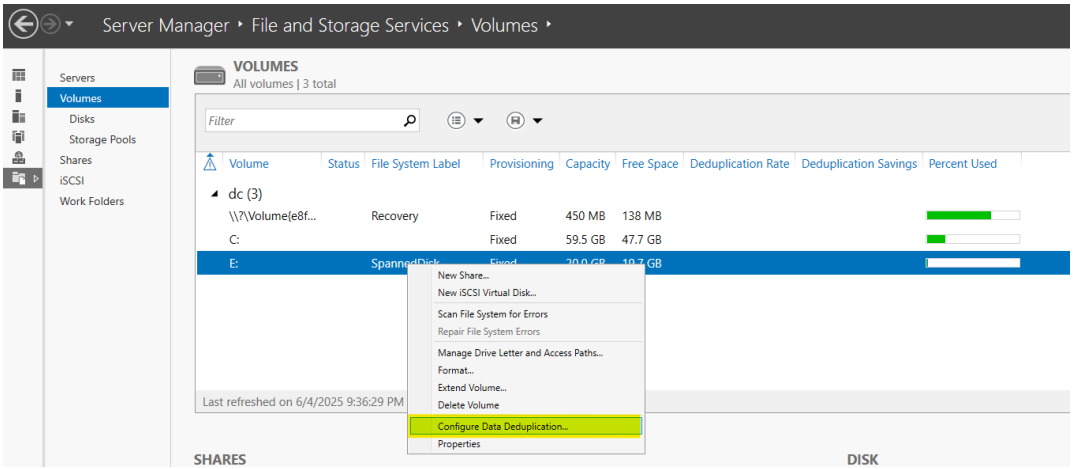


Enabling deduplication on a volume (E:\).

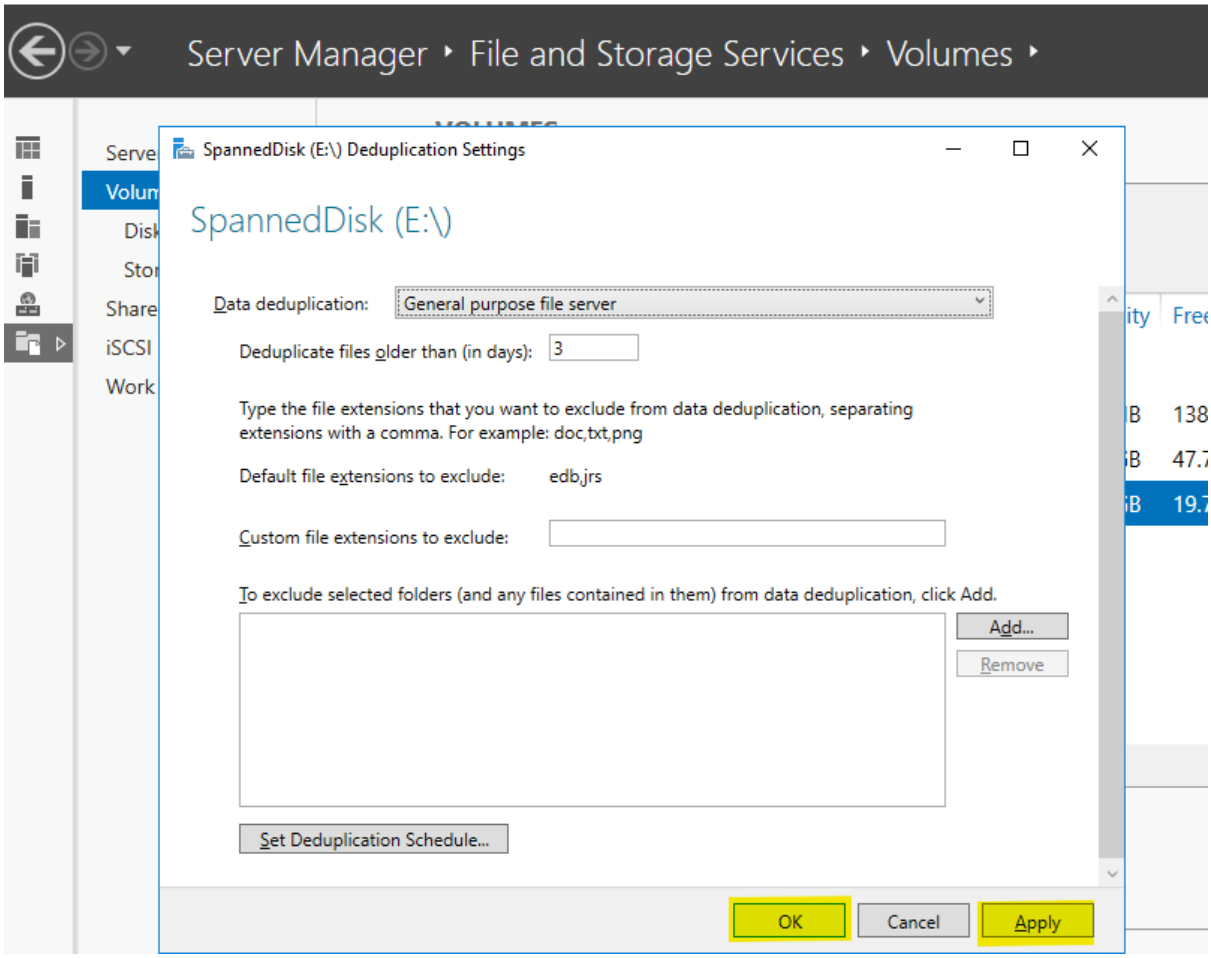
Node01 → Dashboard → File and Storage Services



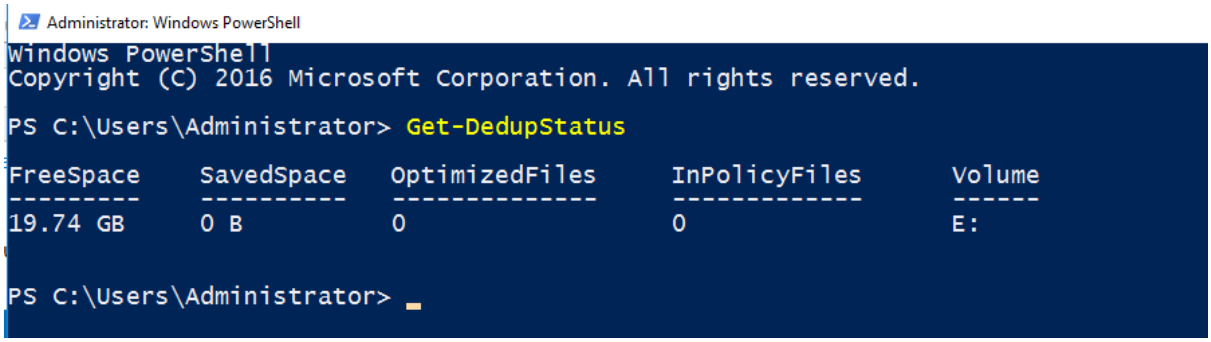
File and storage services → Volumes → select a drive (E:\) → Configure Data Deduplication



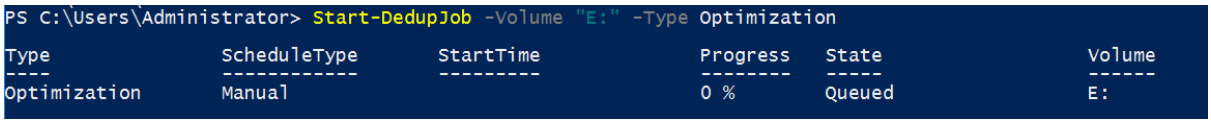
Set data deduplication to “General purpose file server” and deduplicate file older than 3 days.



To Monitor deduplication status,



Start deduplication job manually:



Since there’s no data in E:\ drive, value is “0”.

Note – that’s all for data deduplication

Group Policy Object (GPO)

A Group Policy Object (GPO) is a feature in Microsoft Windows Server Active Directory (AD) that provides centralized management and configuration of operating systems, applications, and user settings in an Active Directory environment.

It allows administrators to control the working environment of users and computers from a central location.

Why is GPO Important?

GPO helps to:

- Enforce security policies
- Deploy software automatically
- Configure user desktop environments
- Restrict or allow features like Control Panel, USB, etc.
- Apply password policies, firewall rules, login scripts, and more

Components of Group Policy

Component	Description
GPO (Group Policy Object)	A container of policy settings
Group Policy Container (GPC)	The AD part of the GPO (stored in AD database)
Group Policy Template (GPT)	The file system part (stored in SYSVOL folder on domain controllers)
Group Policy Editor (GPMC)	Tool used to create, edit, and manage GPOs
Group Policy Processing Engine	The client-side component that applies the policy

Types of GPOs

Type	Description
Local GPO	Stored on individual machines. Applied even without domain.
Non-local GPO (Domain)	Created in Active Directory, applied to users/computers in OUs, sites, or domains.
Starter GPO	A template GPO that contains baseline settings used for creating new GPOs.

GPO Scope and Application Hierarchy - Group Policies are applied in the following order (this is called LSDOU):

1. Local Computer
2. Site-level GPO
3. Domain-level GPO
4. OU-level GPO (Organizational Unit) - Child OUs override parent GPOs

The last applied GPO setting takes precedence in case of conflicts (unless enforced).

GPO Inheritance, Precedence, and Enforcement

- Inheritance: GPOs applied at higher levels (like domain) are inherited by lower levels (like OUs).
- Block Inheritance: Stops GPOs from higher levels being inherited.
- Enforced (Force): Ensures a GPO applies even if Block Inheritance is set.

GPO Filtering and Targeting

1. Security Filtering: Apply GPO only to specific groups or users.
2. WMI Filtering: Apply GPO based on device attributes (e.g., OS version, RAM, etc.).
3. Item-level targeting: Fine-grained targeting within GPO preferences (e.g., apply only if user is member of "HR" group).

Tools Used to Manage GPO

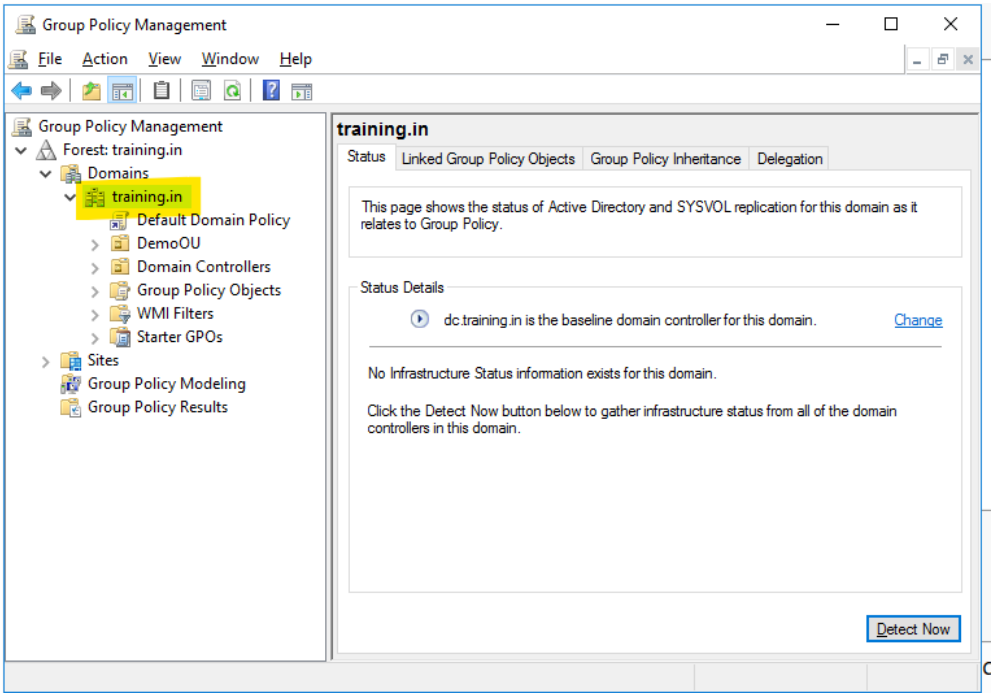
Tool	Purpose
Group Policy Management Console (GPMC)	GUI tool to create, link, and manage GPOs
Group Policy Management Editor (GPME)	GUI editor for defining settings in GPO
gpupdate	Command-line tool to force group policy refresh
gpresult /rs /h	Shows applied GPOs on a machine or user
Resultant Set of Policy (RSoP)	Tool to simulate or report on applied policies

GPO Deployment Process

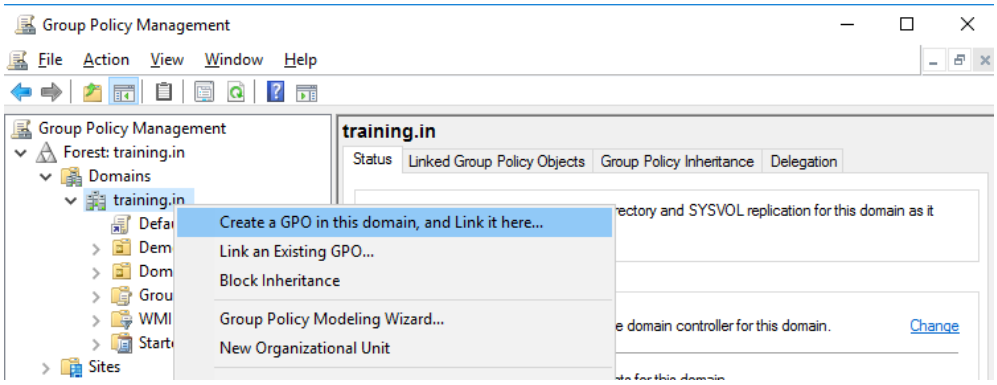
1. **Create GPO** in GPMC
2. **Edit GPO** to define settings
3. **Link GPO** to an OU/domain/site
4. **Test GPO** on limited users/computers
5. **Force apply** using gpupdate /force
6. **Verify** using gpresult /r or rsop.msc

Create a GPO for setting up the wallpaper for whole domain

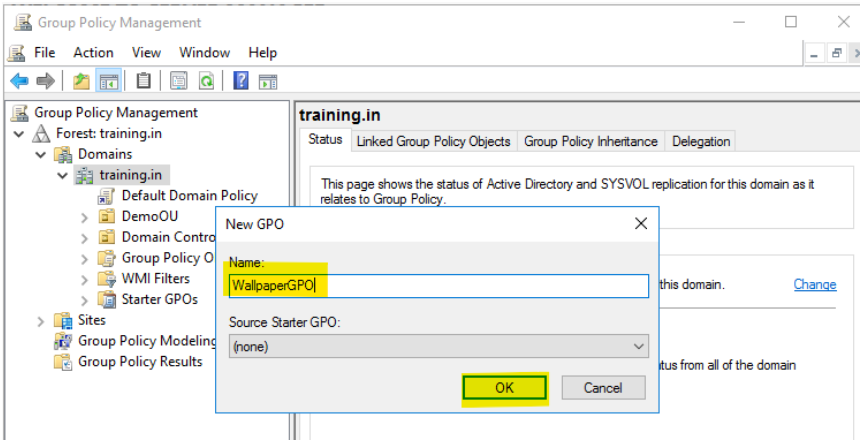
To create and configure GPO → DC → Dashboard → Tools → “Group Policy Management” → expand “forest” → Domains → training.in



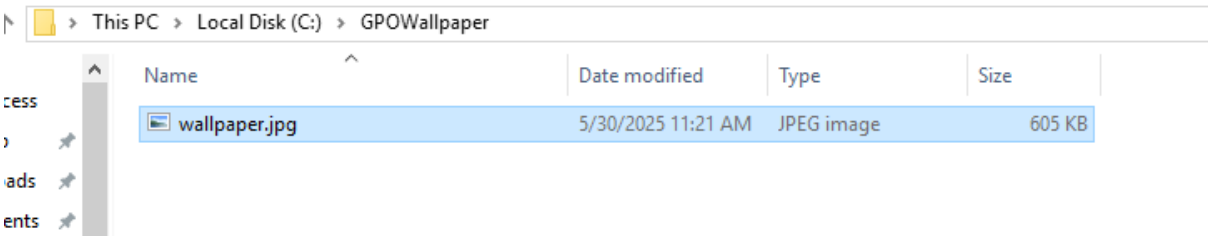
To create a new policy,



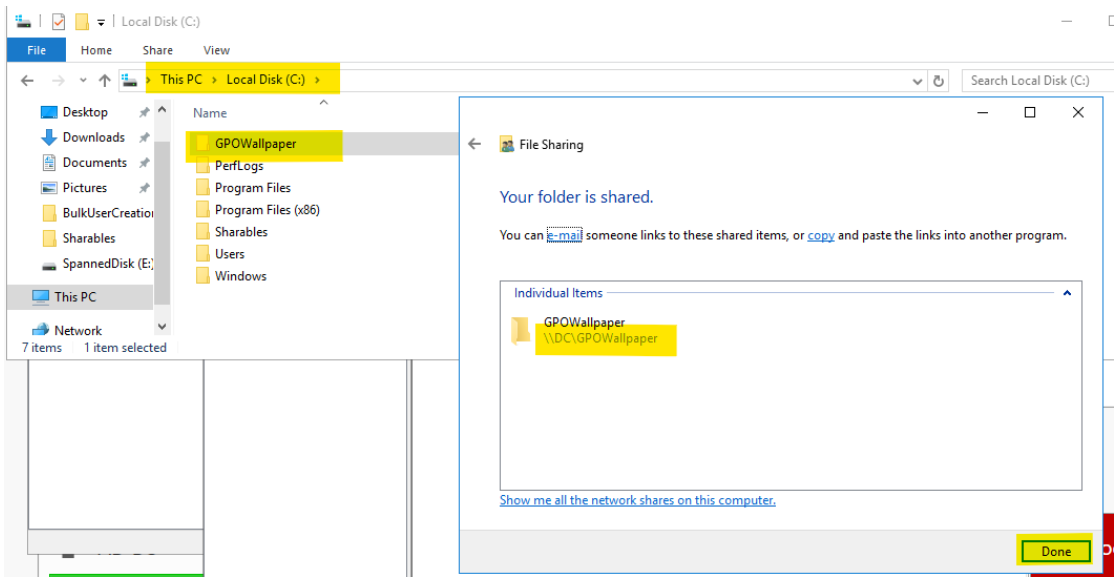
Click on “Create a GPO in this domain, and Link it here…” and provide a name for GPO.



Before editing, create a NFS shared folder under C:\ with a folder name GPOWallpaper and create/paste a wallpaper inside it. (if there is no internet with DC, create a wallpaper using MSPAINT).

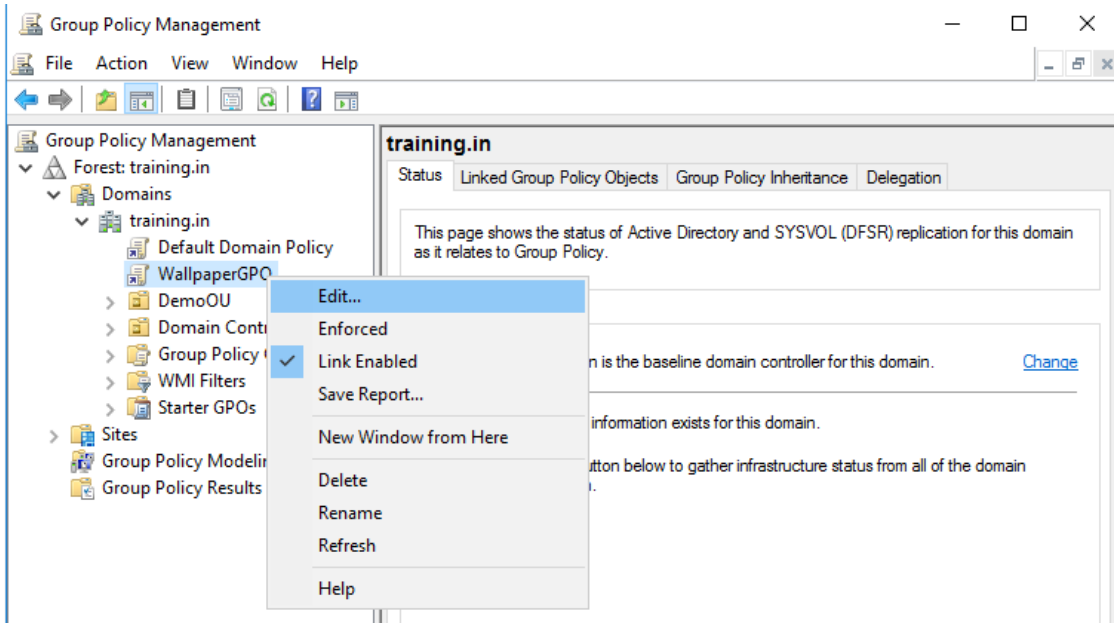


Creating NFS folder:

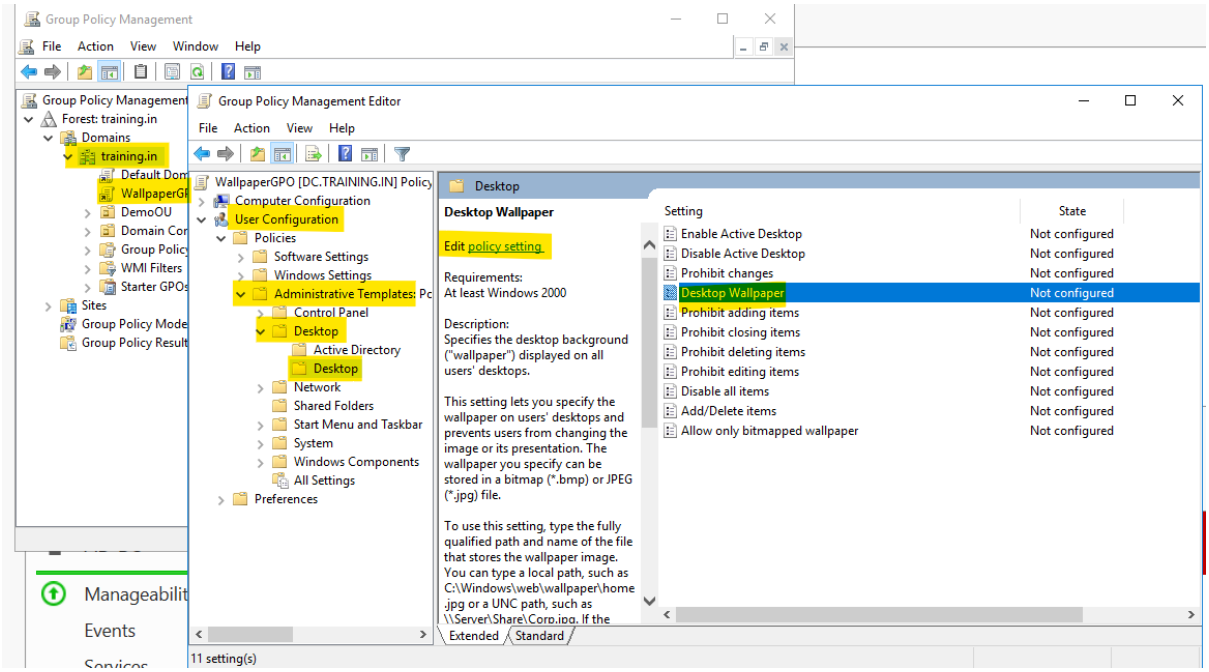


NFS path: \\DC\GPOWallpaper, this path will be used later.

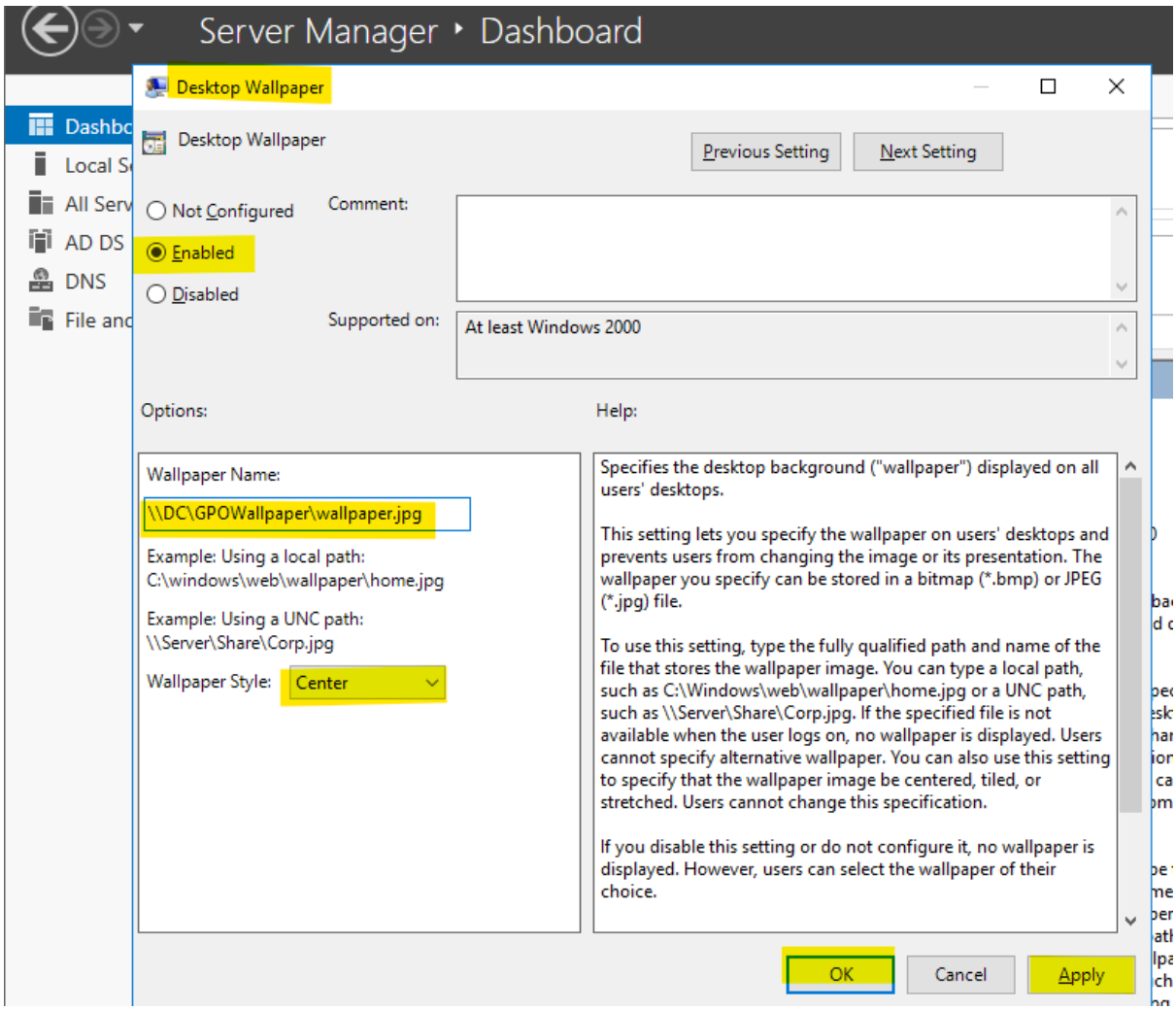
Now, To edit this GPO, right-click on this GPO and click on “Edit”



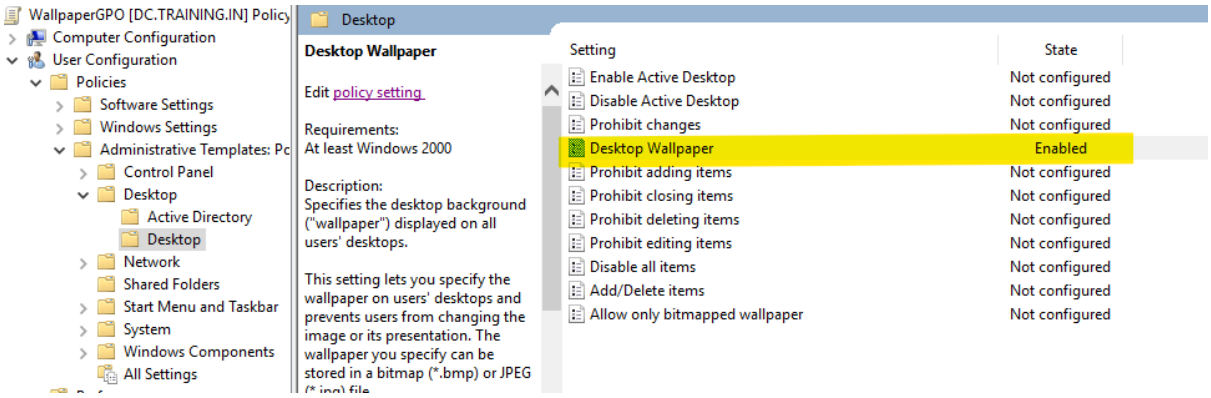
User configuration → Administrative template → Desktop → Desktop → Desktop Wallpaper



Edit policy settings and provide the wallpaper path (with extension) → Apply → Ok.



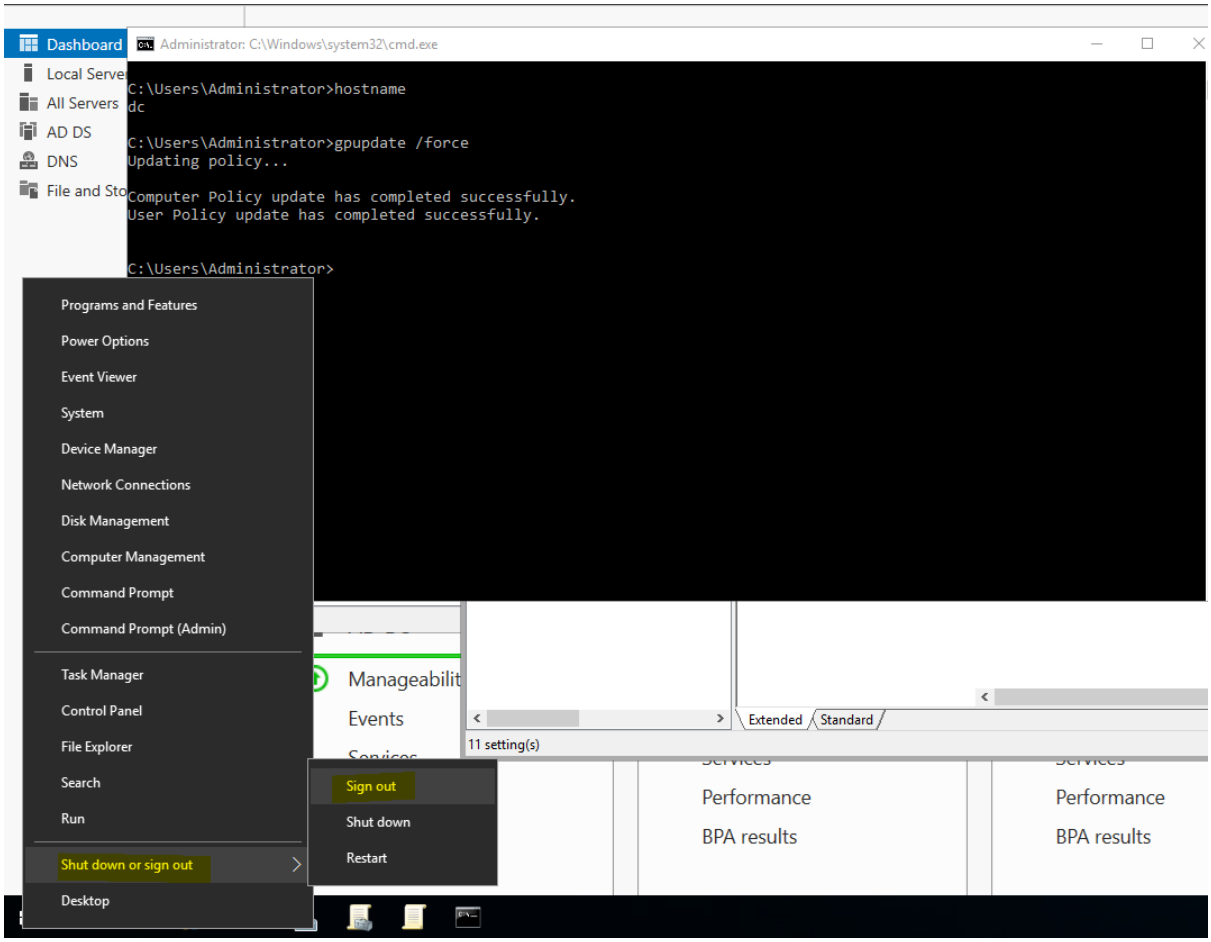
Verify.



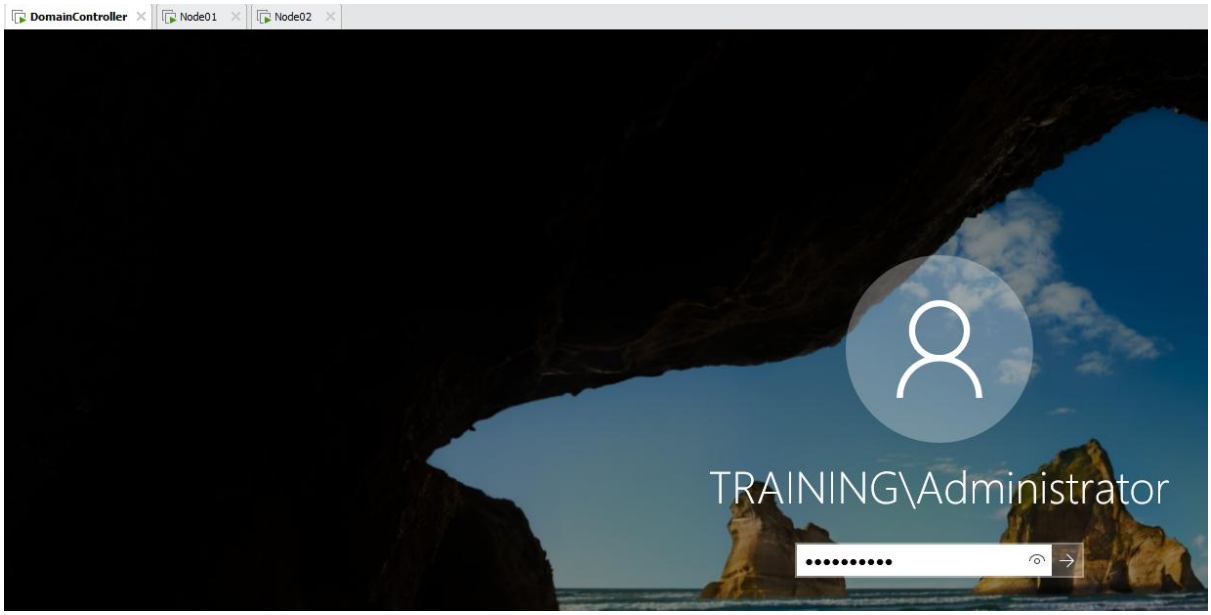
Now to apply group policy on all systems, run → cmd → run command “gpupdate /force” and then you need to sign-out and sign-in again (without this wallpaper will not be applied).

DC

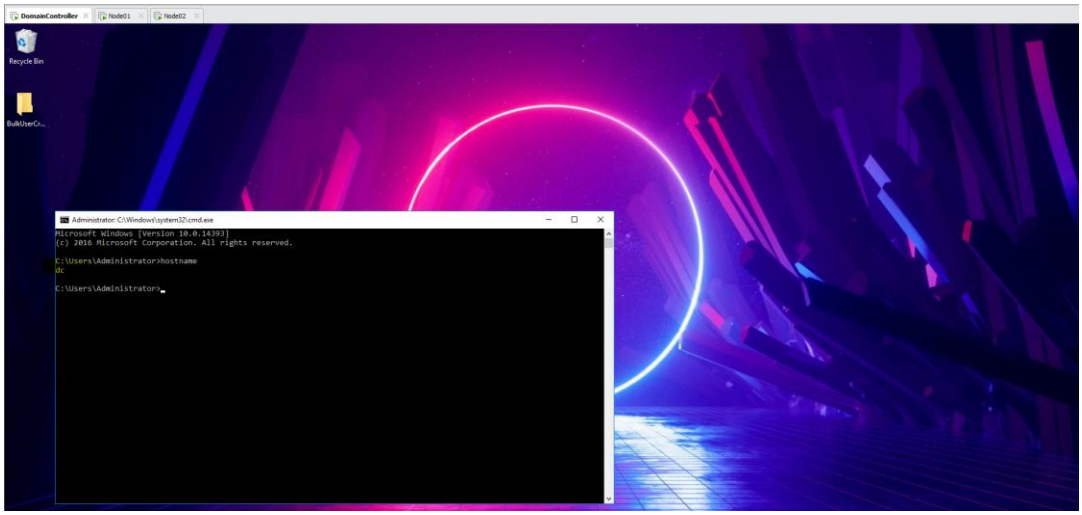
```
C:\Users\Administrator>hostname
dc

C:\Users\Administrator>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.
```



Sign-in again using domain\administrator

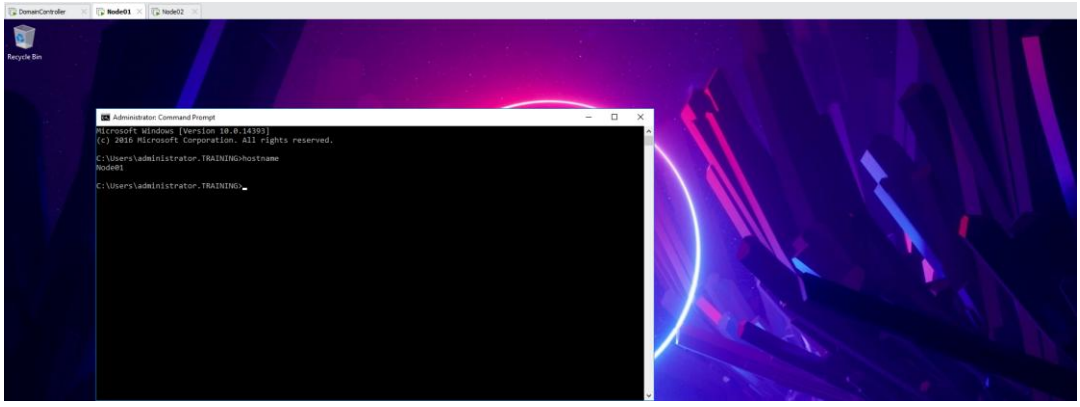


Verify.

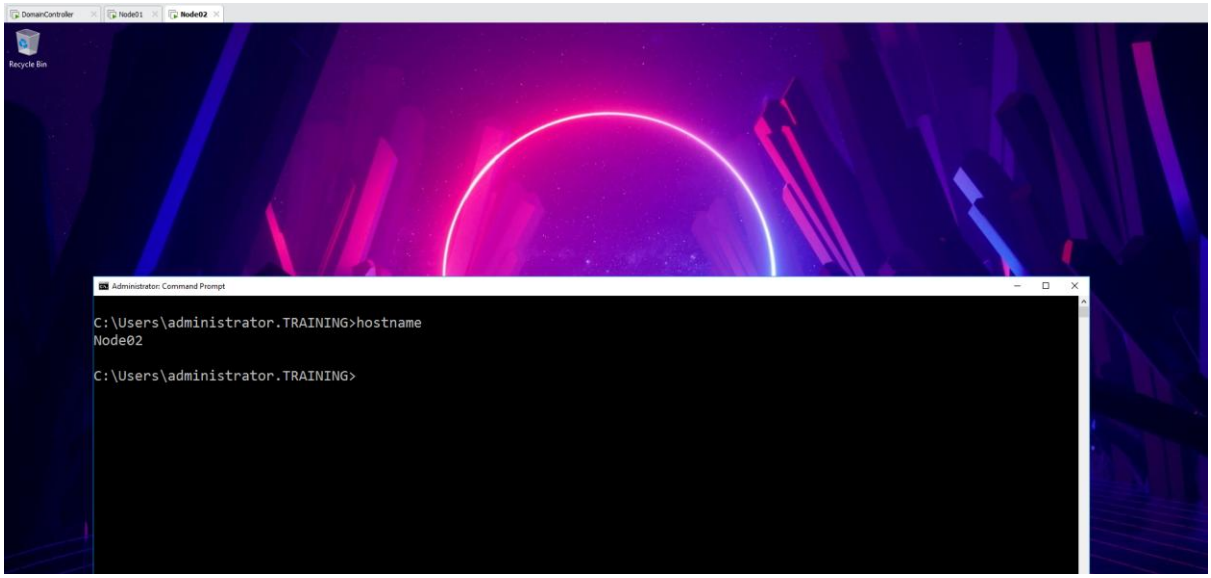


Similarly, update group policy and sign-out and sign-in again on Node01 and Node02

Node01

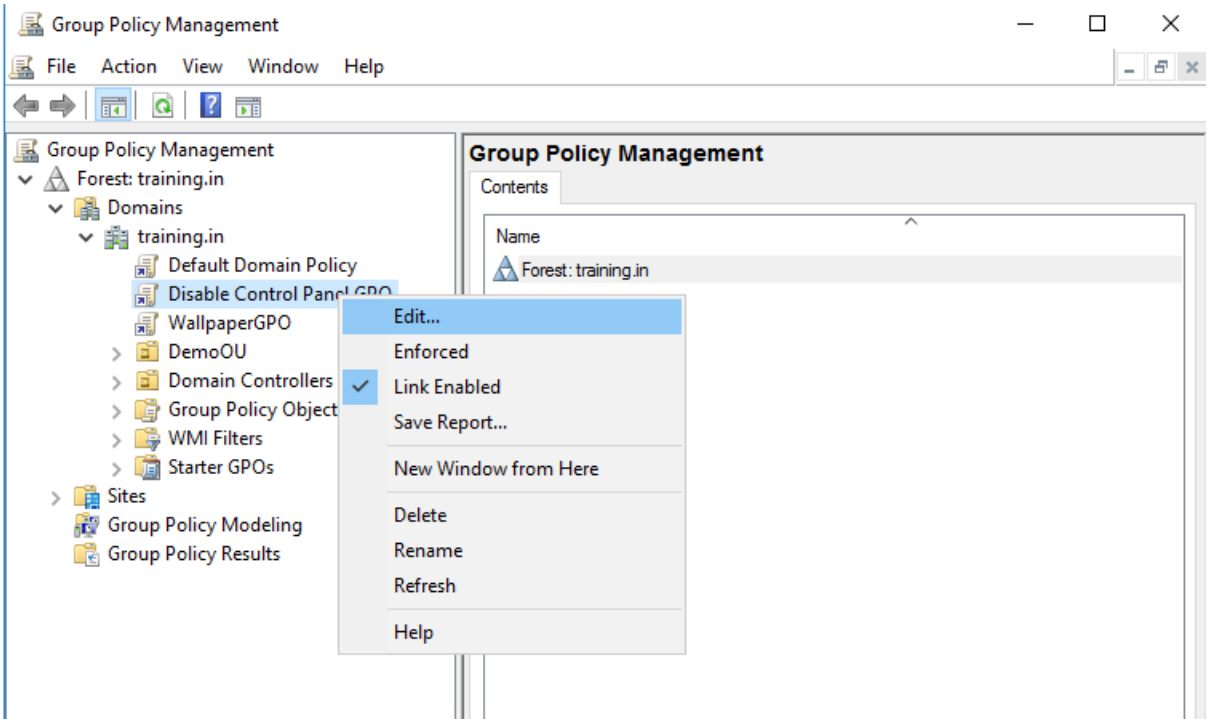


Node02


DomainController
Node01
Node02
Recycle Bin
Administrator: Command Prompt
C:\Users\administrator.TRAINING>hostname
Node02
C:\Users\administrator.TRAINING>

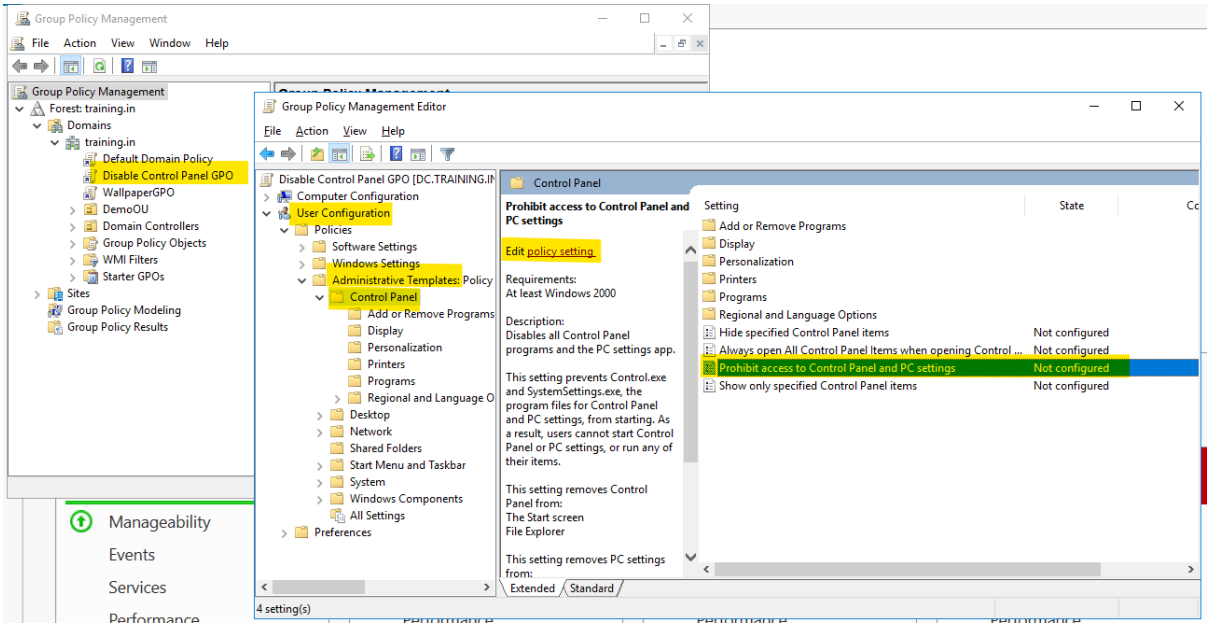
Create a GPO for disabling “Control Panel” for whole domain

Create a new GPO (Disable Control Panel GPO)

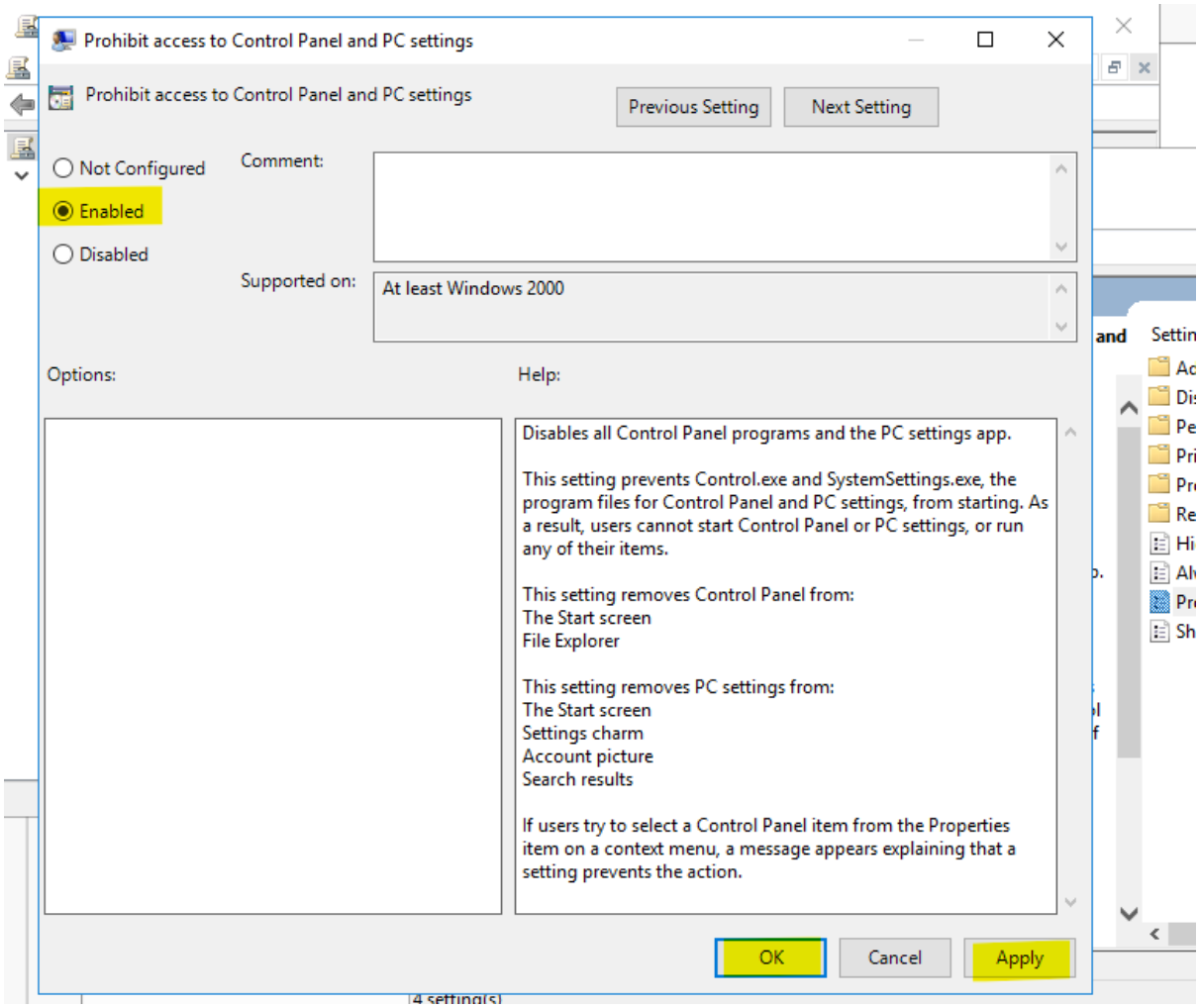


Then edit it.

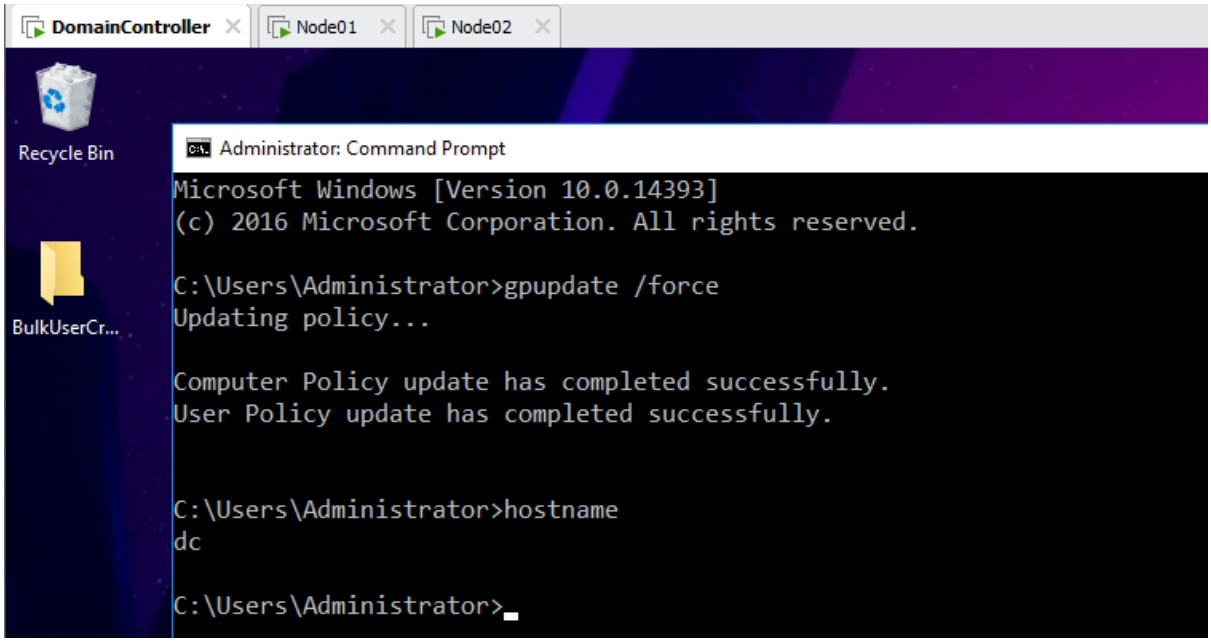
User configuration → Administrative Template → Control Panel → Prohibit access to control panel…



Edit the configuration → Enabled → Apply → OK



Run command “gpupdate /force” on DC, Node01 and Node02

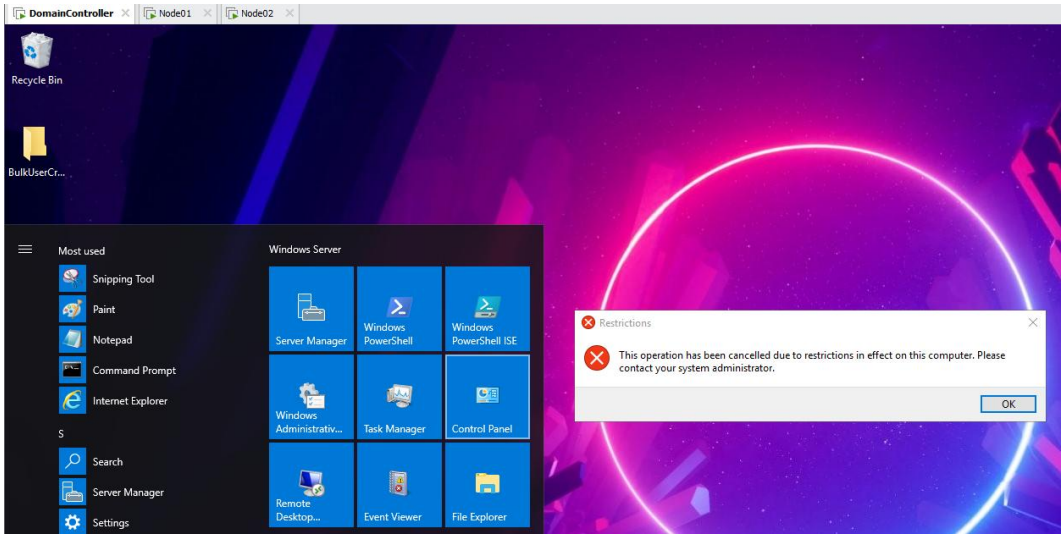


Run command “gpresult /r” to view the applied GPO

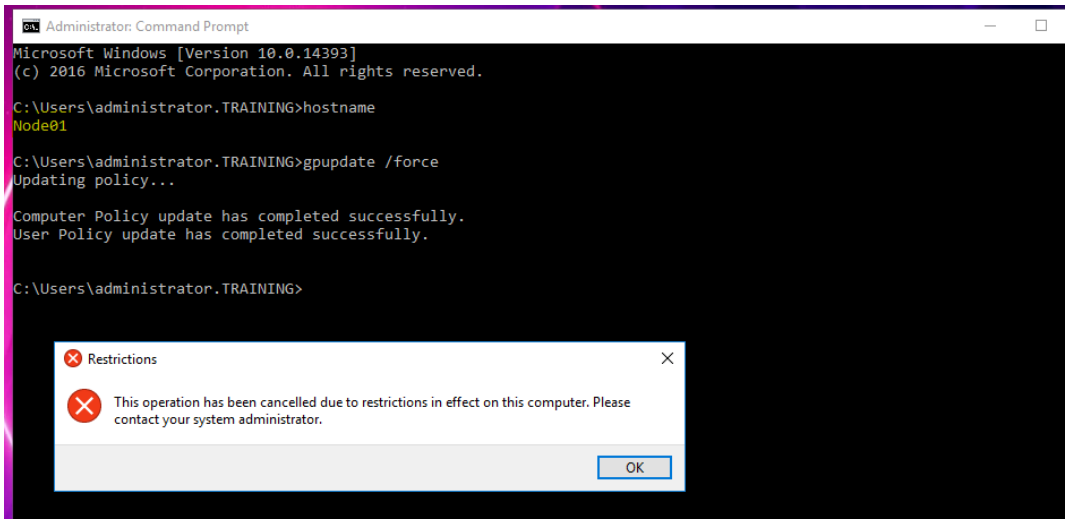
```
C:\Users\Administrator>gpresult /r

Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
© 2016 Microsoft Corporation. All rights reserved.

Created on 6/4/2025 at 10:31:39 PM


RSOP data for TRAINING\Administrator on DC : Logging Mode
------------------------------------------------------------

OS Configuration:            Primary Domain Controller
OS Version:                  10.0.14393
Site Name:                   Default-First-Site-Name
Roaming Profile:             N/A
Local Profile:               C:\Users\Administrator
Connected over a slow link?: No
```

```
Applied Group Policy Objects
-----------------------------
    WallpaperGPO
    Disable Control Panel GPO
```

Verify:

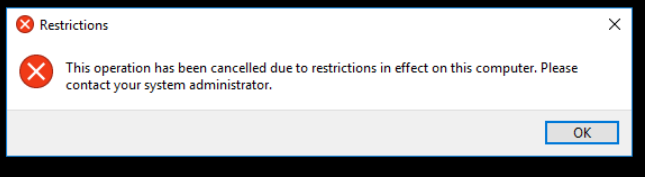


Checking same on Node01

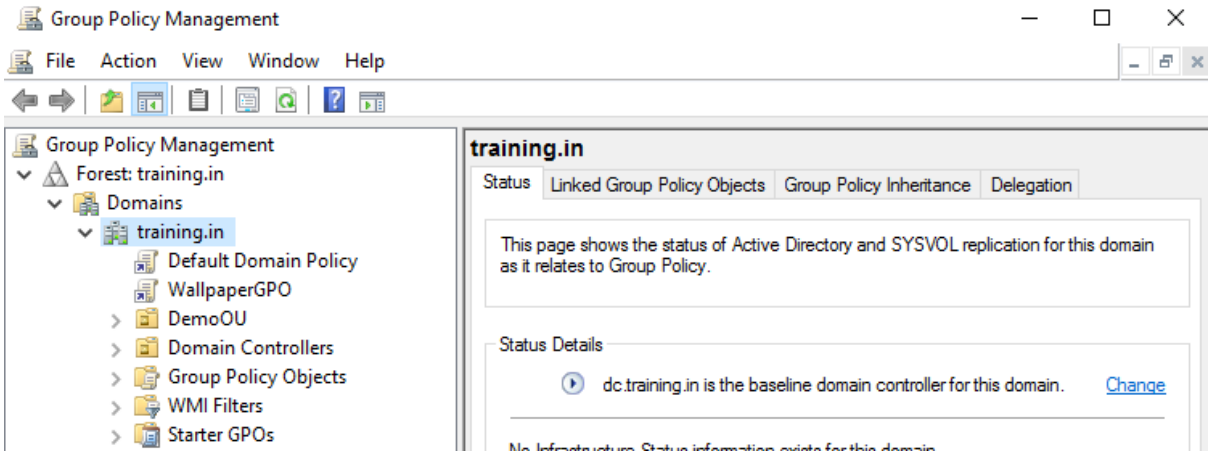


Checking same on Node02

```
C:\Users\administrator.TRAINING>hostname
Node02

C:\Users\administrator.TRAINING>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.


C:\Users\administrator.TRAINING>
```



To remove this GPO, delete the GPO from Group Policy Management Console (GPMC).



And re-run command “gpupdate /force” on all nodes within domain.

Microsoft Deployment Toolkit

What is Microsoft Deployment Toolkit (MDT)?

Microsoft Deployment Toolkit (MDT) is a free, Microsoft-supported solution accelerator that provides a unified collection of tools, processes, and guidance for automating desktop and server deployment.

It is commonly used to deploy:

- Windows client operating systems (Windows 10, 11)
- Windows Server OS (2016, 2019, 2022)
- Applications
- Drivers
- Updates

Key Objectives of MDT

- Automate OS deployment (Zero-Touch / Lite-Touch)
- Simplify large-scale Windows installations
- Create customizable, repeatable deployment environments
- Combine deployment of OS, drivers, apps, and patches

Core Components of MDT

Component	Description
Deployment Workbench	GUI management console to configure deployments
Task Sequences	Series of deployment steps (e.g., install OS, apps, drivers)
Operating System Images	WIM files (captured or from ISO) used in deployments
Boot Images	WinPE images generated by MDT to start deployment
Drivers & Applications	Add necessary device drivers and software for deployment
Answer Files (Unattend.xml)	Automate installation using unattended settings
Deployment Share	Network-accessible folder containing all deployment files
Monitoring	Monitor real-time progress of deployments across machines

Deployment Scenarios

Scenario	Description
Lite-Touch Installation (LTI)	Requires minimal user interaction; initiated manually or via boot media
Zero-Touch Installation (ZTI)	Fully automated; requires integration with Microsoft Endpoint Configuration Manager (SCCM)
User-Driven Installation (UDI)	Offers user choices during deployment via GUI wizard

Requirements

Requirement	Description
Operating System	Windows 10/11 or Windows Server
Windows ADK	Windows Assessment and Deployment Kit (includes WinPE, DISM, USMT)
.NET Framework	Required for the Deployment Workbench
Sufficient Storage	For storing OS images, apps, drivers, logs
Network Access	For PXE/network-based deployment (optional)

What Can You Deploy Using MDT?

- Windows Client OS: Windows 10, Windows 11
- Windows Server OS: 2016, 2019, 2022
- Custom Images: Captured WIM files with preinstalled apps/configs
- Drivers: Imported per model/vendor
- Applications: MSI/EXE with command-line options
- Language Packs and Updates

Deployment Workflow in MDT

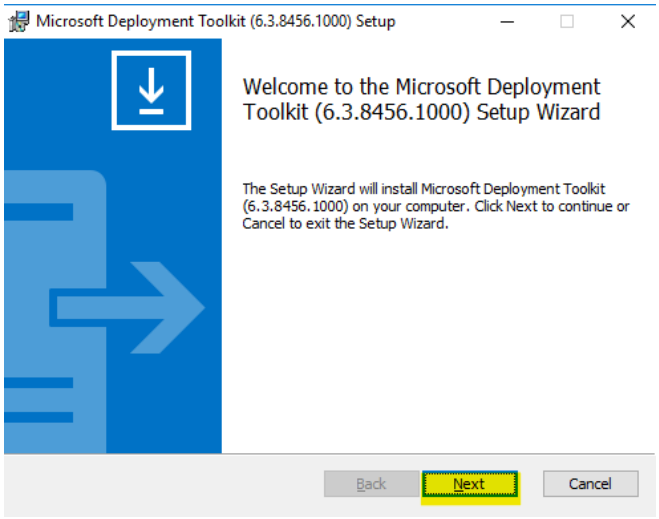
1. **Install Windows ADK** and **WinPE Add-on**
2. **Install MDT**
3. Open **Deployment Workbench**
4. Create a **Deployment Share**
5. Import:
    - Operating System images (WIM files)
    - Drivers
    - Applications
    - Language Packs
6. Create **Task Sequences** to define the deployment process
7. Configure **Unattend.xml** (automated settings)
8. Generate **Boot Image (ISO or WIM)**
9. Use:
    - ISO file (burn to USB/DVD)
    - PXE boot (if WDS is configured)
10. Monitor and manage deployments

Features of MDT

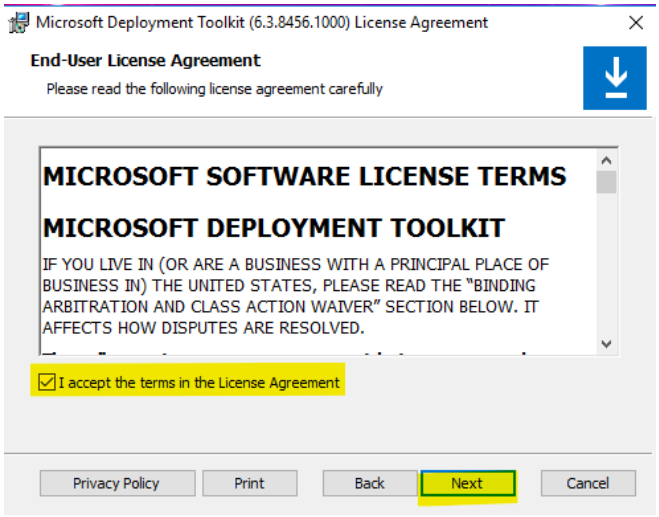
Feature	Description
Custom Task Sequences	Full control over the steps during deployment
Pre- and Post-Installation Scripting	Add PowerShell or VB scripts to customize setup
Integration with WDS	Enables PXE booting for deployments
Driver Injection	Automatically injects model-specific drivers
Offline Media Deployment	Create USB media for disconnected environments
Role-based Deployment	Choose between multiple OS/apps configurations
Monitoring Console	Track deployment progress and errors

Creating and managing deployment images by using MDT

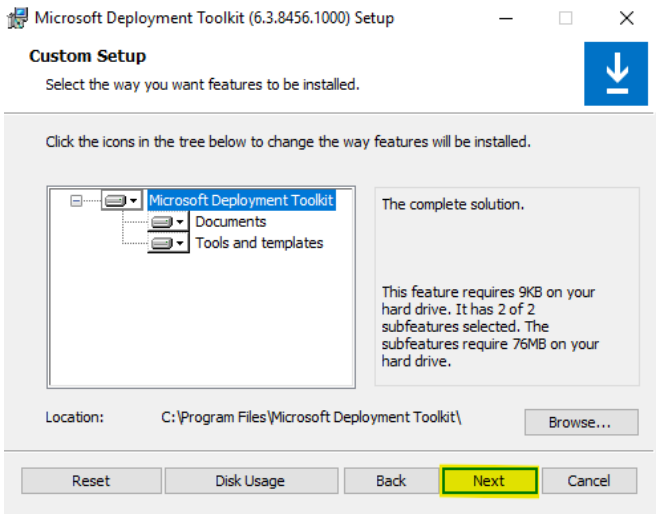
Download MDT using this link. After downloading the setup, install it.



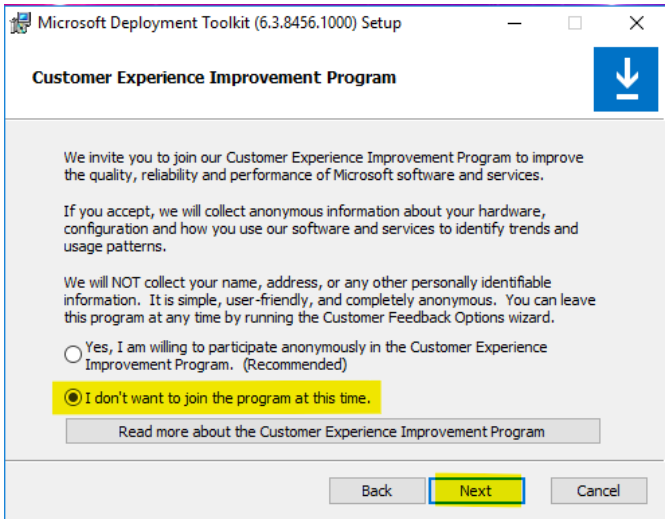
Accept the license.



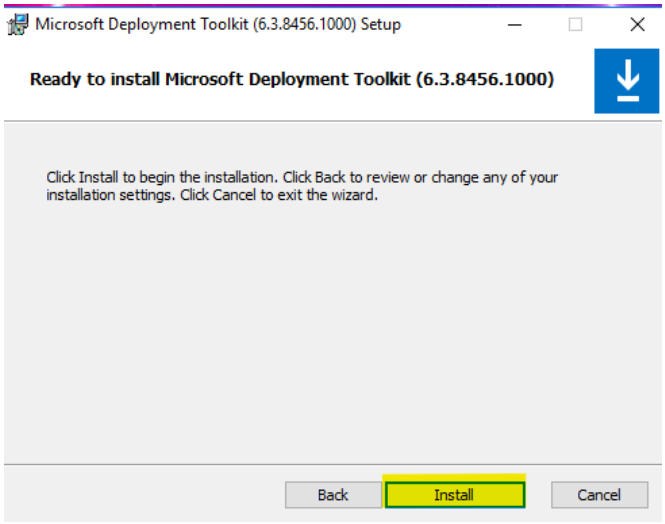
Use default values



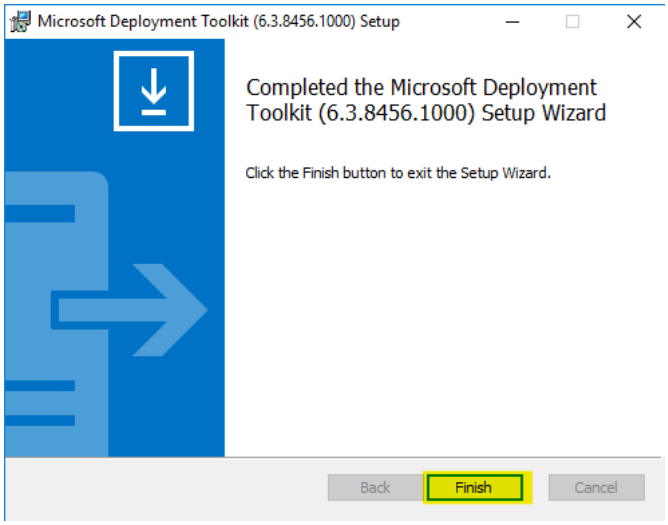
Proceed by clicking on “Next”



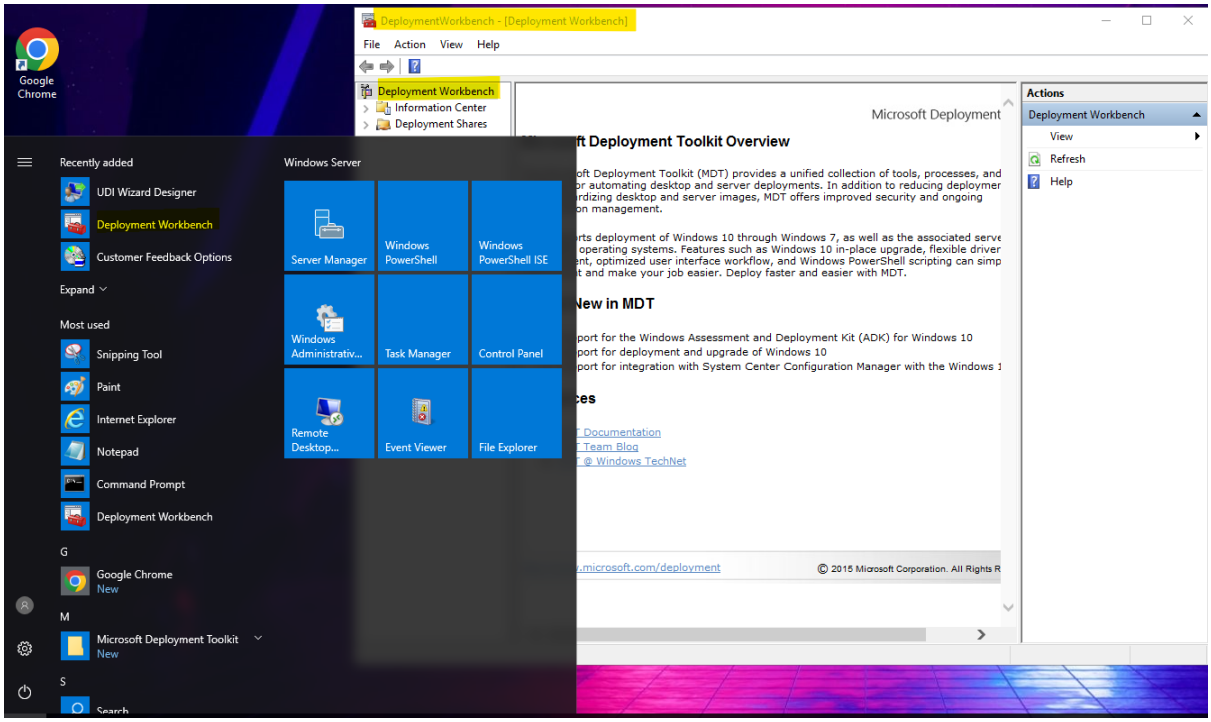
Click install



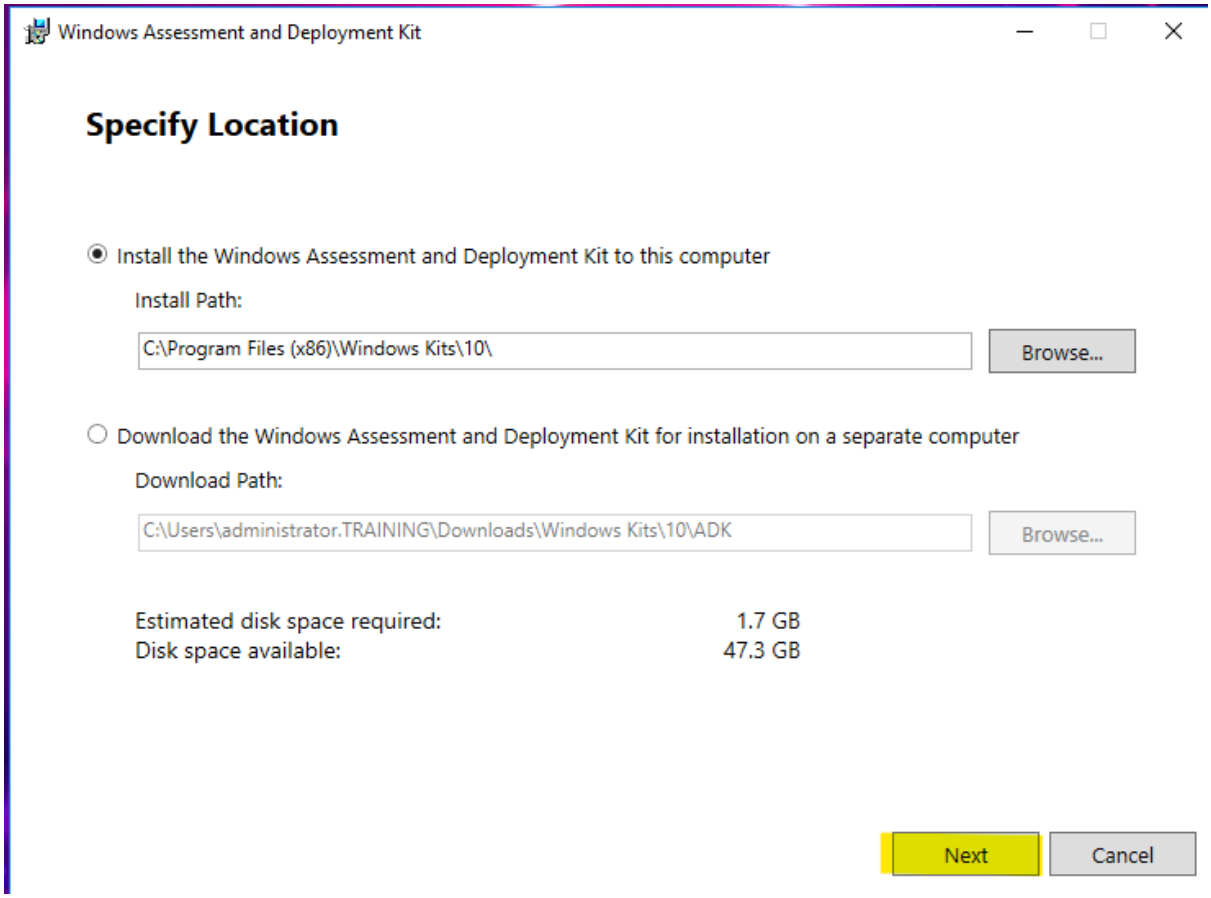
Click Finish

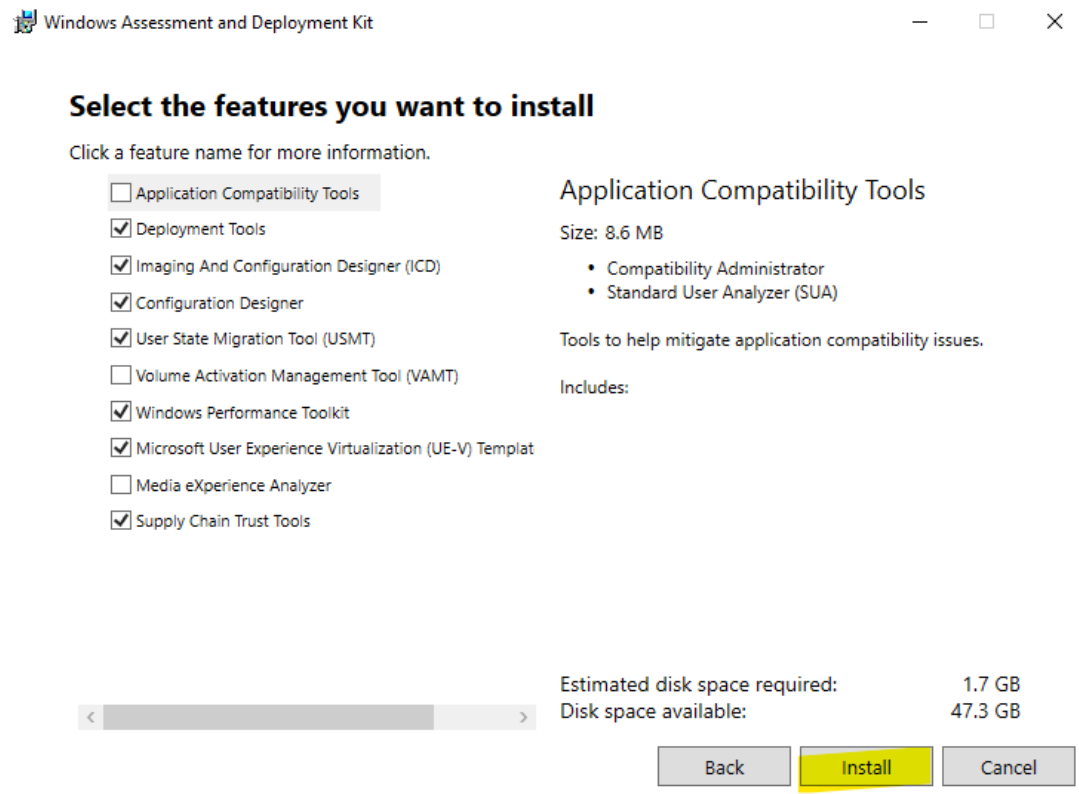


Search for Deployment workbench & open it.

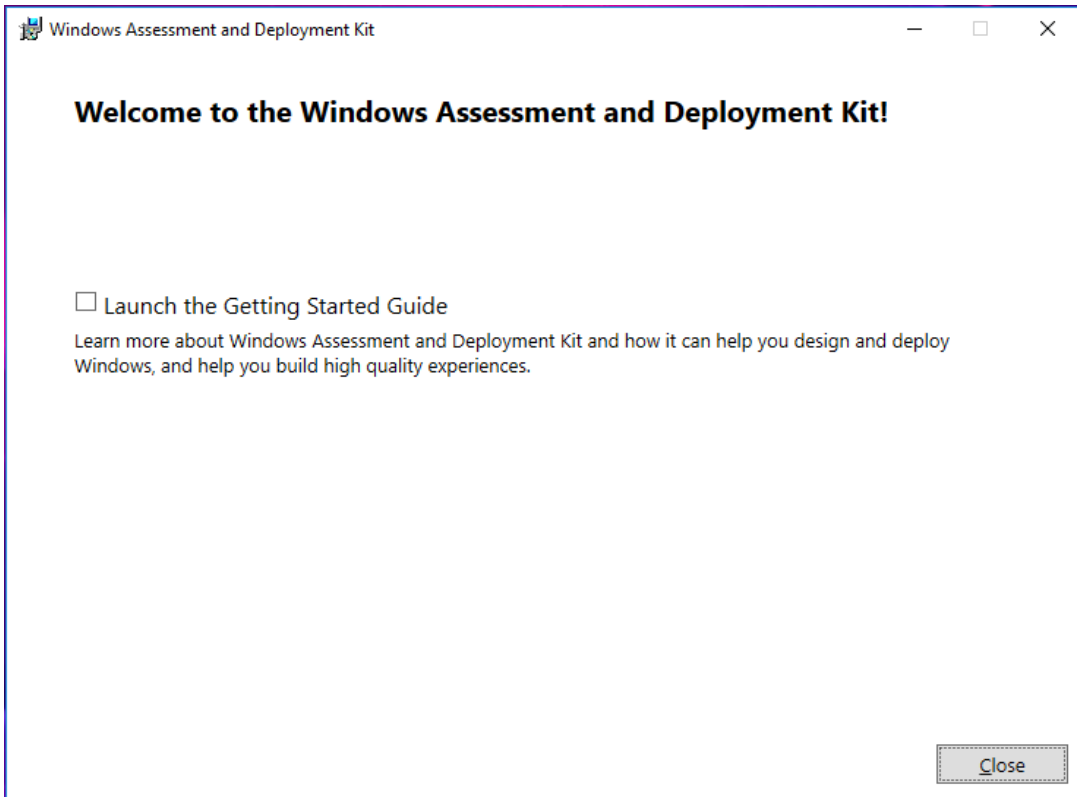


Download and install Assessment and Deployment Kit (Windows ADK) – Link.

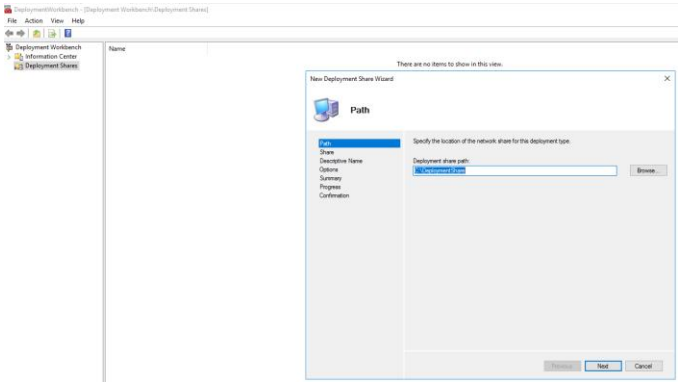




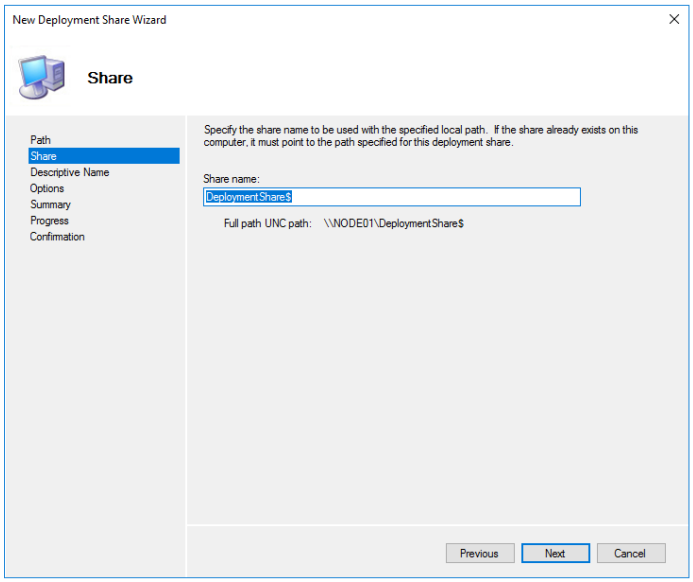
After the download, click “Close”



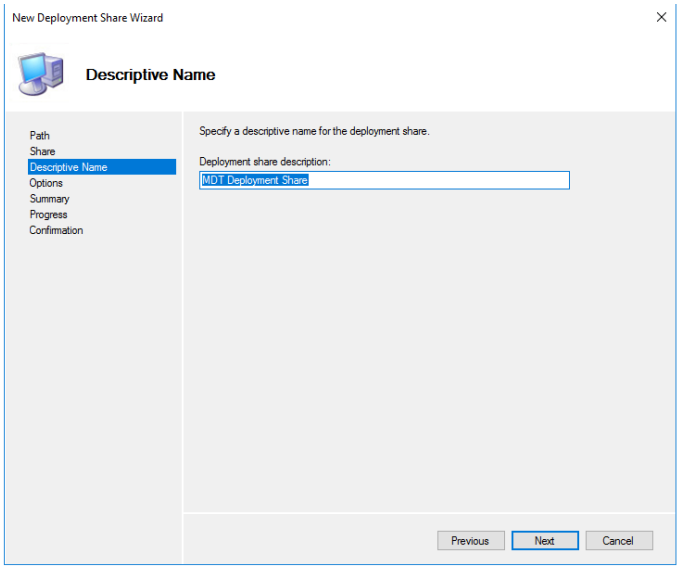
Now open Deployment Workbench and right-click on Deployment share for new wizard



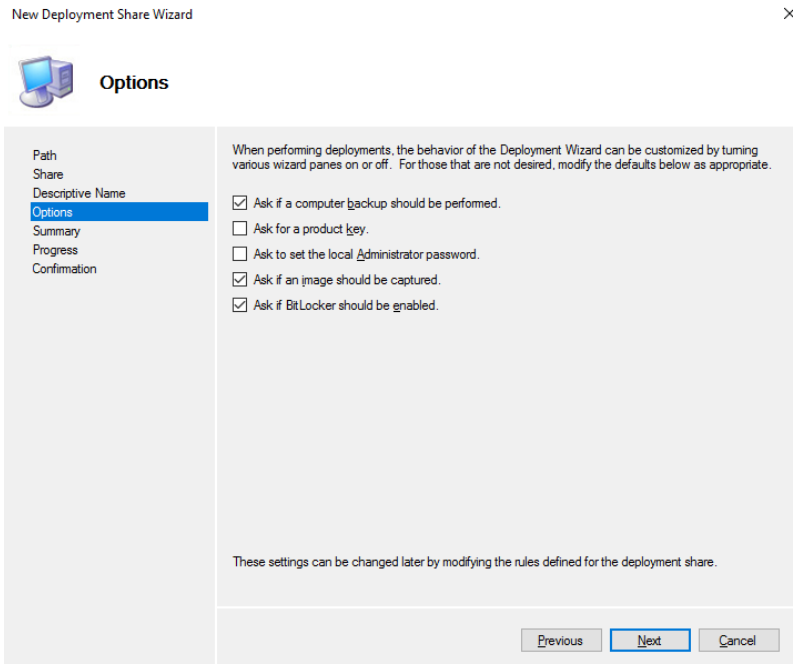
Select the default share name:

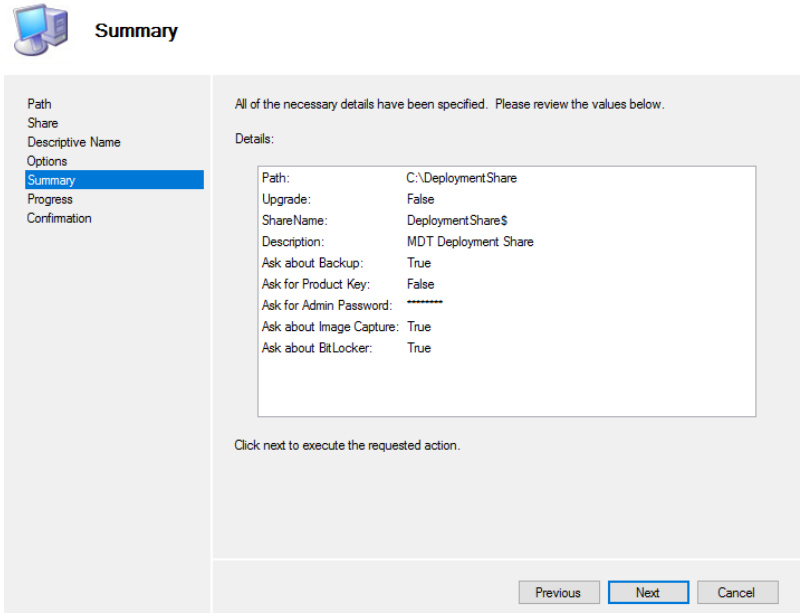


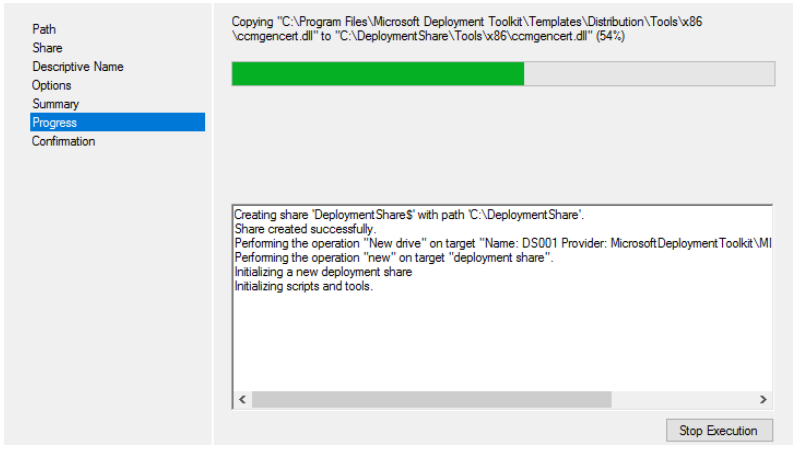
Use default descriptive name:



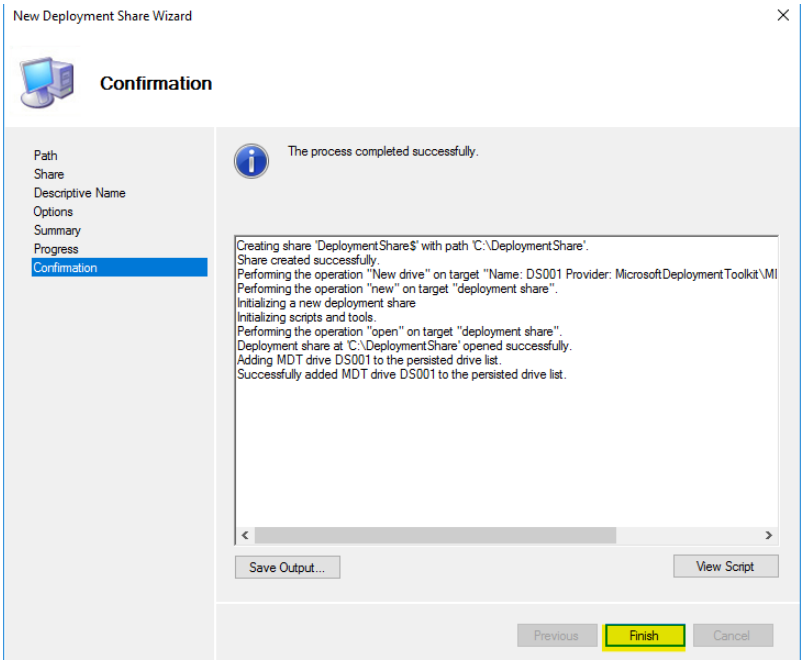
On the Options page, accept the default settings and select Next twice, and then select Finish.







Click finish



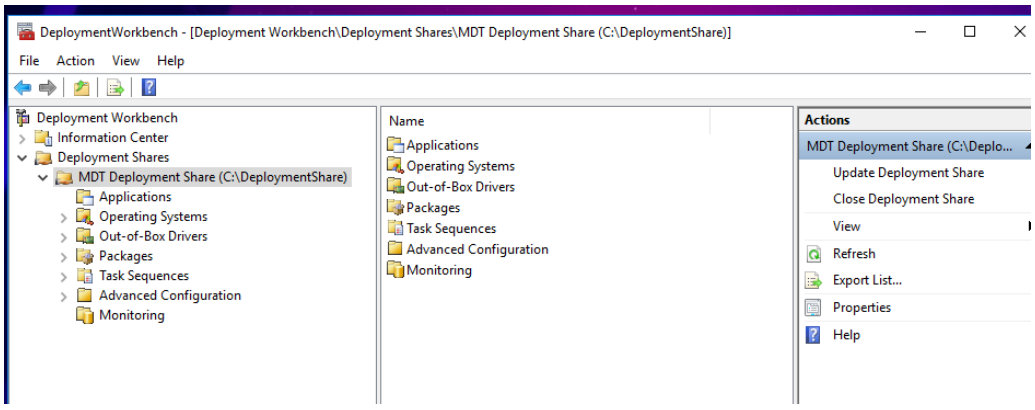
Configure permissions for the production deployment share:

1. Create a new directory
    a. > mkdir C:\MDTProduction
2. Modify NTFS and SMB permission
    a. > icacls.exe "C:\MDTProduction" /grant '"training\administrator":(OI)(CI)(M)'

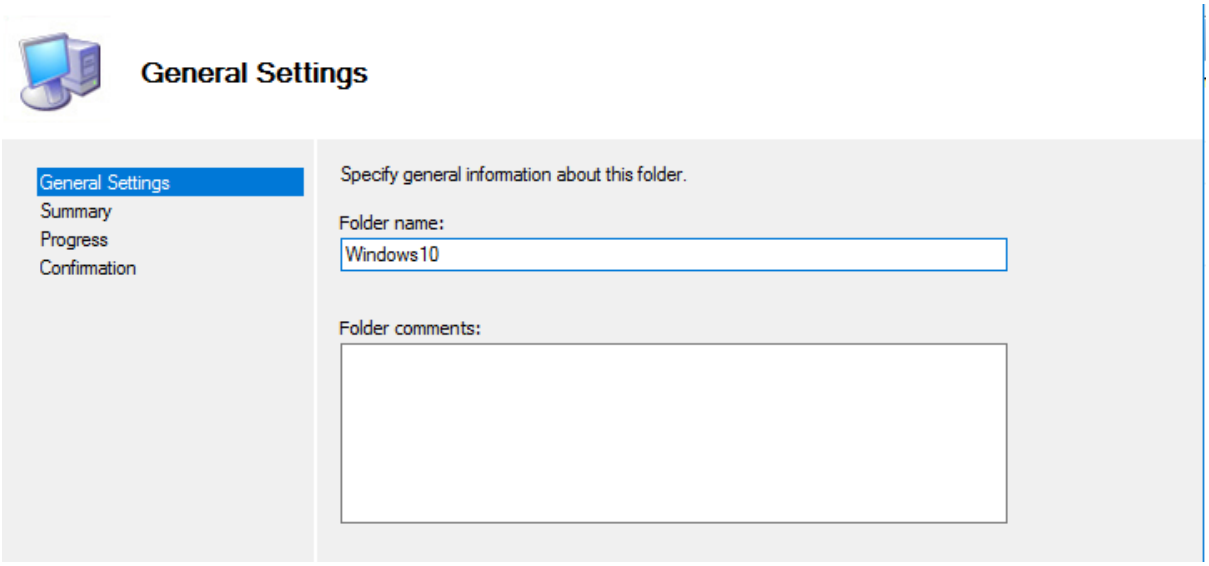
```
PS C:\Users\administrator.TRAINING> mkdir C:\MDTProduction


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         6/4/2025  11:40 PM                MDTProduction


PS C:\Users\administrator.TRAINING> icacls.exe "C:\MDTProduction" /grant '"training\administrator":(OI)(CI)(M)'
processed file: C:\MDTProduction
Successfully processed 1 files; Failed processing 0 files
PS C:\Users\administrator.TRAINING>
```

Now, Add a custom image

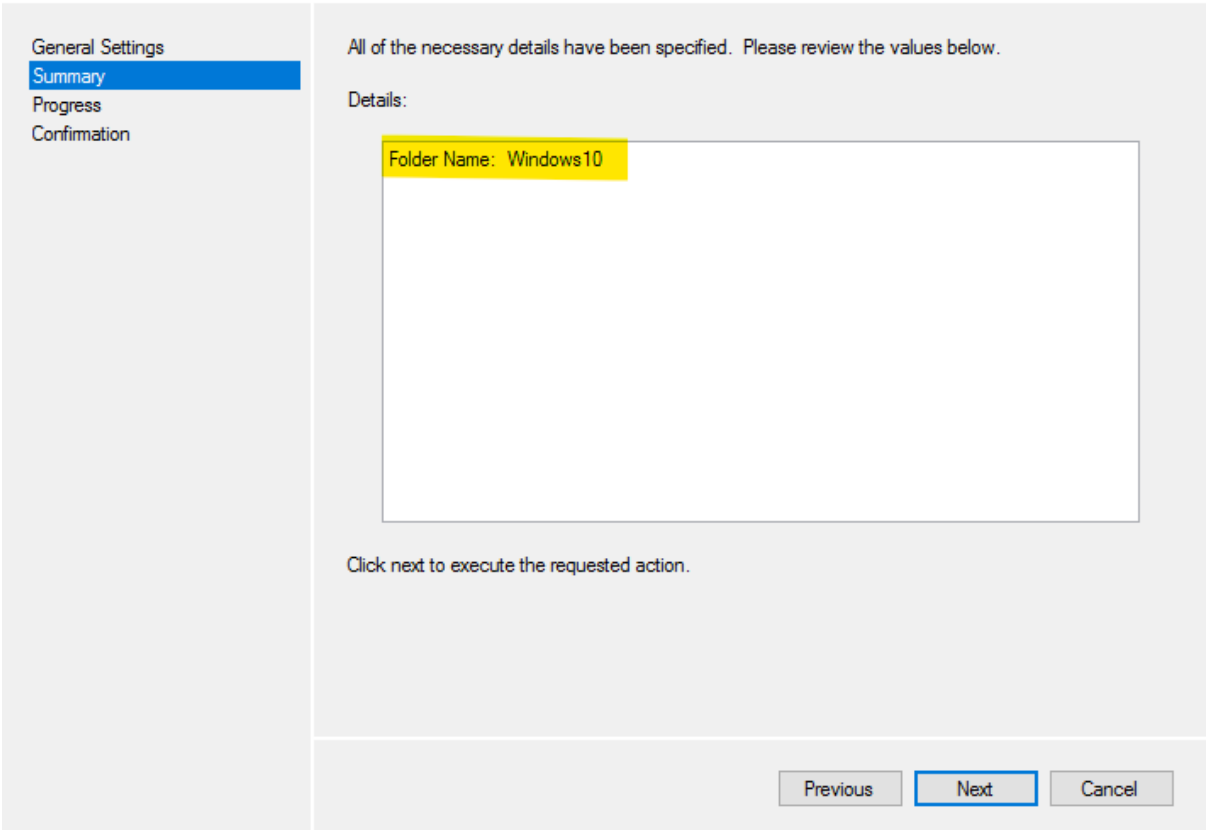
Ensure MDT is configured and ISO is present on Node01 (wither copy from base machine or download a new ISO).



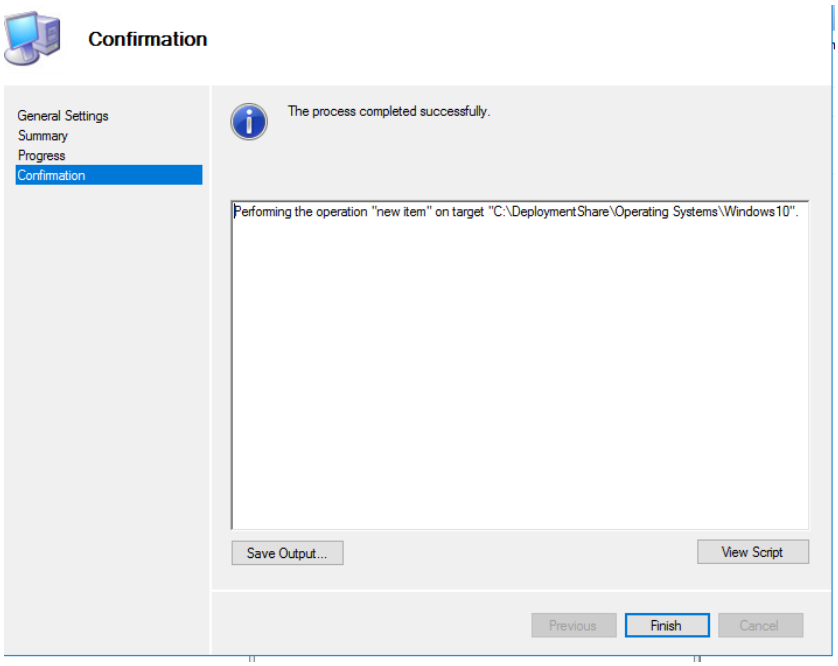
Using the Deployment Workbench, expand the Deployment Shares node, and then expand MDT Production; select the Operating Systems node, and create a folder named Windows 10.



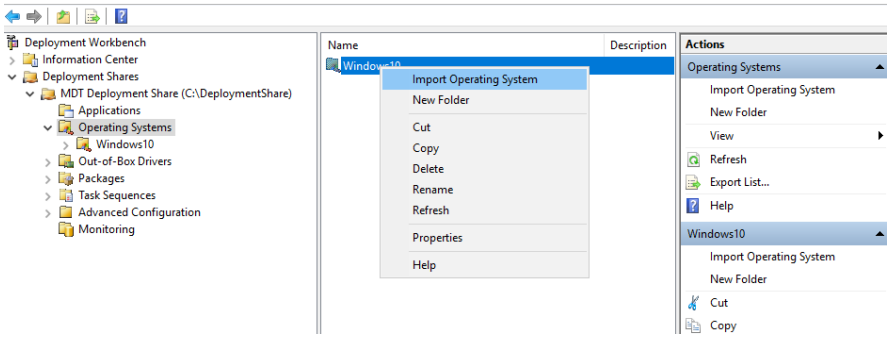
Click Next.



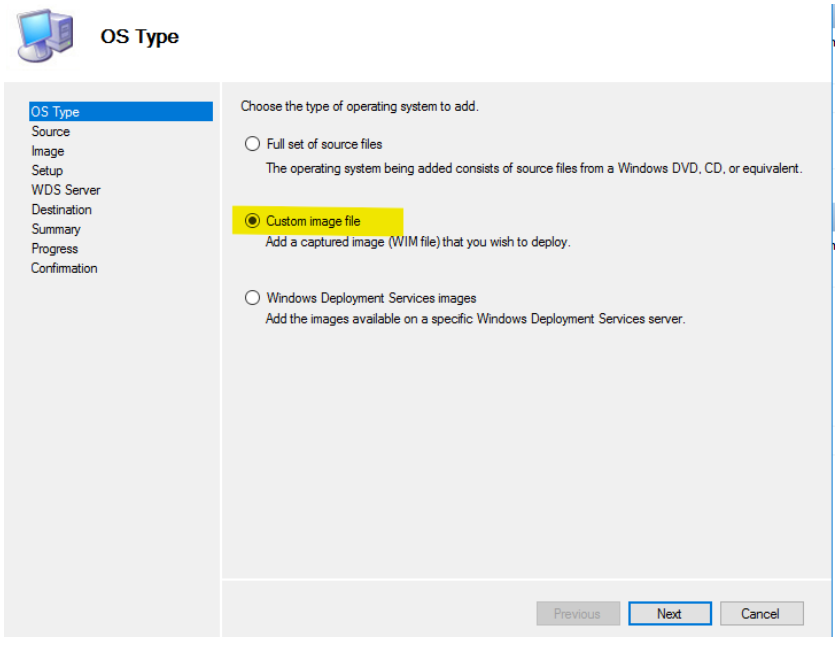
Validate and finish



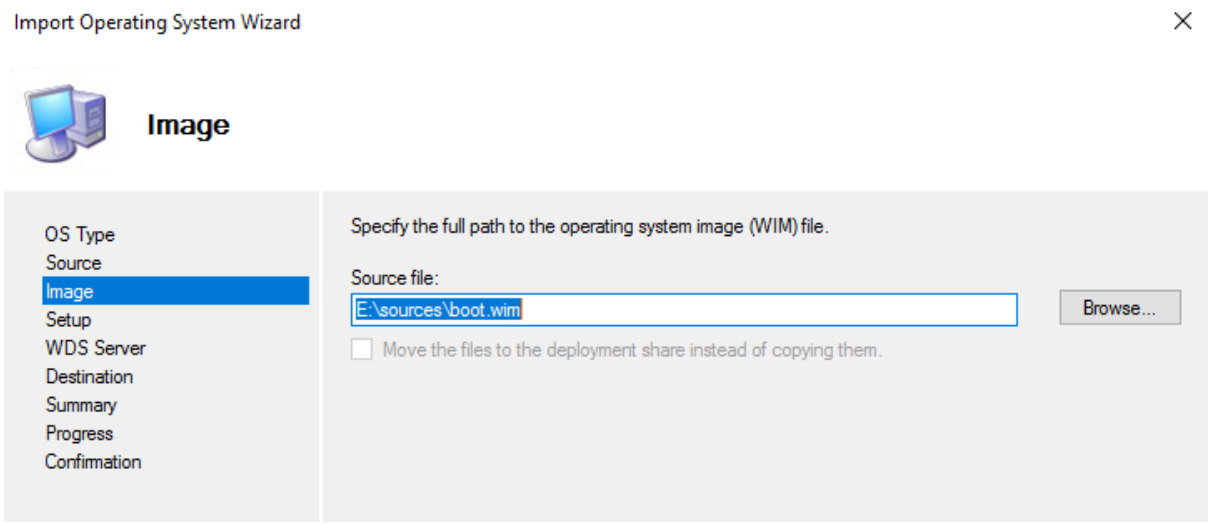
Right-click the Windows 10 folder and select Import Operating System



On the OS Type page, select Custom image file and select Next

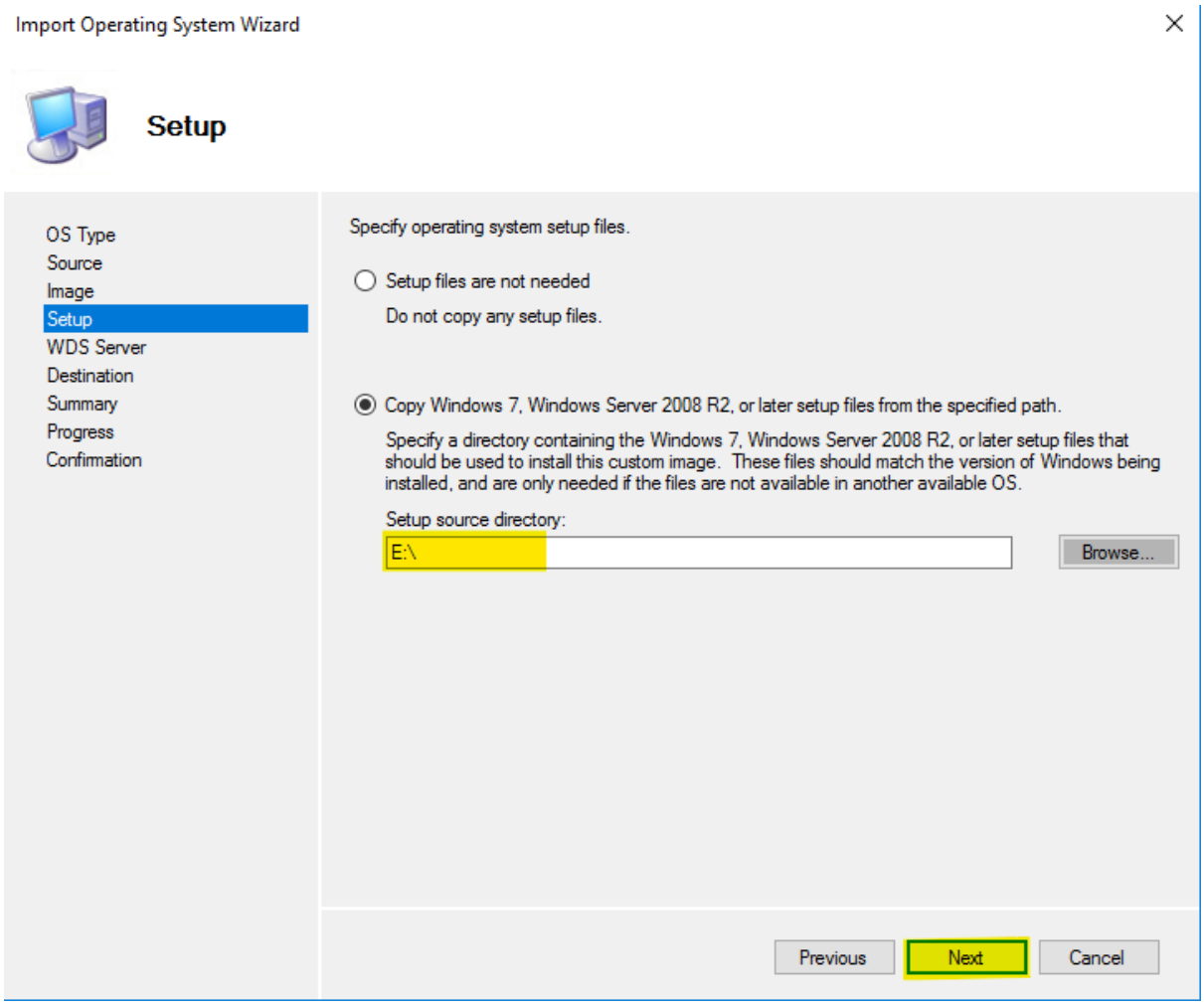


Extract or mount the ISO file and browse to d:\sources\install.wim

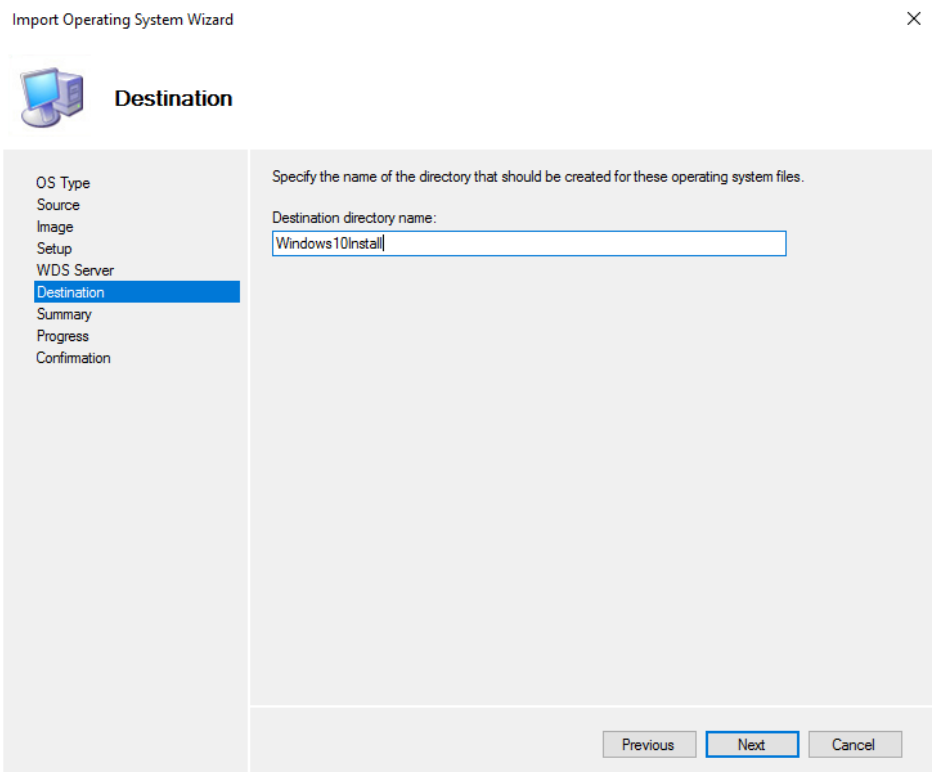


Click Next.

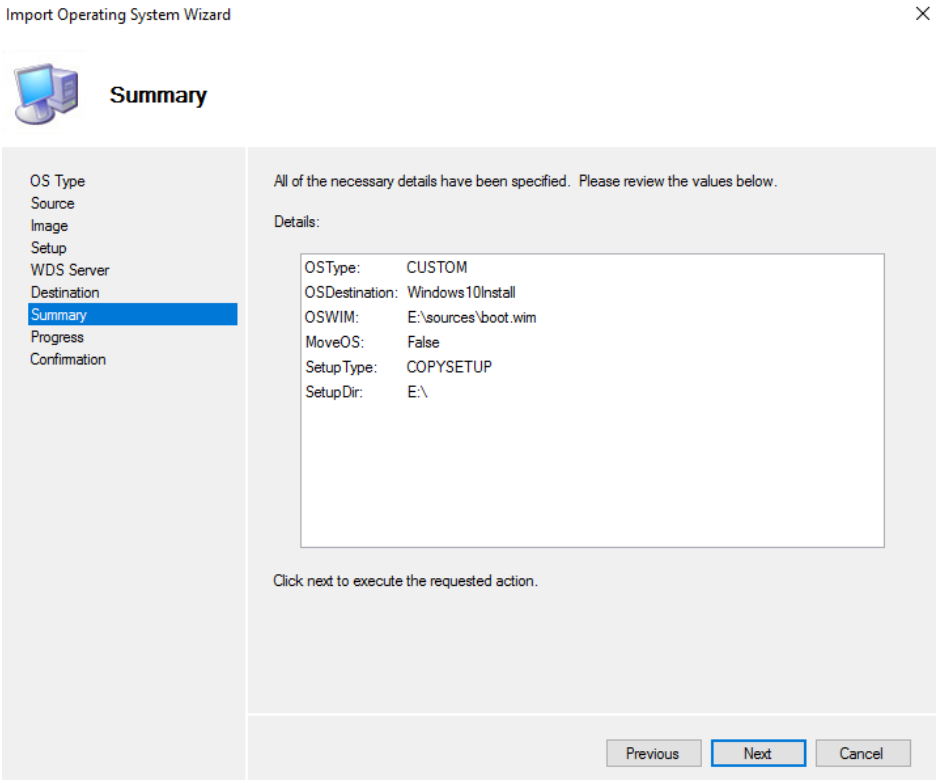
On the Setup page, select the Copy Windows 7, Windows Server 2008 R2, or later setup files from the specified path option; in the Setup source directory text box (D:\ drive)



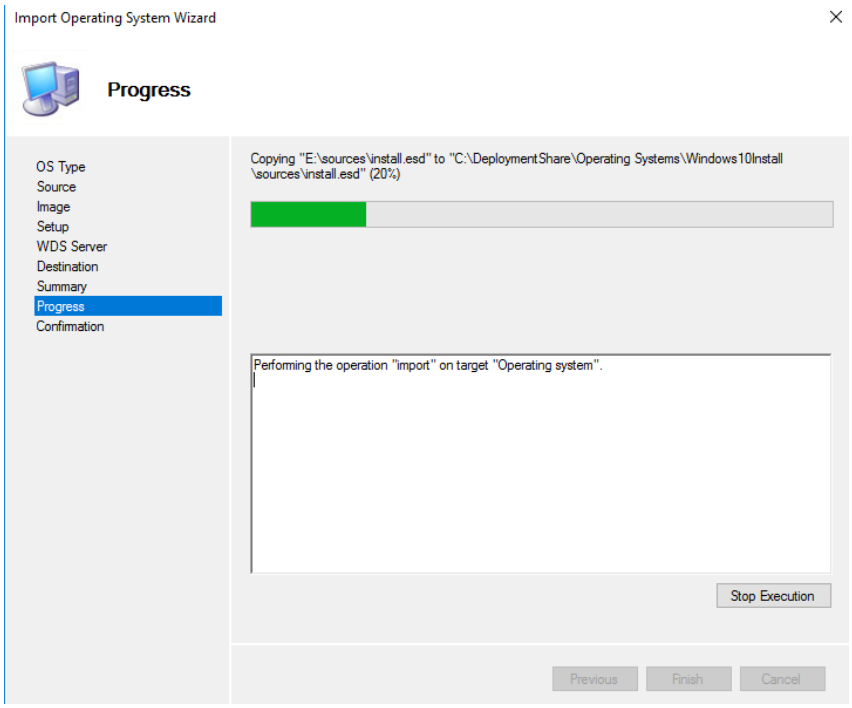
Provide install directory name:



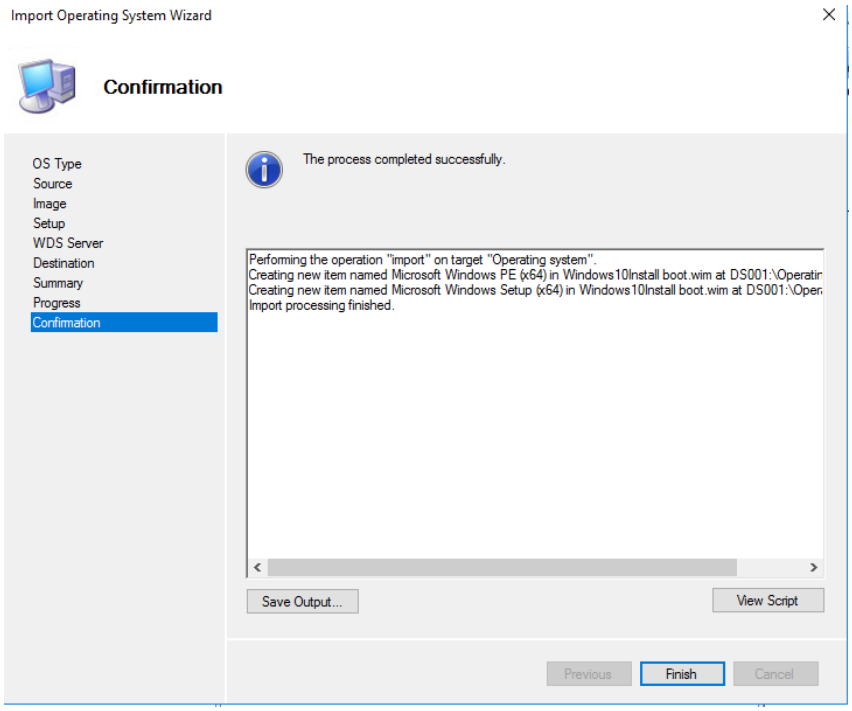
Verify from summary:



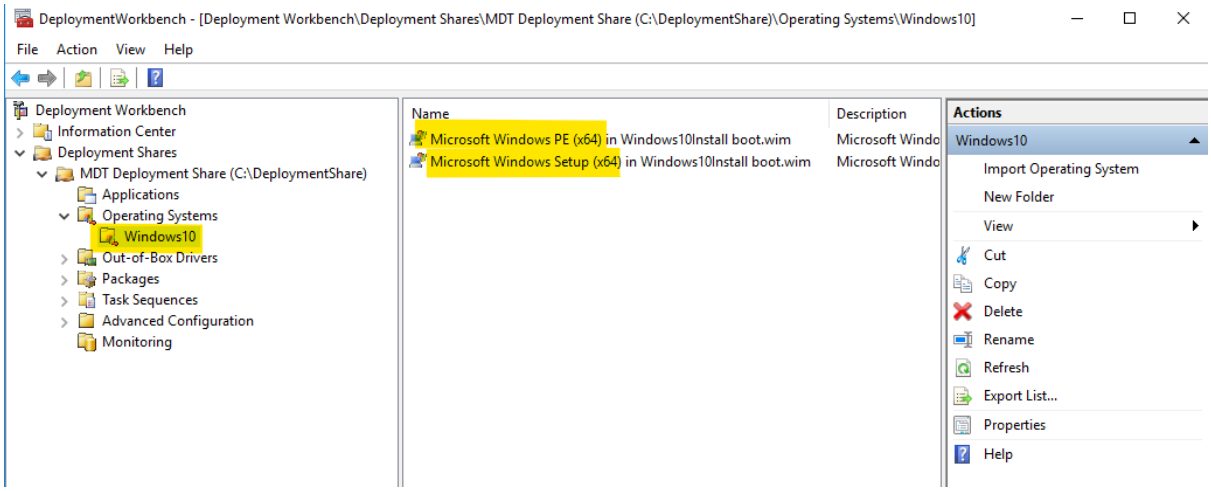
In progress:



Verify and then click finish:



Verify:

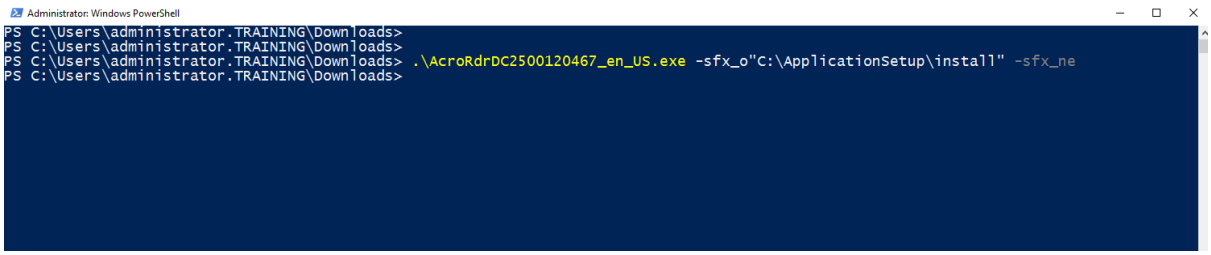


Add an application (Adobe Reader DC) – Link to download

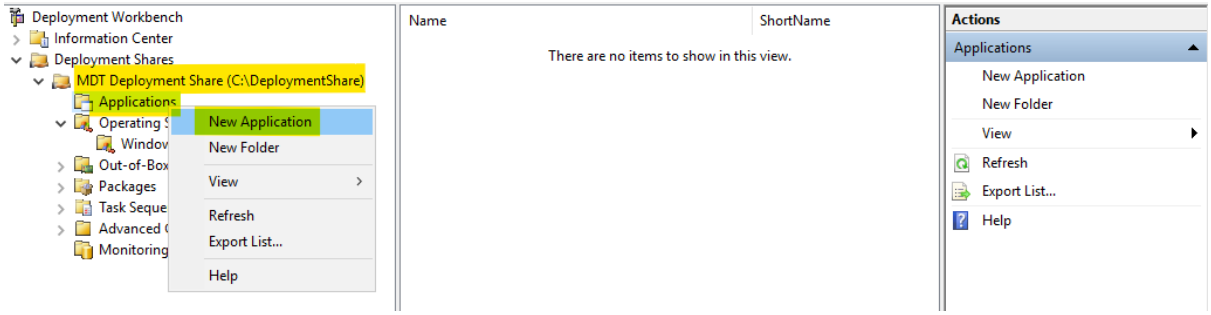
Once downloaded as .exe file, convert this into /msi file using command

PowerShell → *.\AcroRdrDC2500120467_en_US.exe -sfx_o"C:\ApplicationSetup\install" -sfx_ne*

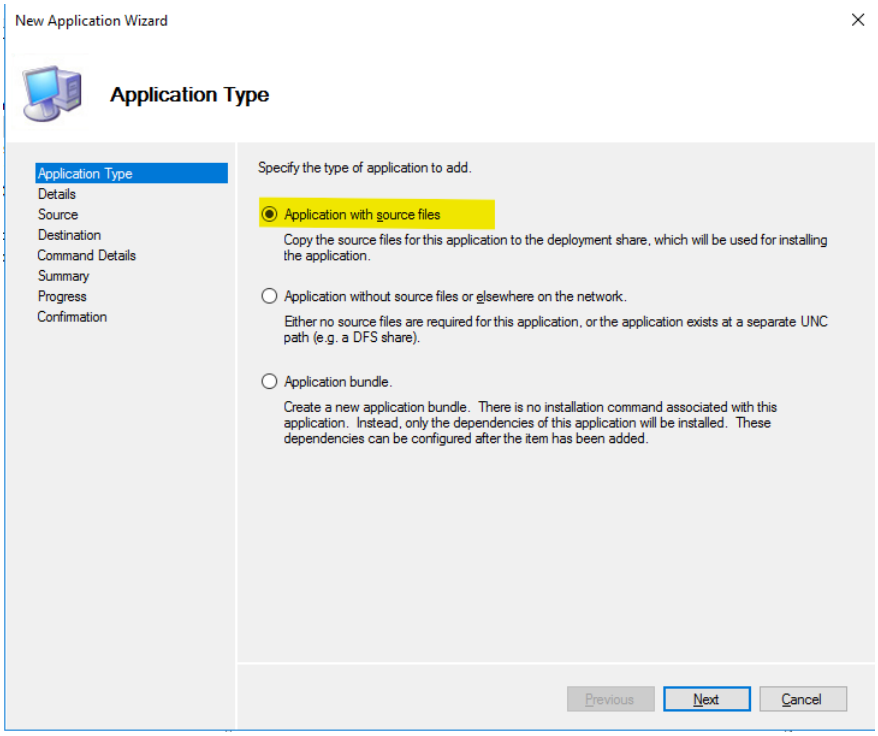
This will extract .msi package under *"C:\ApplicationSetup\install" folder.*



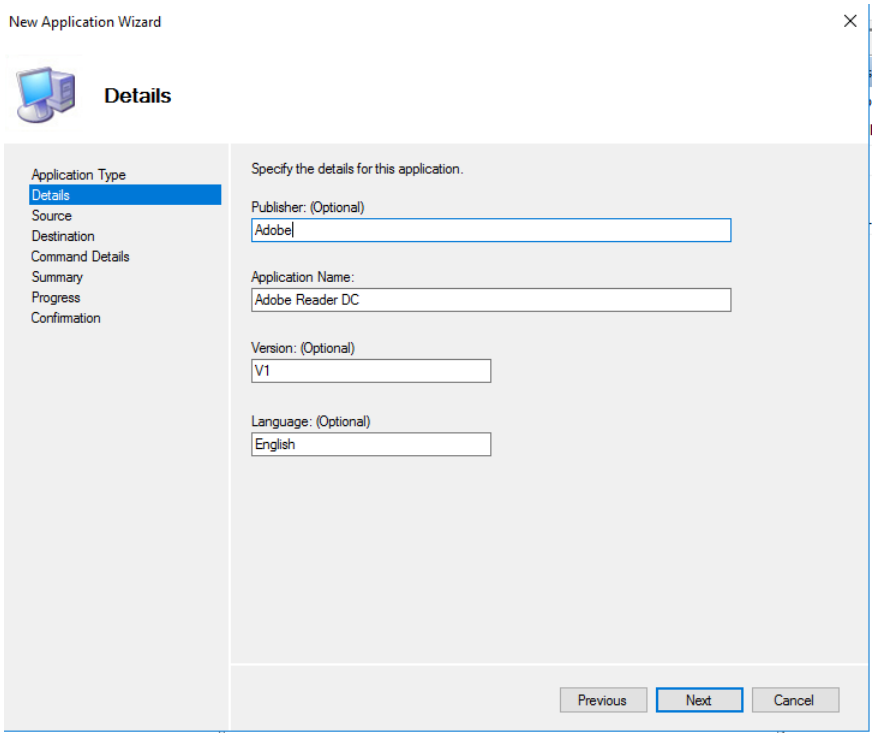
In the Deployment Workbench, expand the DeploymentShare node and navigate to the Applications node. Right-click the Applications node, and create a new folder named Adobe.



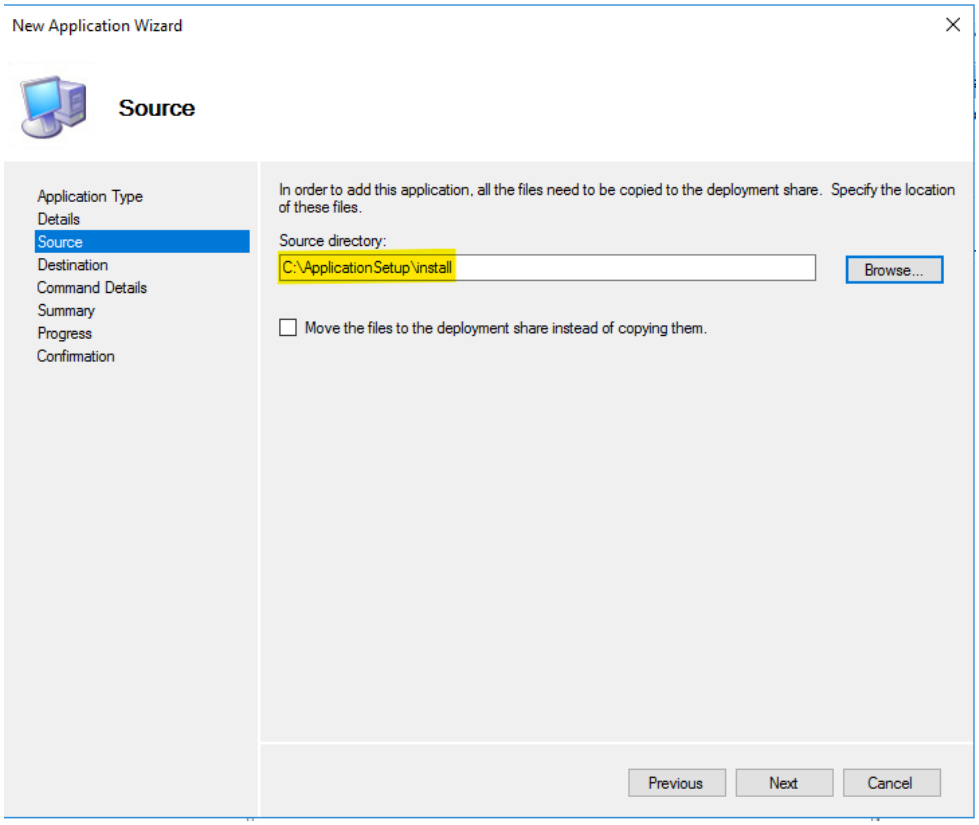
Select Application Type:



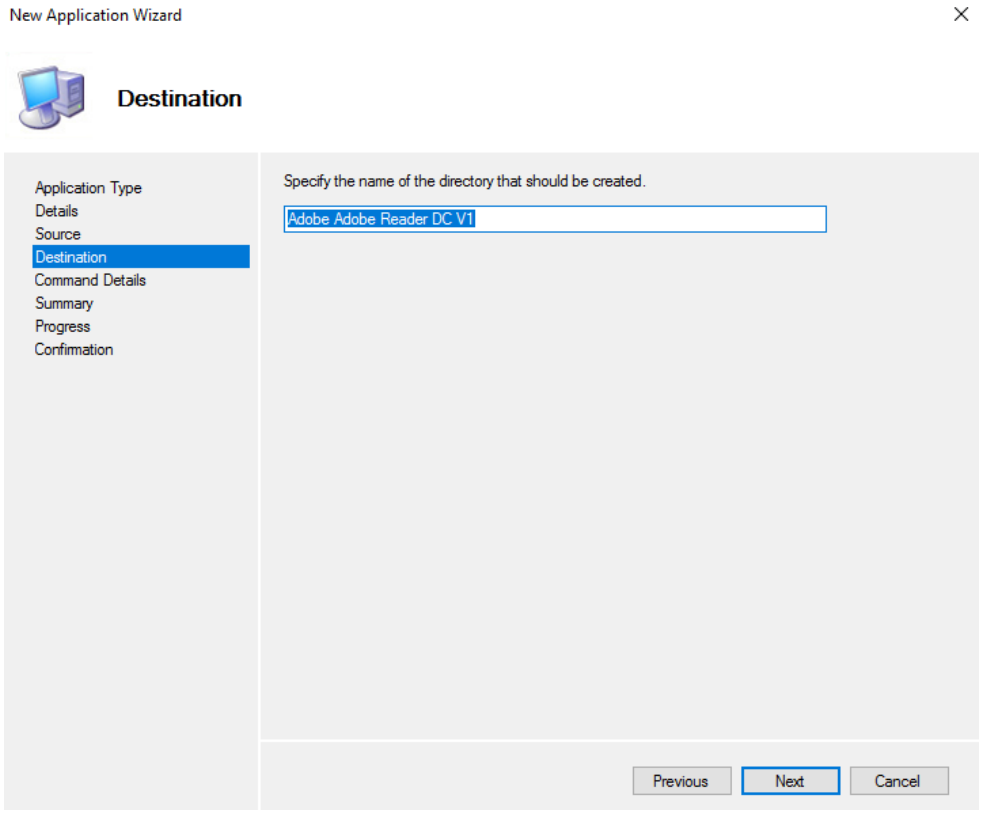
Fill basic details:



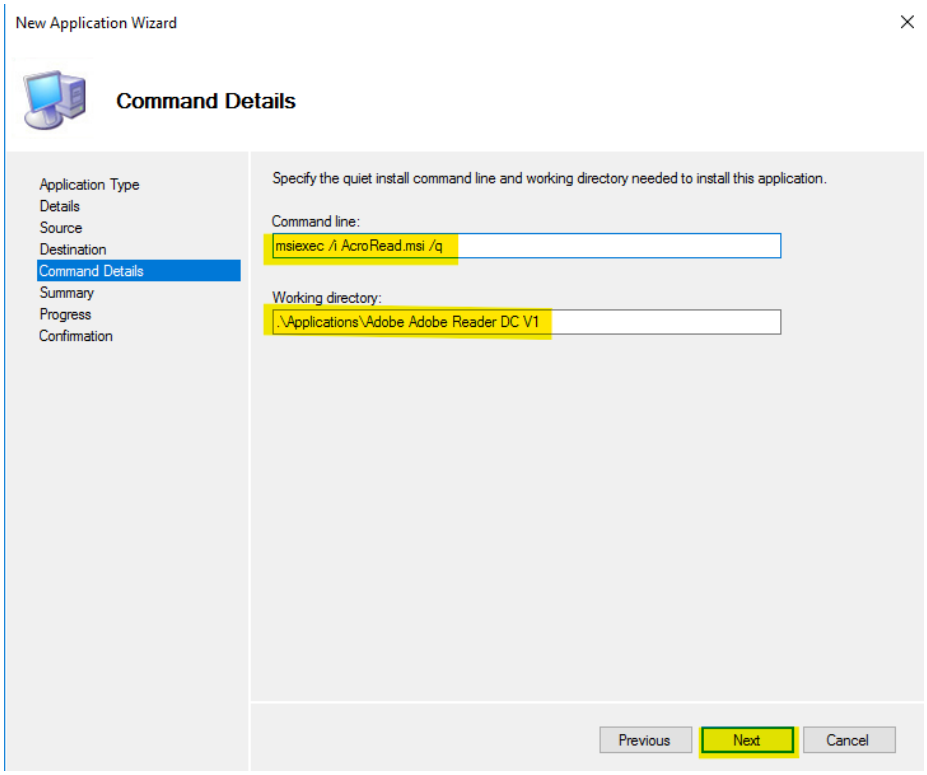
Create a new folder and copy the Adobe Reader application to it and browse the source.



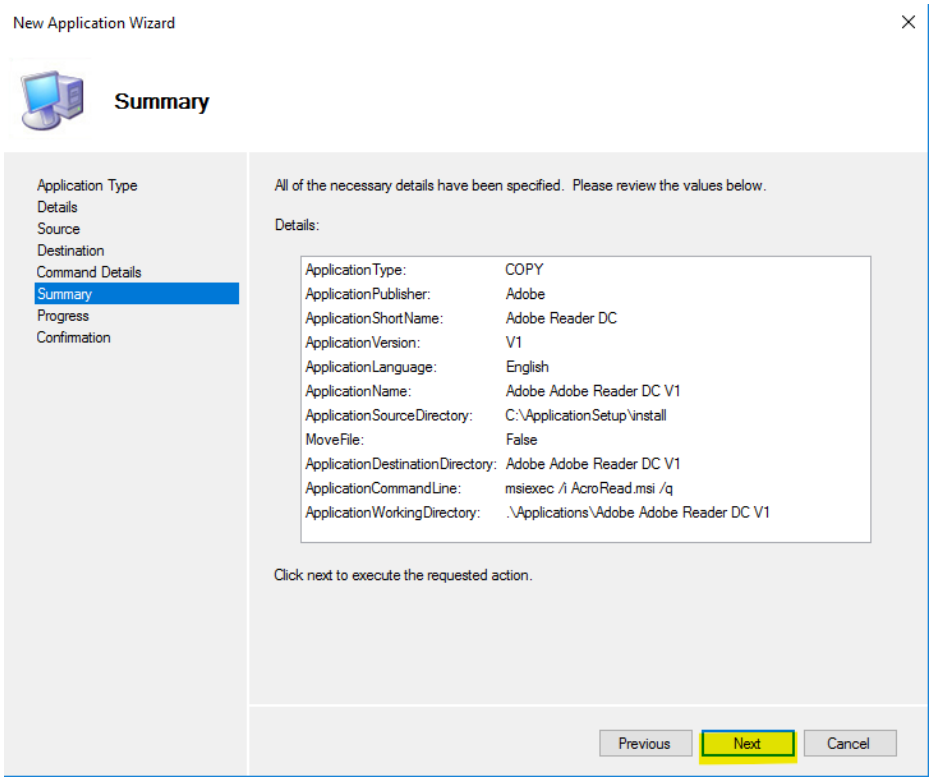
Verify:



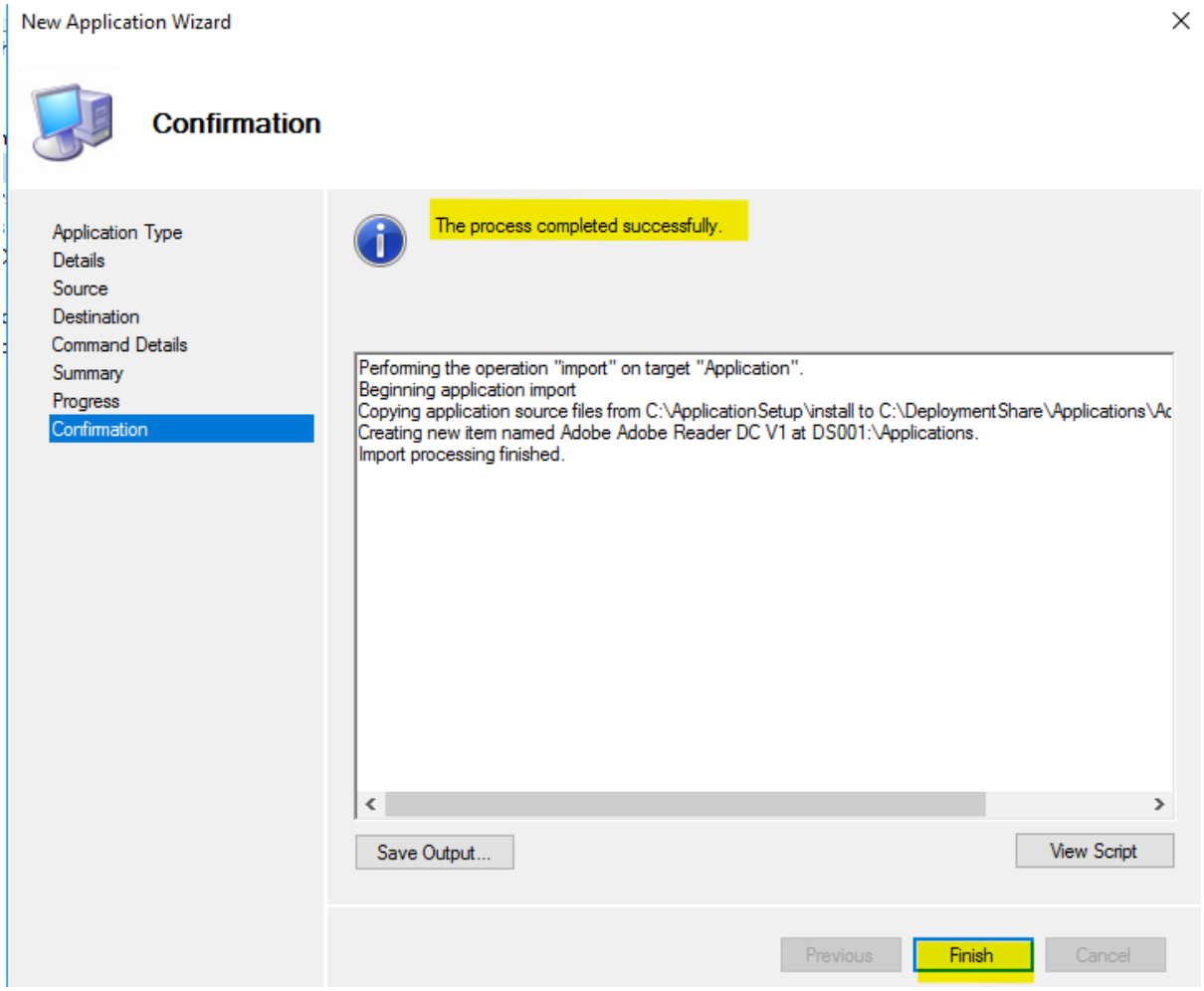
In command details, write command "**msiexec /i AcroRead.msi /q**" to quietly install the setup.



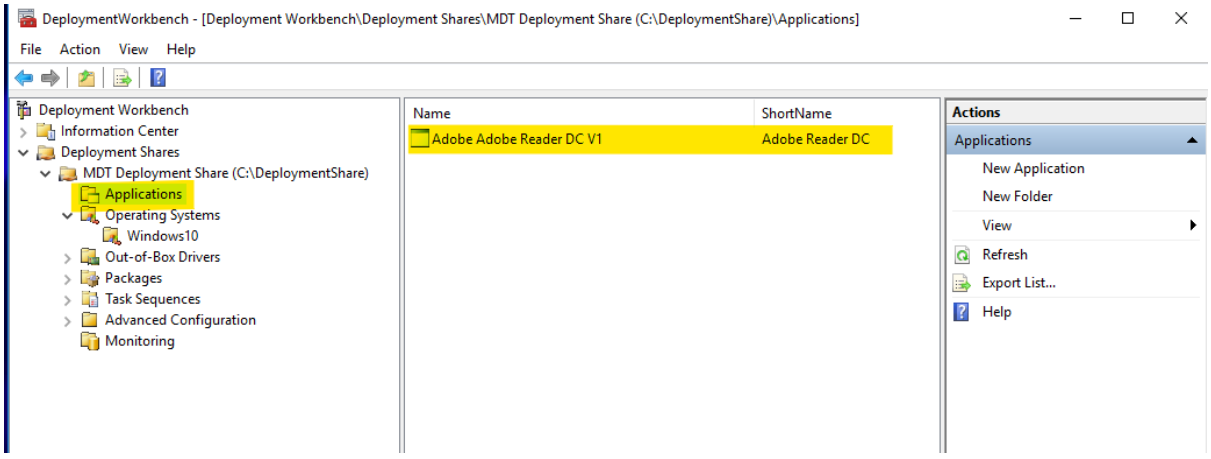
Verify summary:



After the progress is successfully completed, click Finish.

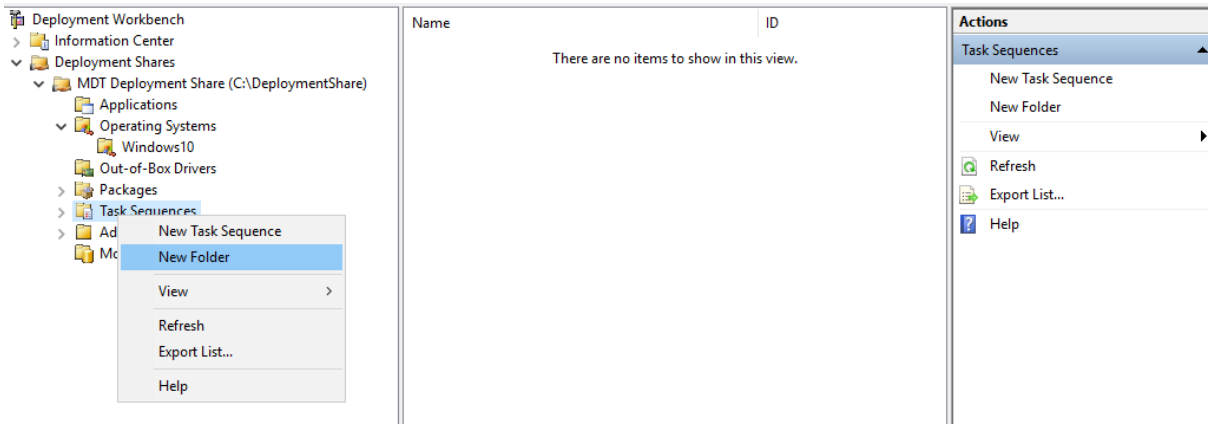


Verify:

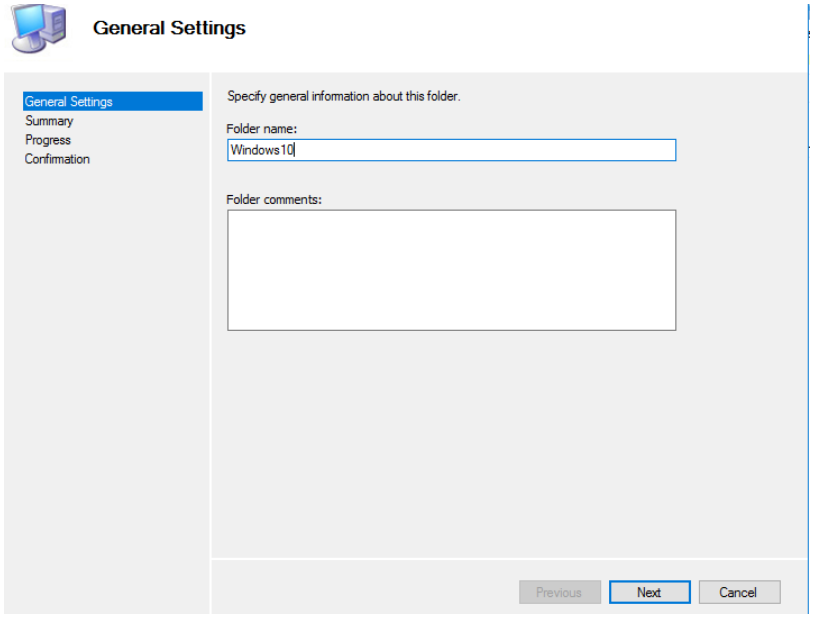


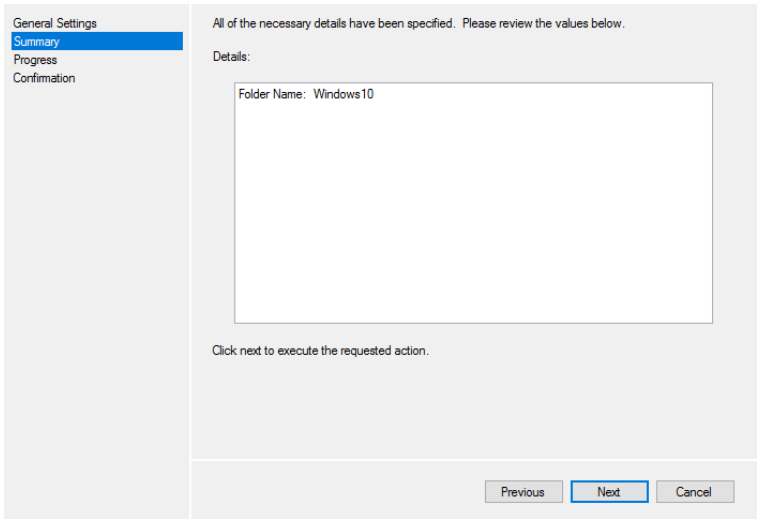
Create a task sequence for Windows 10 Enterprise

In the Deployment Workbench, under the “Deployment Share” node, right-click Task Sequences, and create a folder named Windows 10. Right-click the new Windows 10 folder and select New Task Sequence.

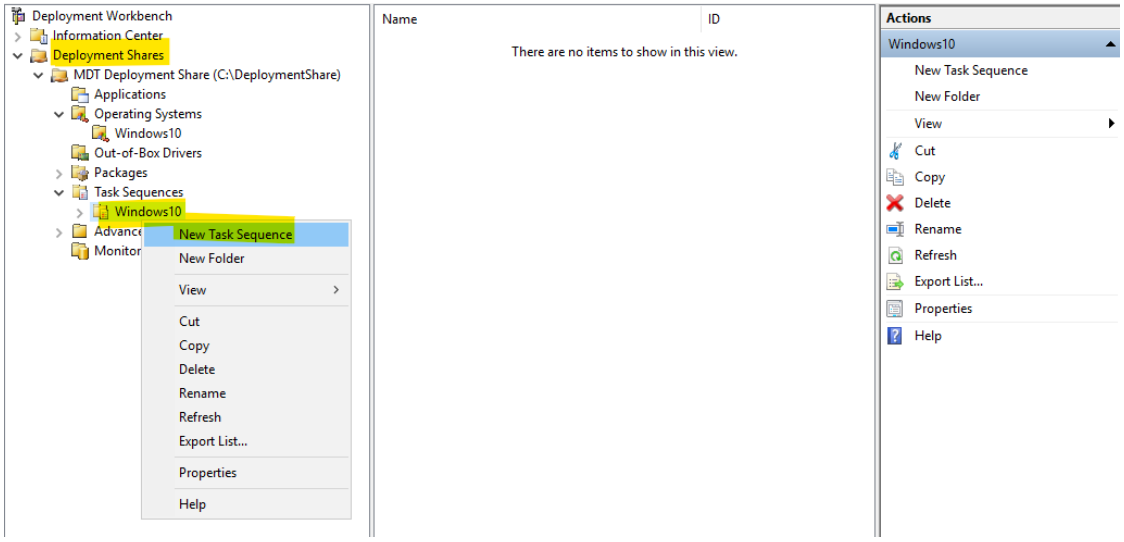


Type window 10

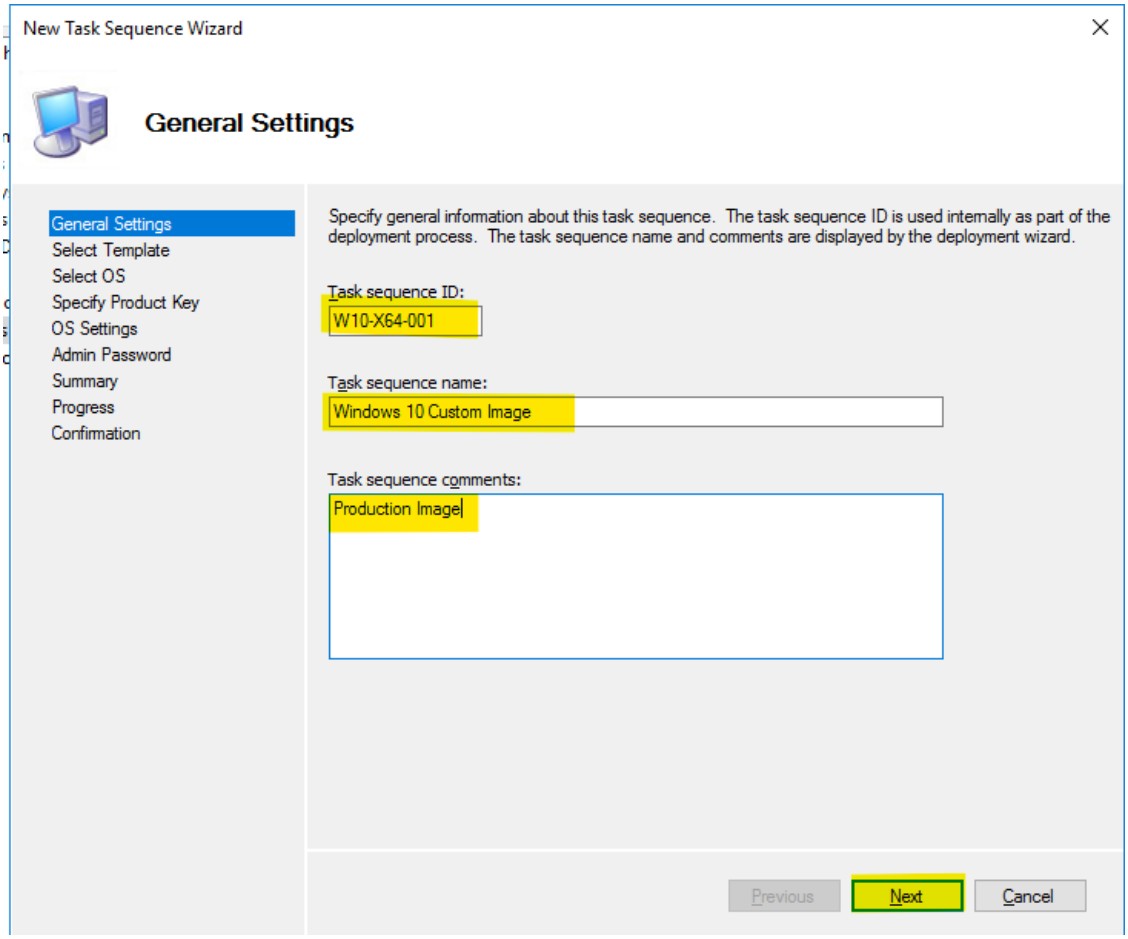




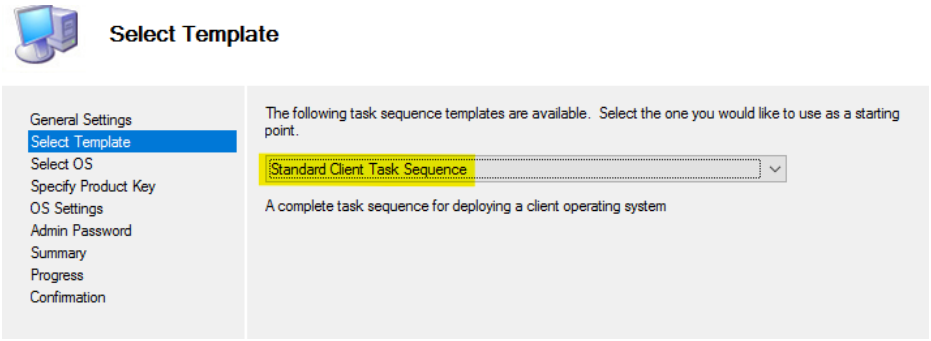
Create New Task Sequence under Windows 10



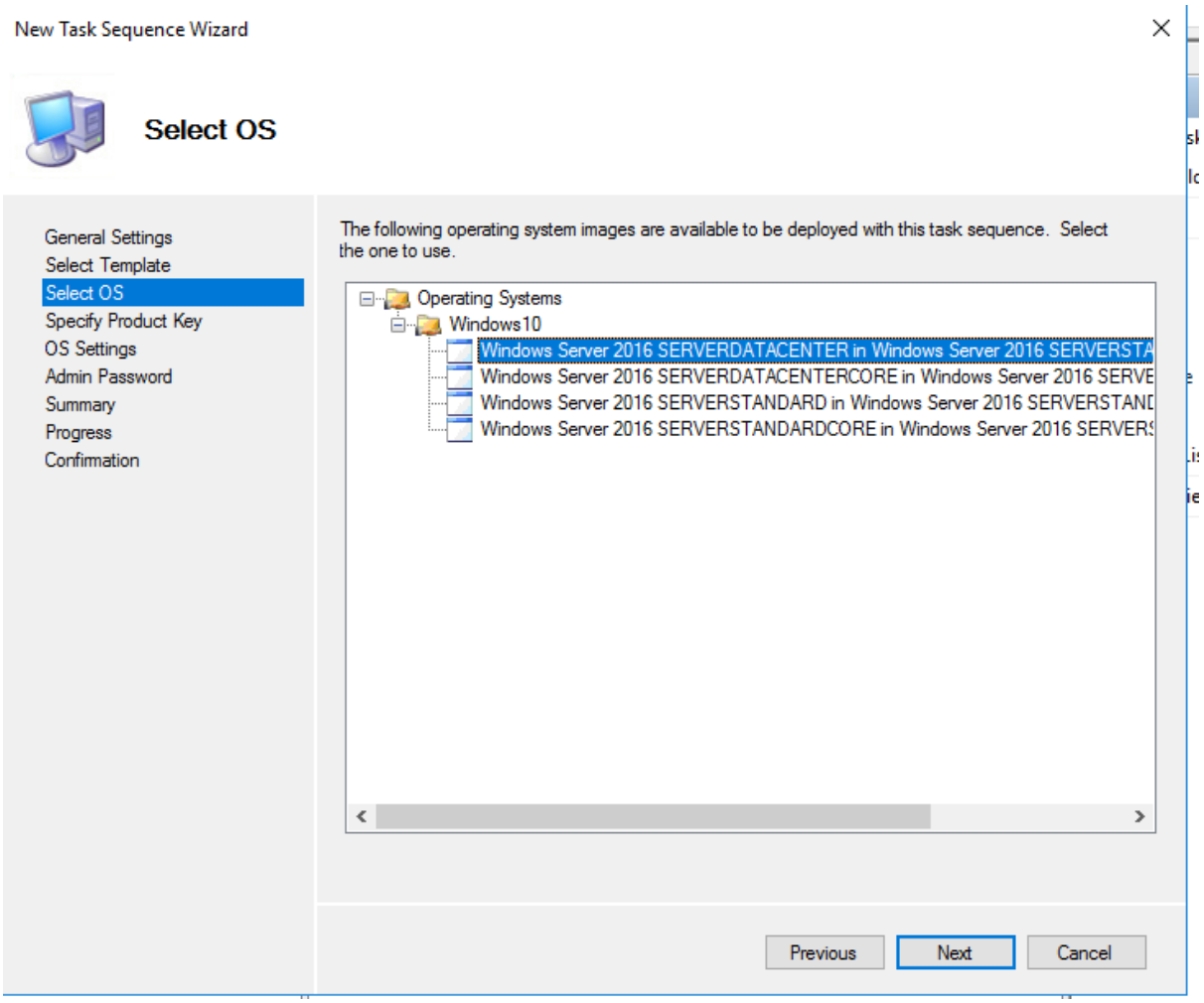
Type the required details:



Select the template as, “Standard Client Task Sequence”

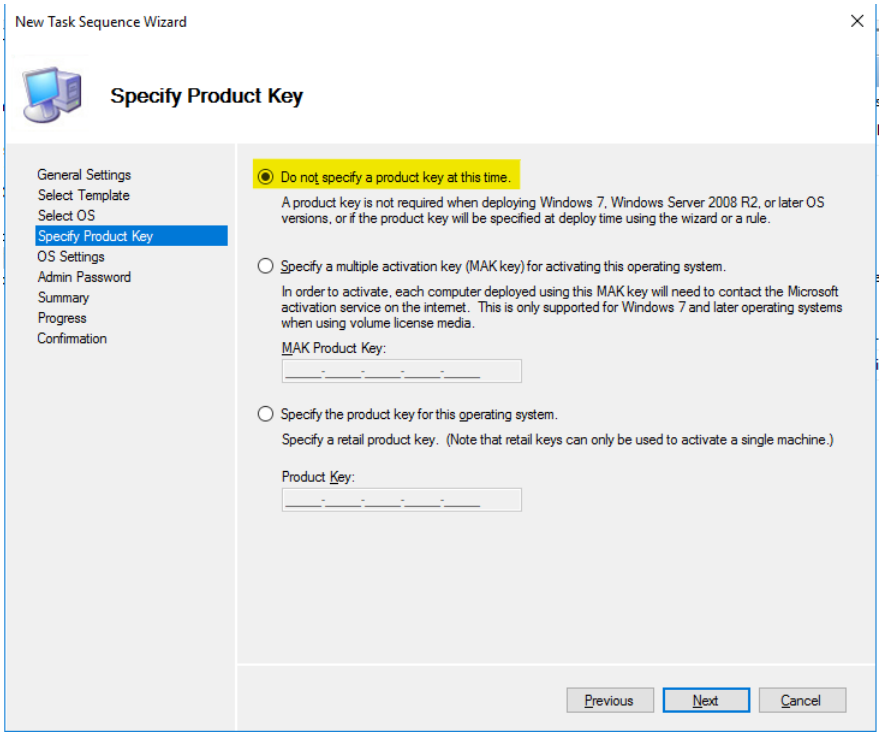


Select OS

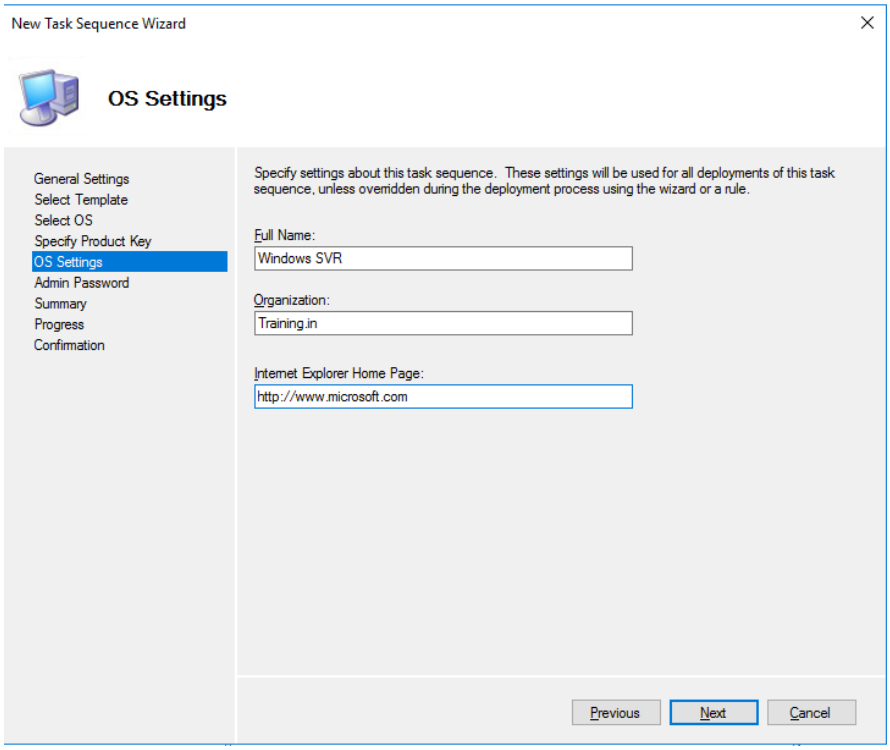


Windows 10 ISO had some issue; I have imported Windows server 2016 ISO file.

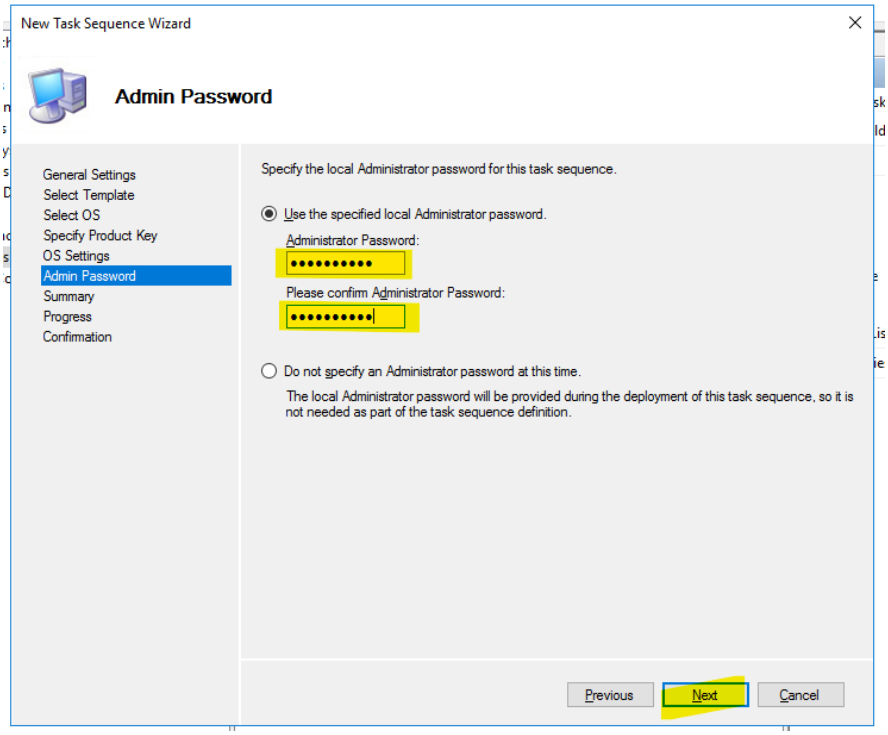
In specify product key, use “do not specify a product key at this time.”



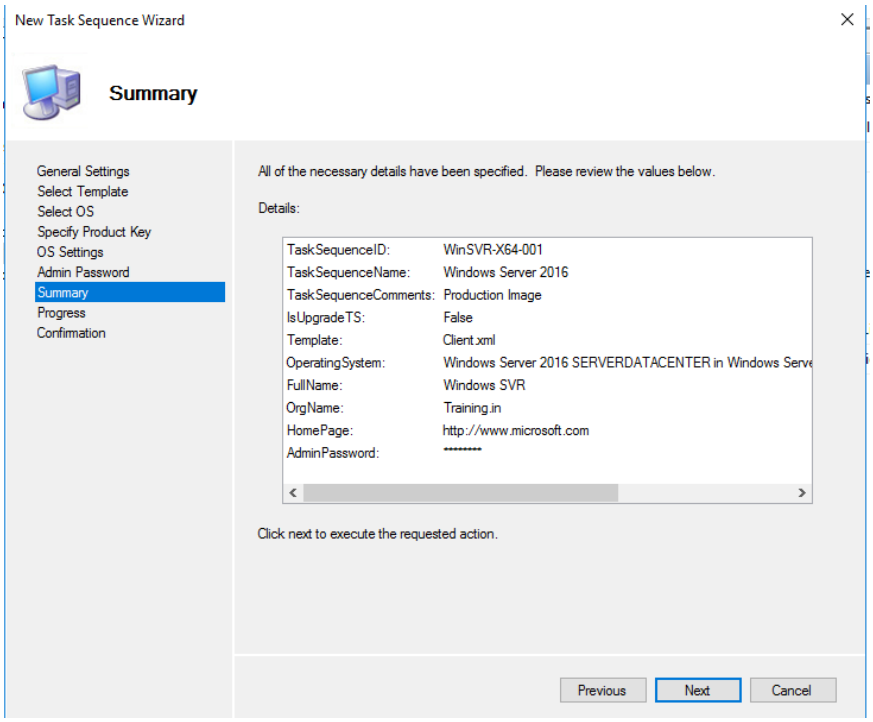
Fill the following values:



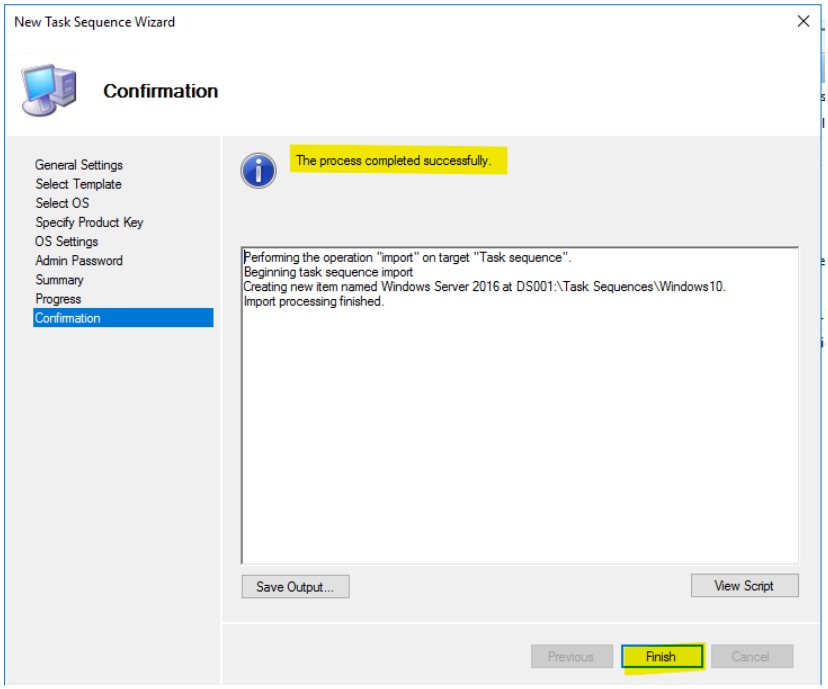
Specify admin password (optional)



Click Next:



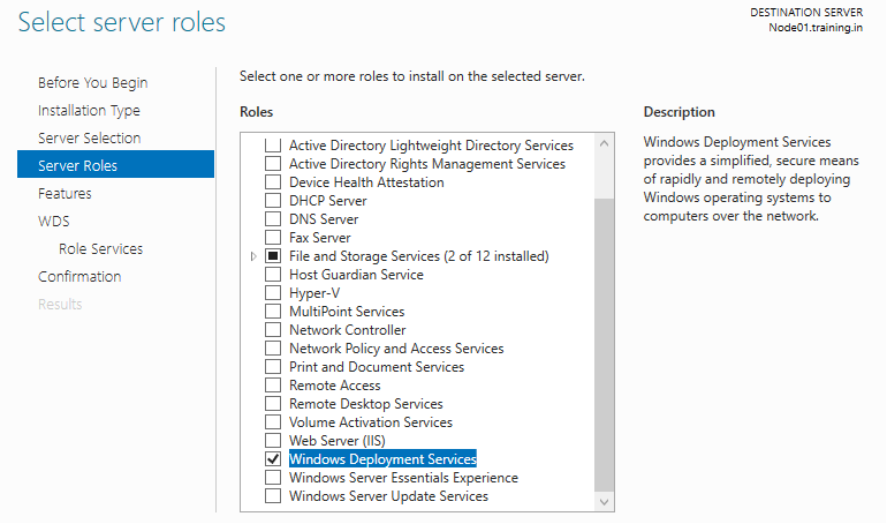
Verify after task completion.



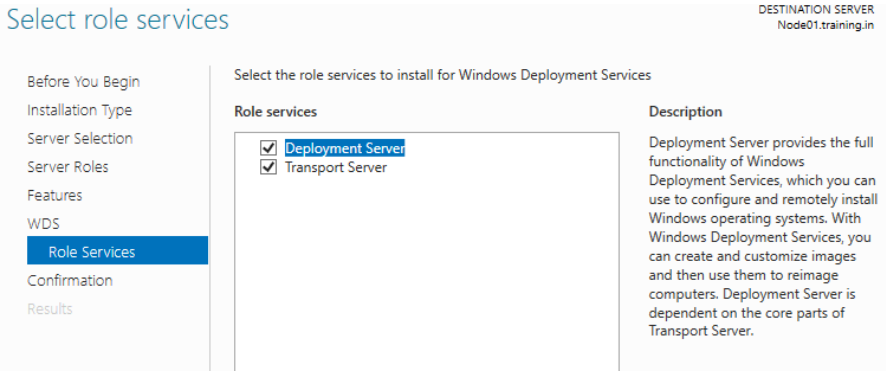
Deploy the Windows 10 client image

Installing WDS on Node01

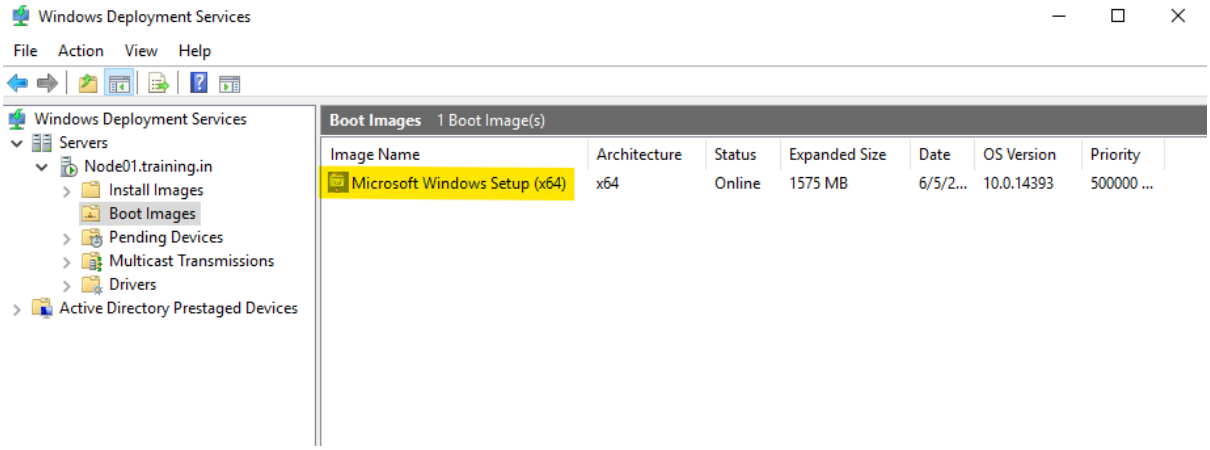
Node01 → Dashboard → Tools → Install Roles and Features → Role → Windows Deployment Service (WDS)



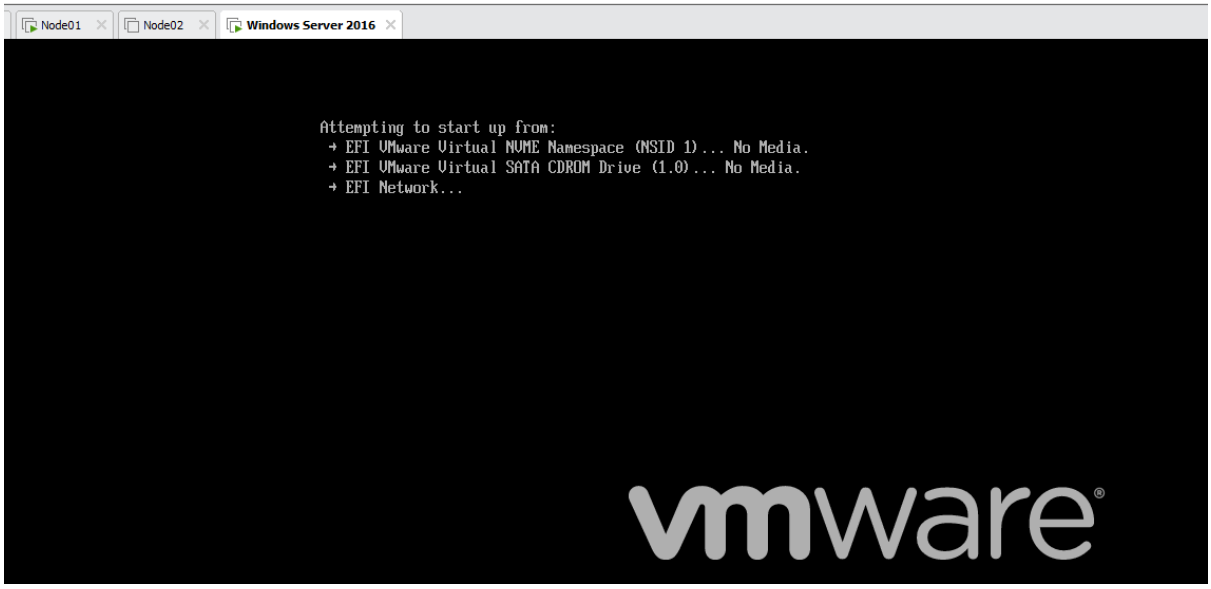
Install both role service



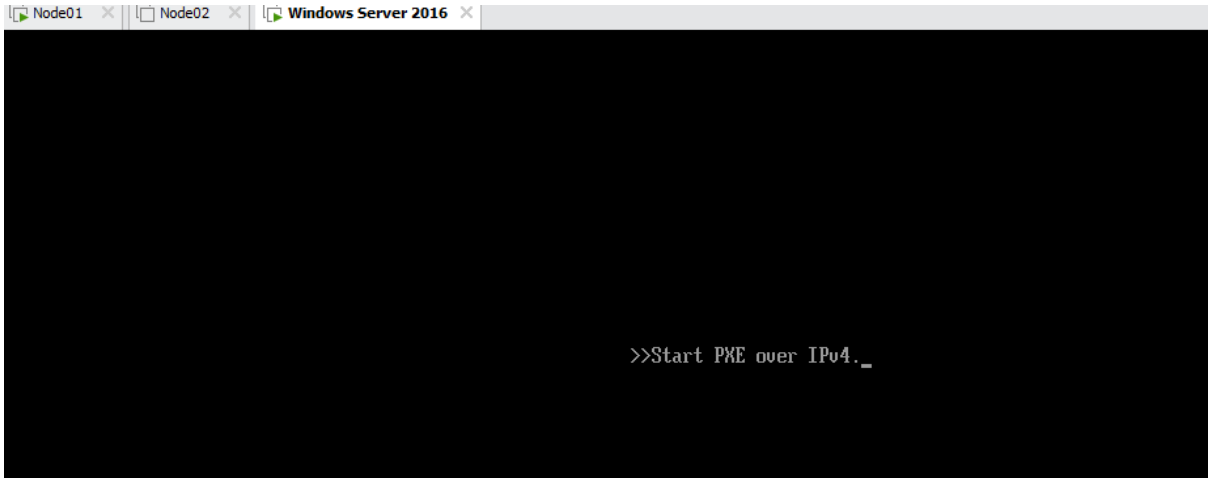
Click “Install”, after this. Post installation, configure WDS with newly setup image (boot.wim)



Create a new VM in VMWare workstation and power on the VM



Select Network



Note – That's all for MDT

Event Viewer

What is Event Viewer?

Event Viewer is a built-in Windows tool that allows administrators and users to view and analyze event logs generated by the operating system, applications, and system services.

Core Purpose of Event Viewer

- Troubleshoot system and application errors
- Monitor security-related activities (logins, logoffs, account lockouts)
- Track service and driver failures
- Audit system access and configuration changes
- Diagnose boot and shutdown issues

Types of Logs in Event Viewer

Log Type	Description
Application	Events from software programs (e.g., MS Office, antivirus)
System	OS-level events (e.g., driver failure, hardware error)
Security	Audit logs like login/logout attempts, account management
Setup	Logs related to system setup and installation (e.g., Windows Updates)
Forwarded Events	Logs forwarded from other computers (via Event Subscriptions)

Applications and Services Logs

More detailed logs for specific services and apps, e.g.:

- Microsoft → Windows → GroupPolicy
- Microsoft → Windows → DNS Server
- Microsoft → Windows → PowerShell

Event Levels

Level	Meaning
Information	Successful operations (e.g., service started)
Warning	Potential problems (e.g., low disk space)
Error	Failed operations (e.g., driver failure)
Critical	Serious errors (e.g., system crash)

Level	Meaning
Verbose	Detailed information (for debugging)
Audit Success/Failure	Security-related logs (e.g., login succeeded/failed)

Key Components of an Event Entry

Field	Description
Event ID	Unique identifier for each type of event (e.g., 4625 = failed login)
Source	Origin of the event (e.g., Security, DNS, GroupPolicy)
Date/Time	When the event occurred
User	Account involved in the event
Computer	Hostname where the event occurred
Description	Human-readable explanation of the event
Level	Severity level (Info, Error, Warning, etc.)

Important Security Event IDs

Event ID	Description
4624	Successful user login
4625	Failed login attempt
4634	Logoff
4672	Special privileges assigned to new logon
4648	Logon with explicit credentials
4720	New user account created
4726	User account deleted
4740	Account locked out
4768	Kerberos authentication ticket requested
1102	Audit log cleared

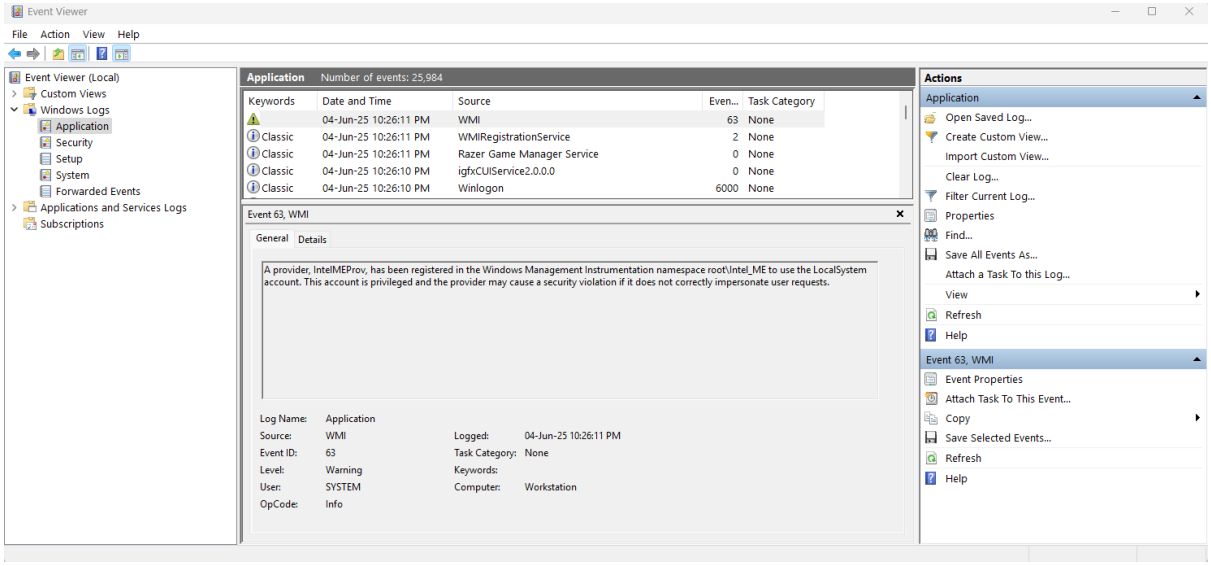
How to Open Event Viewer

GUI Method:

1. Press Win + R
2. Type eventvwr.msc and hit **Enter**

Other Ways:

- Start Menu → Search “Event Viewer”
- Control Panel → Administrative Tools → Event Viewer



Advanced Features

- Event Subscriptions
  - Allows you to collect logs from multiple remote computers into one central server using Windows Remote Management (WinRM).
- Scheduled Tasks Triggered by Events
  - You can attach a task to a specific event using Task Scheduler.
- Security Auditing
  - Can be used to detect:
    - Unauthorized access attempts
    - Account lockouts
    - Changes to group memberships
    - File access (if object auditing is enabled)

PowerShell

What is PowerShell?

PowerShell is a task automation and configuration management framework developed by Microsoft. It consists of:

- A command-line shell
- A scripting language
- A configuration management platform

PowerShell is designed to automate administrative tasks on Windows, Linux, and macOS systems.

Core Components of PowerShell

Component	Description
Shell	Interactive command-line interface for executing commands
Cmdlets	Built-in PowerShell commands (e.g., Get-Process, Set-Service)
Scripting Language	Allows creation of complex scripts and logic
Modules	Packages of related cmdlets and functions
Pipelines	Pass data from one cmdlet to another using `
Providers	Access data stores like file systems, registry, and certificate stores as if they were file systems
Remoting	Execute PowerShell commands on remote computers
Objects	PowerShell outputs structured .NET objects, not plain text

History and Versions

Version	Highlights
PowerShell 1.0 (2006)	Initial release with Windows Server 2008
PowerShell 2.0 (2009)	Remoting, modules, background jobs
PowerShell 3.0/4.0	Enhanced automation, workflows
PowerShell 5.1 (2016)	Last Windows-only version, DSC improvements
PowerShell 7+	Cross-platform (Windows, Linux, macOS), open-source (pwsh)

Common Cmdlets

Category	Cmdlets
Files & Folders	Get-ChildItem, Copy-Item, Remove-Item
Services	Get-Service, Start-Service, Stop-Service
Processes	Get-Process, Stop-Process
System Info	Get-ComputerInfo, Get-WmiObject
Networking	Test-Connection, Get-NetIPAddress, Get-NetAdapter
Users & Groups	Get-LocalUser, New-LocalUser, Add-LocalGroupMember
Event Logs	Get-EventLog, Get-WinEvent
Software	Get-Package, Install-Package, Uninstall-Package

PowerShell Security Features

Feature	Description
Execution Policy	Controls script execution (Restricted, RemoteSigned, Unrestricted, etc.)
Code Signing	Ensures scripts are trusted
Just Enough Administration (JEA)	Role-based delegation of administrative tasks
Transcript Logging	Logs PowerShell activity
ScriptBlock Logging	Captures dynamic code execution

PowerShell in Automation

- Scheduled Tasks
- Windows Deployment Toolkit
- Group Policy Scripts
- Server Provisioning
- Backup Scripts
- SCCM, Intune integration

Domain Name System (DNS)

What is DNS?

DNS (Domain Name System) is the system that translates human-friendly domain names (like www.google.com) into IP addresses (like 100.200.10.102) that computers use to identify each other on networks.

Why DNS is Important

- Converts domain names to IP addresses
- Enables website browsing using URLs instead of IPs
- Supports Active Directory operations (essential for domain controllers)
- Used in email routing, file sharing, cloud services, and more

Key DNS Terminologies

Term	Description
Domain Name	Human-readable name like example.com
IP Address	Numerical address of a server, e.g., 192.168.1.1
DNS Server	System that holds DNS records and responds to queries
Zone	Portion of the DNS namespace managed by a server
Record	Entry in a DNS database (e.g., A, MX, CNAME, etc.)
Resolver	Client component that queries the DNS server
Forwarder	DNS server that forwards queries it can't resolve locally

Types of DNS Records

Record Type	Purpose
A (Address)	Maps a domain to an IPv4 address
AAAA	Maps a domain to an IPv6 address
CNAME (Canonical Name)	Alias of another domain name
MX (Mail Exchanger)	Specifies mail server for a domain
NS (Name Server)	Specifies authoritative DNS servers for a domain
PTR (Pointer)	Used for reverse DNS lookups (IP → Domain)
SOA (Start of Authority)	Defines the authoritative DNS zone

DNS Resolution Process

1. User types www.example.com in browser.
2. OS checks local hosts file or DNS cache.
3. If not found, it queries the configured DNS server (usually from DHCP).
4. If the DNS server can't resolve:
    - It forwards the query (if a forwarder is set), OR
    - It performs an iterative query to the root DNS servers, then TLD servers, then authoritative servers.
5. IP address is returned and used to connect.

DNS in Windows Server

DNS is built into Windows Server and integrated with Active Directory. When you install AD DS (Active Directory Domain Services), DNS is often installed alongside.

Key Features in Windows DNS Server:

- Forward Lookup Zones
- Reverse Lookup Zones
- Conditional Forwarding
- Zone Transfers
- DNS Scavenging (Stale Record Cleanup)
- DNSSEC (Security Extensions)
- Integration with Active Directory

Types of DNS Zones

Zone Type	Description
Primary Zone	Holds the master copy of DNS records
Secondary Zone	Read-only copy of the primary zone (used for redundancy)
Stub Zone	Contains only necessary info (NS records) to reach authoritative DNS servers
Reverse Lookup Zone	Maps IP addresses to hostnames
AD-integrated Zone	Stored in AD, allows multimaster updates and replication

DNS Forwarding & Conditional Forwarders

- Forwarders: DNS server forwards all unresolved queries to another server (like ISP DNS or Google DNS).
- Conditional Forwarders: Forward queries for specific domains to specific DNS servers (e.g., for cross-forest or hybrid cloud setups).

DNS Security Features

Feature	Description
DNSSEC	Validates DNS responses to prevent spoofing
Secure Dynamic Updates	Only authenticated computers can update DNS
Access Control Lists (ACLs)	Control who can read/write to the DNS records
Scavenging	Removes stale records automatically

DNS Security Features

Feature	Description
DNSSEC	Validates DNS responses to prevent spoofing
Secure Dynamic Updates	Only authenticated computers can update DNS
Access Control Lists (ACLs)	Control who can read/write to the DNS records
Scavenging	Removes stale records automatically

Troubleshooting DNS

Tool/Command	Usage
nslookup	Query DNS records
ipconfig /displaydns	Show DNS cache
Resolve-DnsName	Advanced PowerShell DNS query
Test-Connection	Ping host
dcdiag /test:dns	Diagnose domain controller DNS setup
Get-DnsServerResourceRecord	View records using PowerShell

Active Directory Domain Services (ADDS) Replication

AD DS Replication is the process by which the directory data stored on one Domain Controller (DC) is synchronized with other DCs in the same Active Directory Forest. This ensures that all domain controllers have consistent, up-to-date information about users, computers, policies, and other AD objects.

Replication allows AD to be distributed, fault-tolerant, and scalable, so users can authenticate and access resources even if one DC fails.

Key Concepts of AD DS Replication

1. Multi-Master Replication Model

- Every DC is a peer; changes can be made on any DC.
- When a change occurs on one DC, it replicates to others.
- This differs from a single-master model (like some databases) where only one server accepts writes.

2. Replication Scope

- AD replication occurs within sites and between sites.
- Intrasite replication: Frequent, fast, low latency replication within a site (usually LAN).
- Intersite replication: Less frequent, compressed, scheduled replication between sites (usually WAN).

3. Partitions (Naming Contexts)

- AD data is divided into partitions:
    - Domain partition: Contains user, computer, group info.
    - Configuration partition: Contains topology and service info.
    - Schema partition: Contains definitions of object classes and attributes.
    - Application partitions: Custom partitions for specific apps.
- Each partition replicates only to DCs that need it.

How AD DS Replication Works

Change Notification and Polling

- When a DC makes a change, it notifies partner DCs that it has updates.
- The notified DCs pull the changes via replication.
- If no notification is received, DCs will poll their partners at regular intervals.

Replication Topology

- Created by the Knowledge Consistency Checker (KCC), a built-in AD component.
- It automatically generates the replication links between DCs.
- Uses Connection Objects to define replication paths.

Replication Types

- Intrasite Replication: Uses the RPC over IP protocol.
- Intersite Replication: Uses the Remote Procedure Call (RPC) over IP or Simple Mail Transfer Protocol (SMTP) (SMTP is rarely used and only for configuration partition).

Update Sequence Number (USN) and Versioning

- Each change is assigned a USN.
- DCs use USNs and timestamps to track changes and avoid duplication.
- Conflicts are resolved using version numbers and timestamps.

Replication Schedule and Latency

- Intrasite: Replication happens almost immediately (within seconds).
- Intersite: Replication happens based on schedules to optimize bandwidth.
- Admins can configure schedules and costs for site links to control replication frequency.

Conflict Resolution

- In case of conflicting changes, AD uses a “last writer wins” approach based on timestamps.
- Deleted objects are handled via the tombstone mechanism and garbage collection.

Tools for Managing and Monitoring Replication

- repadmin.exe: Command-line tool to check replication status and troubleshoot.
- Active Directory Sites and Services: GUI tool to view and configure replication topology.
- Event Viewer: Logs replication events and errors.

Repadmin commands

Command	Description
repadmin /replsummary	Provides a summary of replication status for all domain controllers. Shows errors if any.
repadmin /showrepl <DCName>	Shows detailed inbound replication status on the specified domain controller.
repadmin /showrepl * /csv > repl.csv	Exports replication status of all DCs to a CSV file for analysis.
repadmin /syncall <DCName>	Forces synchronization of all replication partners for the specified DC.
repadmin /queue	Displays replication requests currently queued on a domain controller.
repadmin /showconn <DCName>	Lists inbound replication connections to the specified DC.
repadmin /showobjmeta <DCName> <ObjectDN>	Shows metadata for a specific object on a DC, including version and USN info.
repadmin /showchanges <DCName> <ObjectDN>	Displays changes for a specific object pending replication.
repadmin /bridgeheads	Lists all bridgehead servers in the forest (servers that replicate between sites).
repadmin /removelingeringobjects <DCName> <NC> <GUID> /advisory_mode	Detects and optionally removes lingering objects on a DC.
repadmin /kcc <DCName>	Forces the Knowledge Consistency Checker (KCC) to recalculate replication topology.
repadmin /failcache <DCName>	Shows replication failures cached on the specified DC.

Folder Redirection

Folder Redirection is a Group Policy feature in Windows that allows administrators to redirect the path of certain user profile folders (like Documents, Desktop, Pictures, etc.) from the local computer to a network location (usually a file server). This enables users to access their data from any domain-joined computer and helps centralize data storage and backup.

Why Use Folder Redirection?

- Centralized data management: User data is stored on servers, making backups and management easier.
- Roaming user experience: Users get the same data regardless of which computer they log on to.
- Reduced local disk usage: Saves space on client machines.
- Improved security: Data can be protected on centralized servers with controlled access.
- Offline availability: When configured with Offline Files, users can access redirected folders even offline.

Folders You Can Redirect

Common folders that can be redirected include:

- Desktop
- Documents (My Documents)
- Start Menu
- Pictures
- Music
- Videos
- AppData (Roaming)

How Folder Redirection Works

When a user logs on, the redirected folders are mapped from the local profile to the network share defined by the administrator via Group Policy. The system transparently redirects file access to the network location.

Requirements and Prerequisites

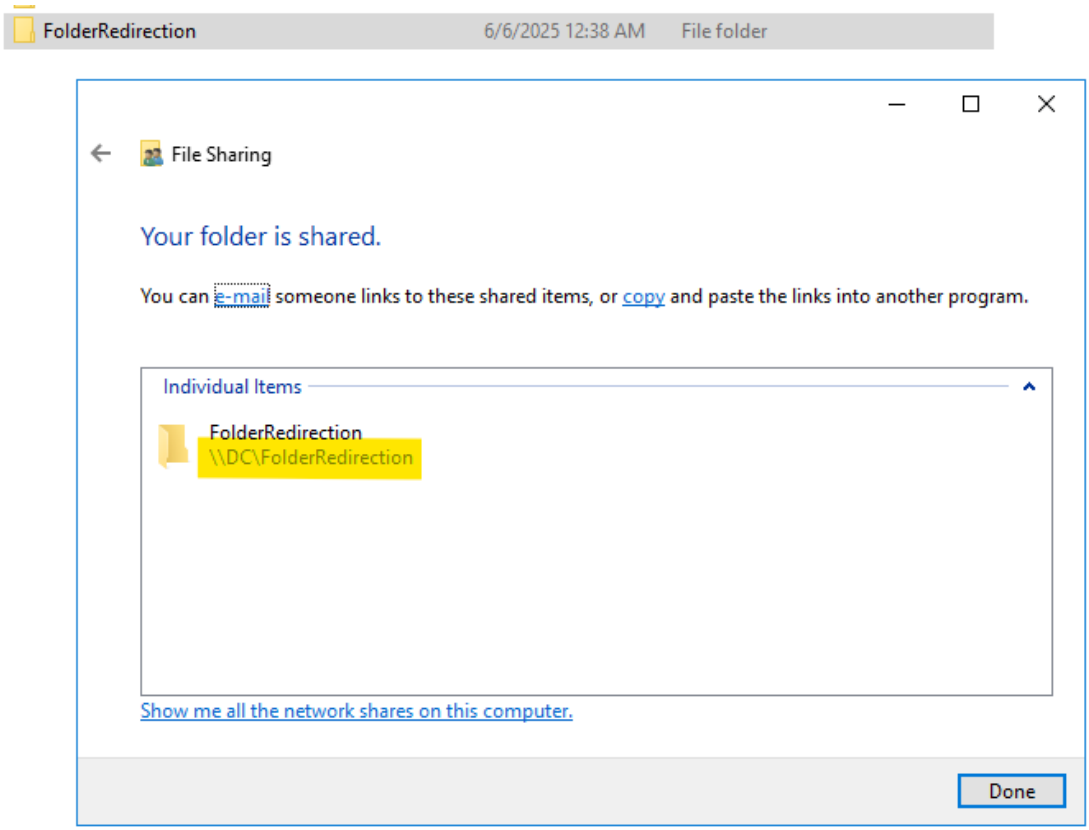
- **File Server with shared folders**: A network share where users' redirected folders will be stored.
- **Appropriate permissions** on the share and NTFS permissions to allow users to create and modify files.
- **Group Policy Management Console (GPMC)** to create and apply Folder Redirection policies.
- Clients must be **domain-joined** Windows machines.
- Network connectivity to the file server during logon.

Step-by-Step Folder Redirection Configuration

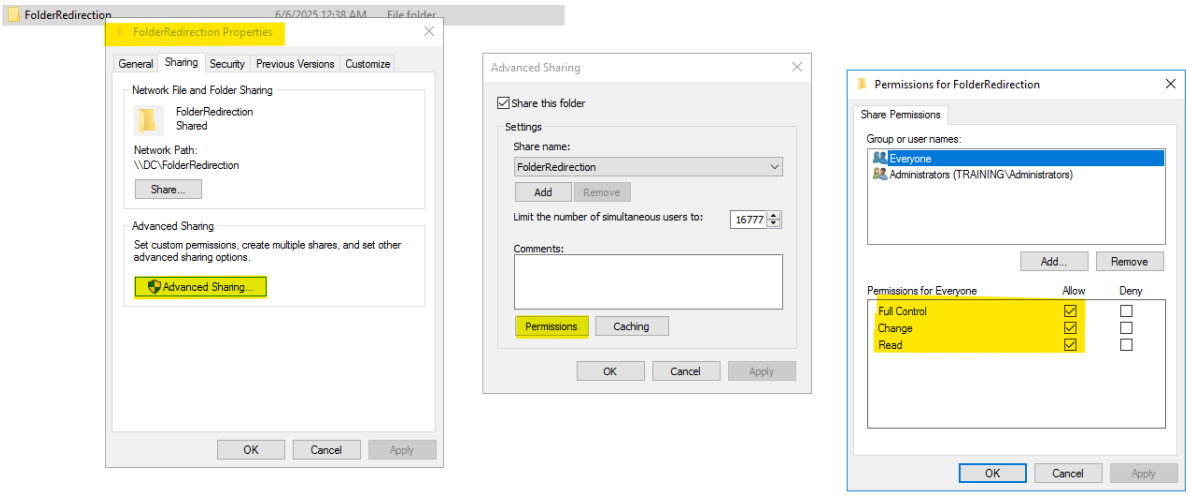
1. Create a Network Share

- On the file server, create a folder (e.g., \\FileServer\Users).
- Share the folder and set share permissions to allow **Full Control** for **Authenticated Users** or a security group containing users.
- Set NTFS permissions so each user has **Full Control** on their own folder (use the "Creator Owner" permission or configure permissions with user-specific folders).

Create an NFS folder with Read/Write access



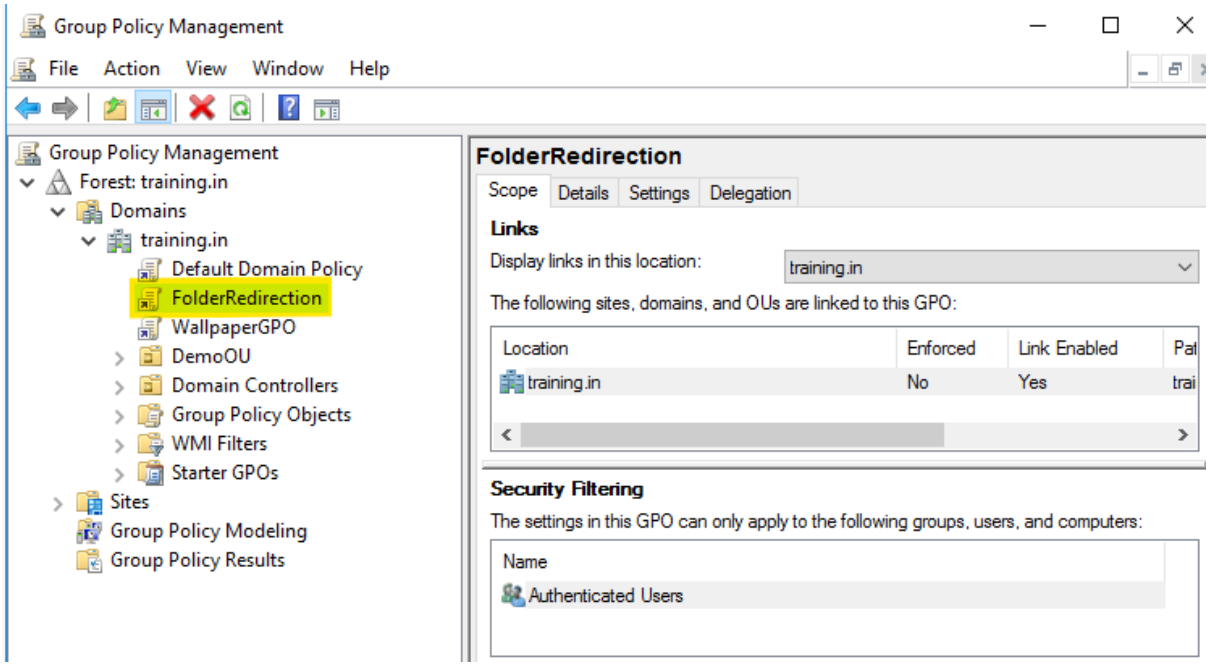
Verify, if full access is provided.



2. Open Group Policy Management Console (GPMC)

- On a domain controller, open gpmc.msc.

Create a new GPO “FolderRedirection”

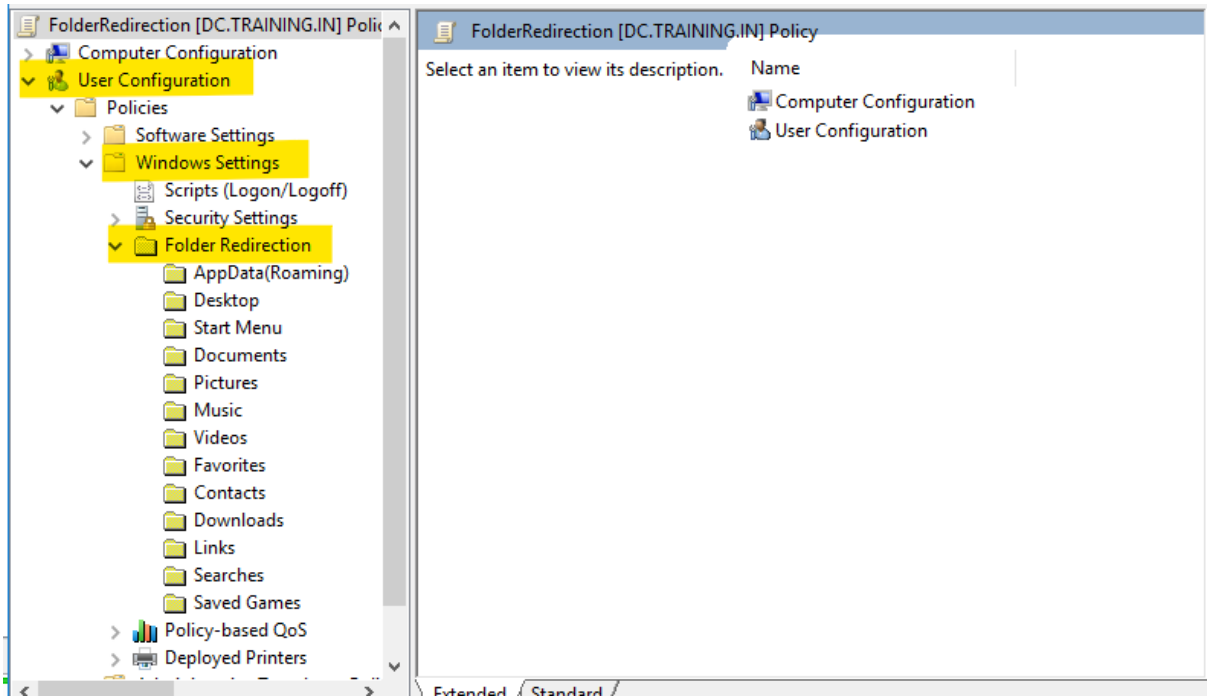


3. Create or Edit a GPO

- Create a new GPO or edit an existing one linked to the OU containing the user accounts.

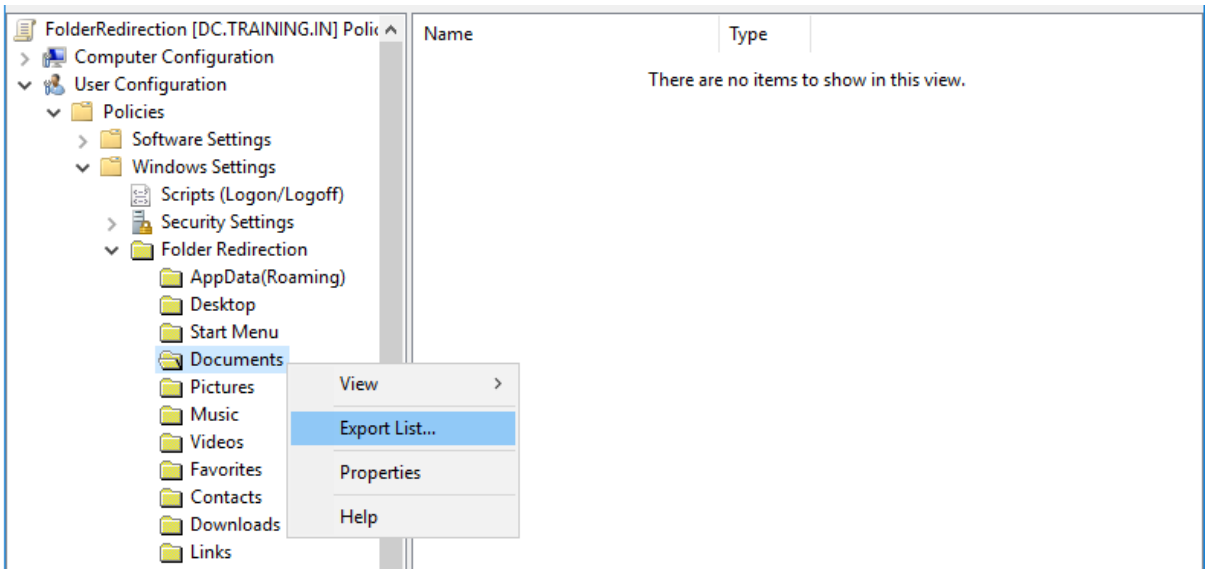
4. Navigate to Folder Redirection Policy

- Goto: User Configuration → Policies → Windows Settings → Folder Redirection

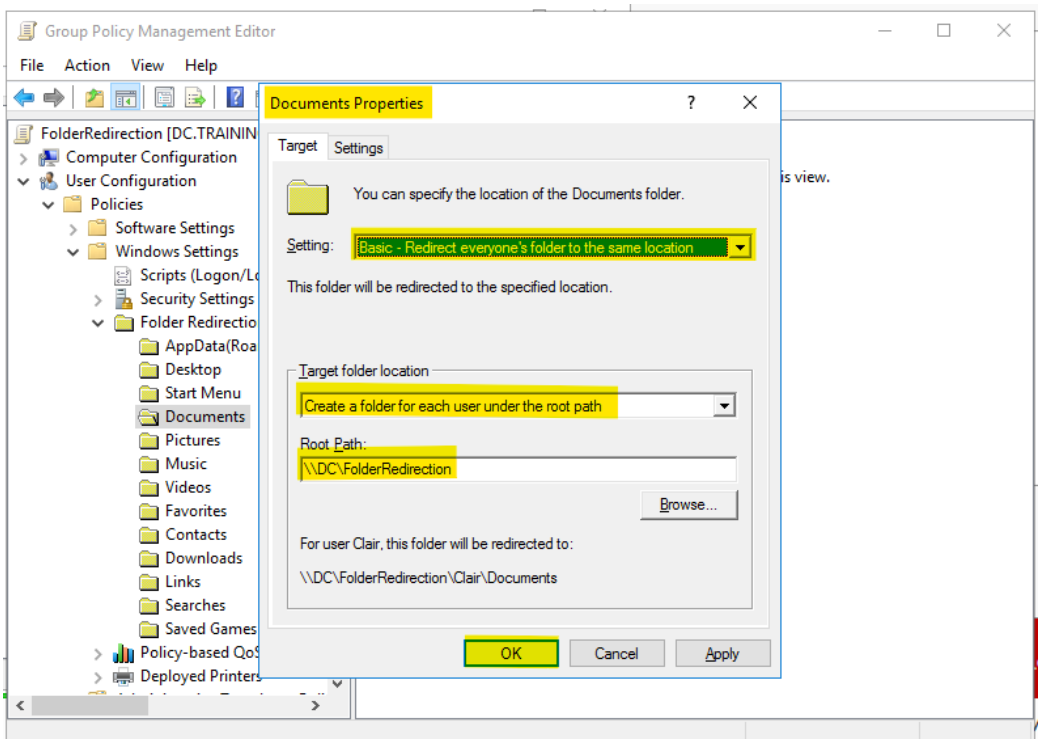


5. Configure Folder Redirection

- Right-click on the folder you want to redirect (e.g., **Documents**) and select **Properties**.

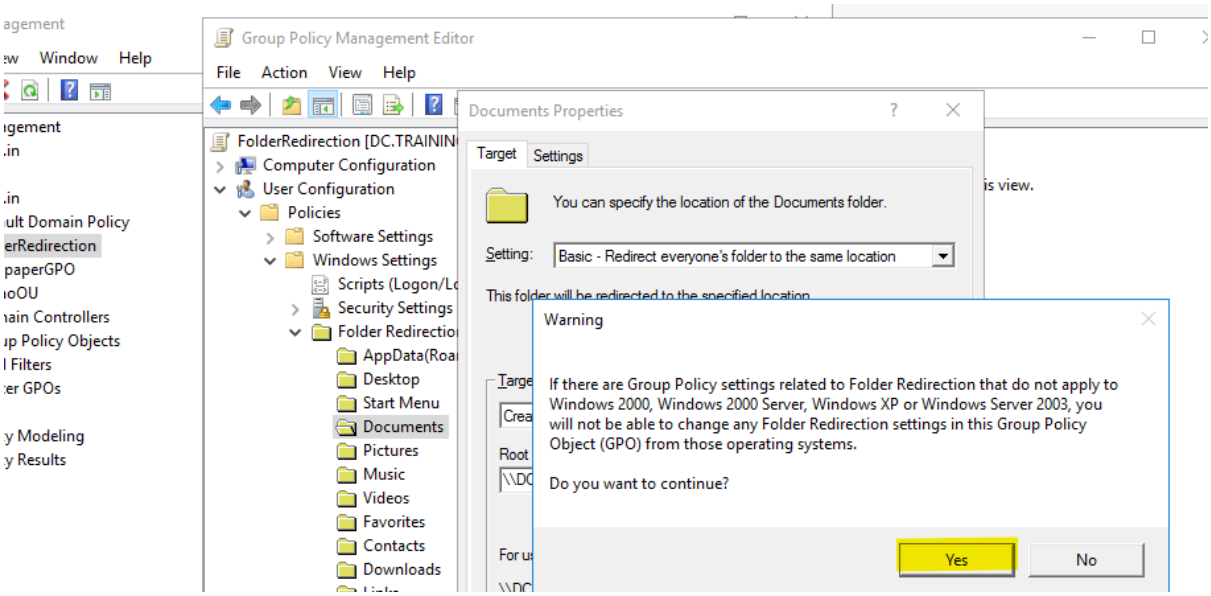


- In the **Target** tab, choose the redirection setting:
  - **Basic - Redirect everyone's folder to the same location** (common for most cases).
  - **Advanced - Specify locations for various user groups** (if different groups require different locations).
- Set the **Target folder location**:
  - **Create a folder for each user under the root path** (recommended). Example: \\FileServer\Users

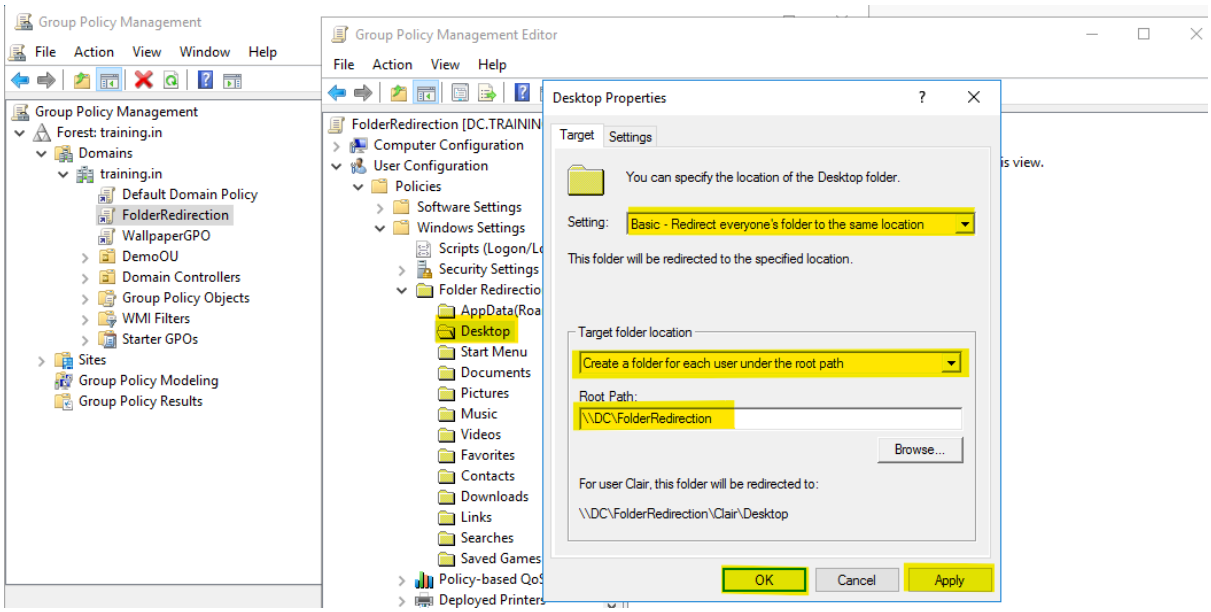


6. Apply and Close

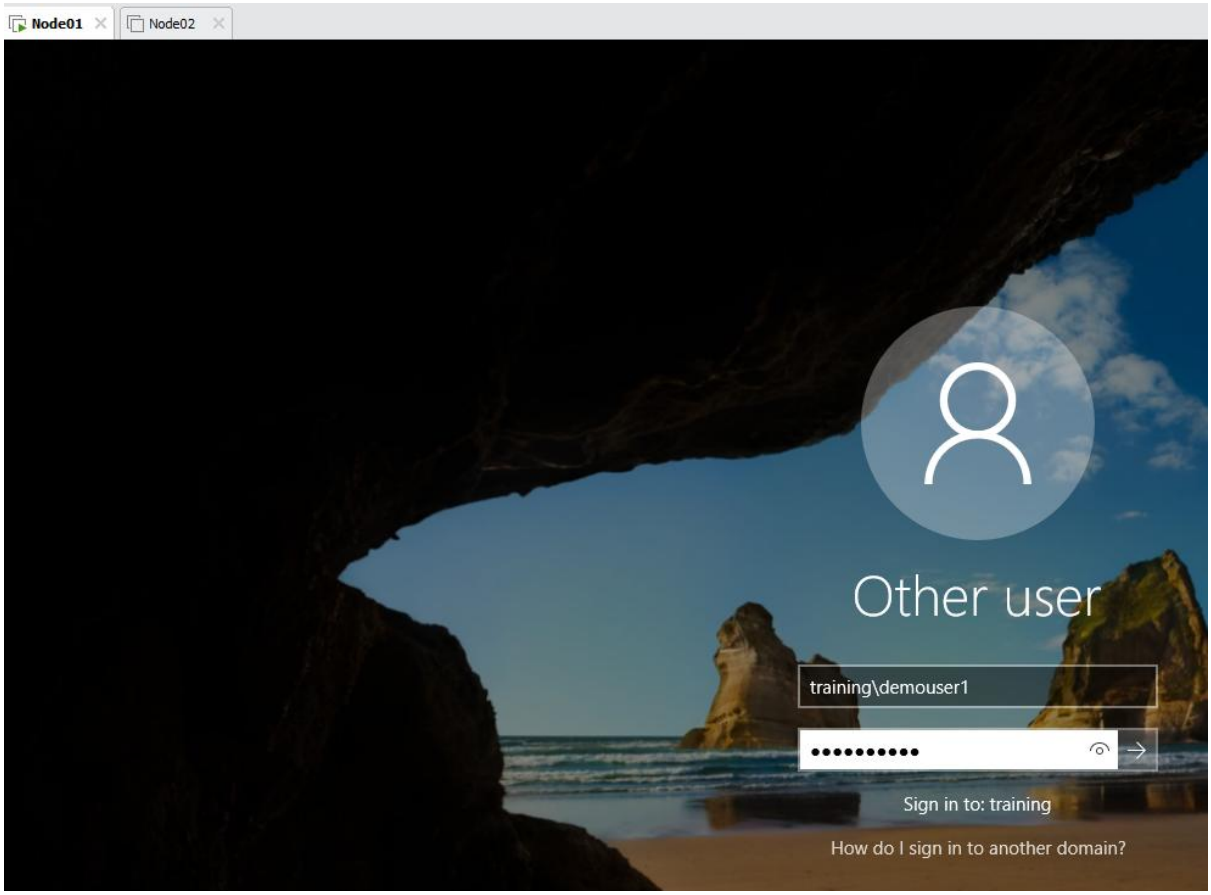
- Click **OK** to save the settings.
- Link the GPO to the appropriate OU containing user accounts if not already linked.

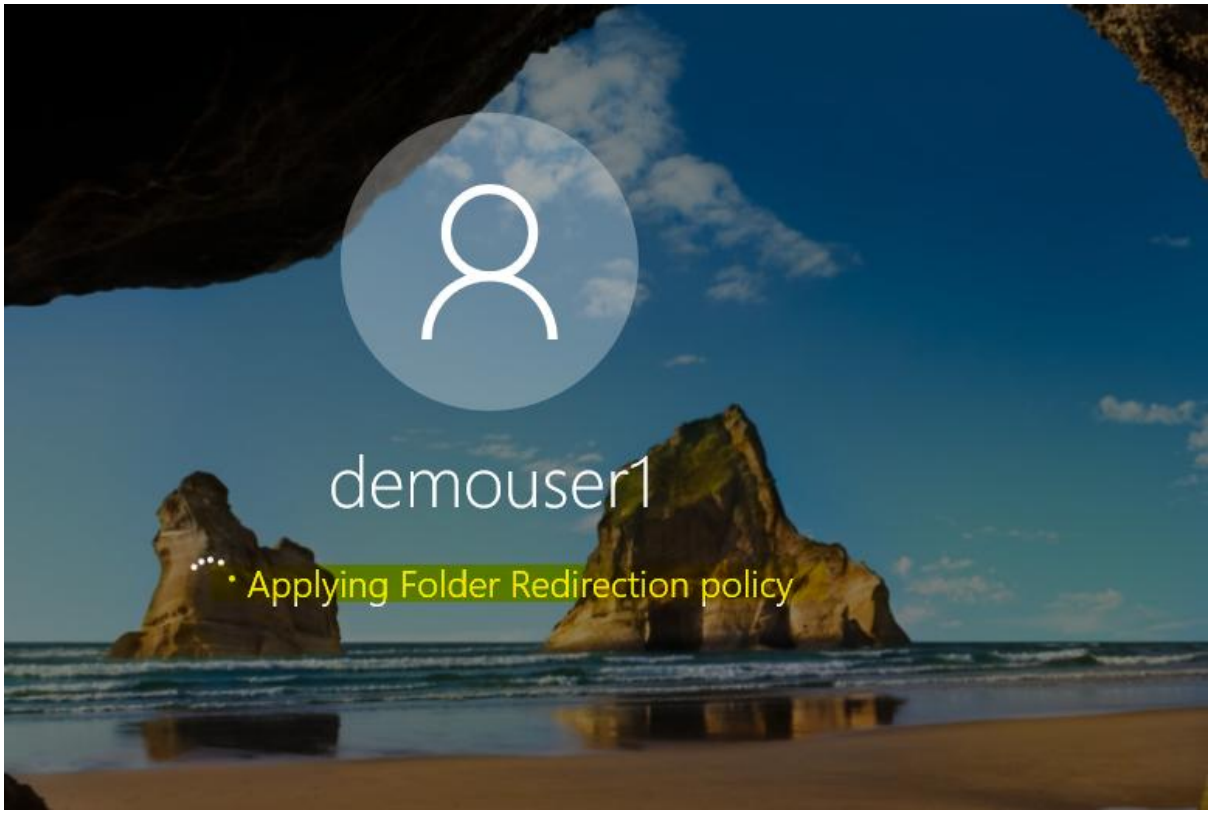


Applying same for Desktop:

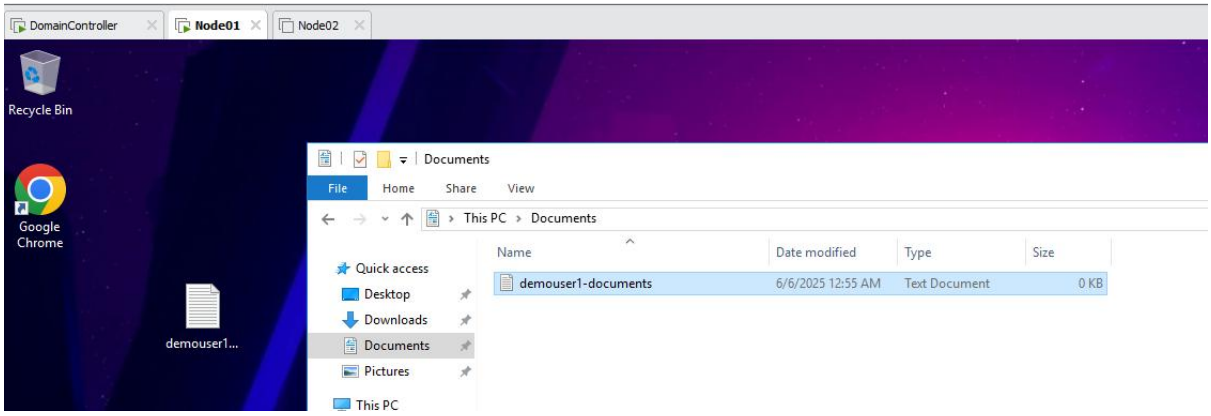


Login to Node01 as ‘demouser1’

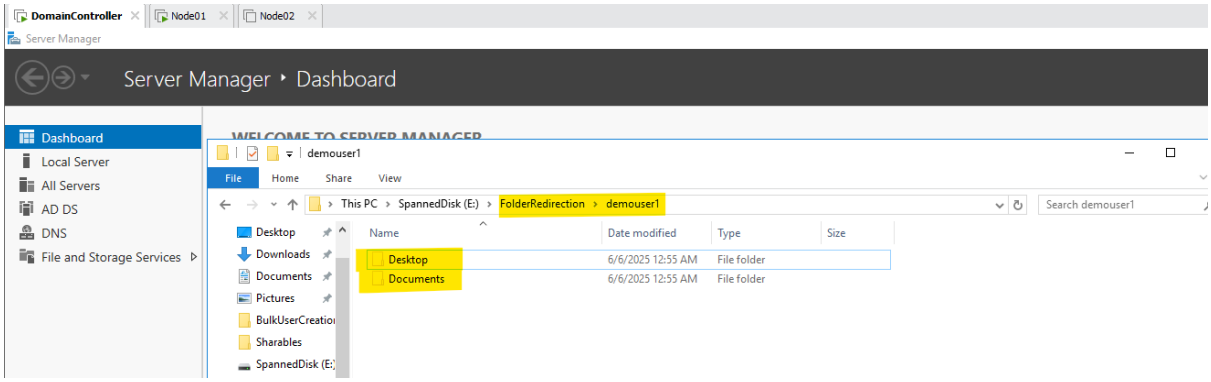




Create some file and folders on desktop and documents



Switch back to DC machine and verify the NFS location.



Note – That's all for Folder redirection

Active Directory Certificate Service (ADCS)

What is AD CS (Active Directory Certificate Services)?

Active Directory Certificate Services (AD CS) is a server role in Windows Server that allows organizations to build their own Public Key Infrastructure (PKI). It issues, manages, validates, and revokes digital certificates for users, devices, and services, thereby enabling secure communication, authentication, encryption, and digital signatures within an enterprise network.

Why Use AD CS?

- Secure email (S/MIME)
- SSL/TLS encryption for websites and internal services
- Smart card and VPN authentication
- Code and document signing
- Wireless network security (802.1X)
- Device certificates for IoT or domain-joined devices

Components of AD CS

Component	Description
Certification Authority (CA)	The server role that issues and manages certificates. It can be root or subordinate.
Certificate Templates	Define the rules and formats for certificates (validity period, key usage, etc.).
Online Responder (OCSP)	Responds to individual certificate status queries quickly (alternative to CRL).
Network Device Enrollment Service (NDES)	Allows network devices (routers, switches) to obtain certificates.
Certificate Enrollment Web Services	Web-based interface to enroll and renew certificates securely over HTTP/HTTPS.
CRL (Certificate Revocation List)	A list of revoked certificates no longer trusted.
OCSP (Online Certificate Status Protocol)	Real-time certificate revocation check.

AD CS Hierarchy Models

1. Single-tier PKI (Not Recommended for Production)

- One CA that acts as both Root CA and Issuing CA.
- Simple to deploy, but not secure, as the root must remain always online.

2. Two-tier PKI (Recommended for Enterprise Use)

- Offline Root CA: Secured and powered off after issuing certificates to Subordinate CAs.
- Online Issuing CA: Issues certificates to users, computers, and devices.

3. Three-tier PKI (Advanced Security)

- Rarely used; includes an intermediate CA layer between the root and issuing CA.

How AD CS Works – Certificate Lifecycle

1. Certificate Request: A client (user or computer) generates a key pair and submits a Certificate Signing Request (CSR).
2. Certificate Enrolment: Request goes to CA, validated against a template and policy.
3. Certificate Issuance: The CA signs the certificate and returns it to the requester.
4. Usage: The certificate is used for authentication, encryption, or signing.
5. Renewal: Before expiration, the certificate is renewed.
6. Revocation: If compromised or no longer needed, the certificate is revoked and added to the CRL.

Certificate Enrolment Methods

Method	**Description**
Manual enrollment	Admin or user manually requests and installs certificates.
Auto-enrollment	Certificates are automatically deployed via Group Policy.
Web enrollment	Certificates requested through a web interface (certsrv).
NDES/SCEP	Used by network devices and mobile phones for enrollment.
Enrollment Web Services	Secure certificate requests from non-domain-joined devices.

Managing AD CS

- Certification Authority Console (certsrv.msc): View issued, pending, revoked certificates.
- Certificate Templates (certtmpl.msc): Create/edit templates.
- Group Policy Management: Configure auto-enrollment policies.
- PKIView.msc: Monitor PKI health and availability.
- PowerShell (Get-Certificate, New-SelfSignedCertificate, etc.): Automate tasks.

Use Cases

Use Case	Certificate Issued To	Purpose
SSL/TLS	Web servers (IIS, Nginx, etc.)	Secure web traffic (HTTPS)
User Authentication	Domain users	Smart card or VPN logon
Email Security (S/MIME)	Email clients	Encrypt/sign emails
Code Signing	Developers or publishers	Ensure app authenticity
Wi-Fi Authentication	Devices/users	Secure wireless access (802.1X)

Security Best Practices

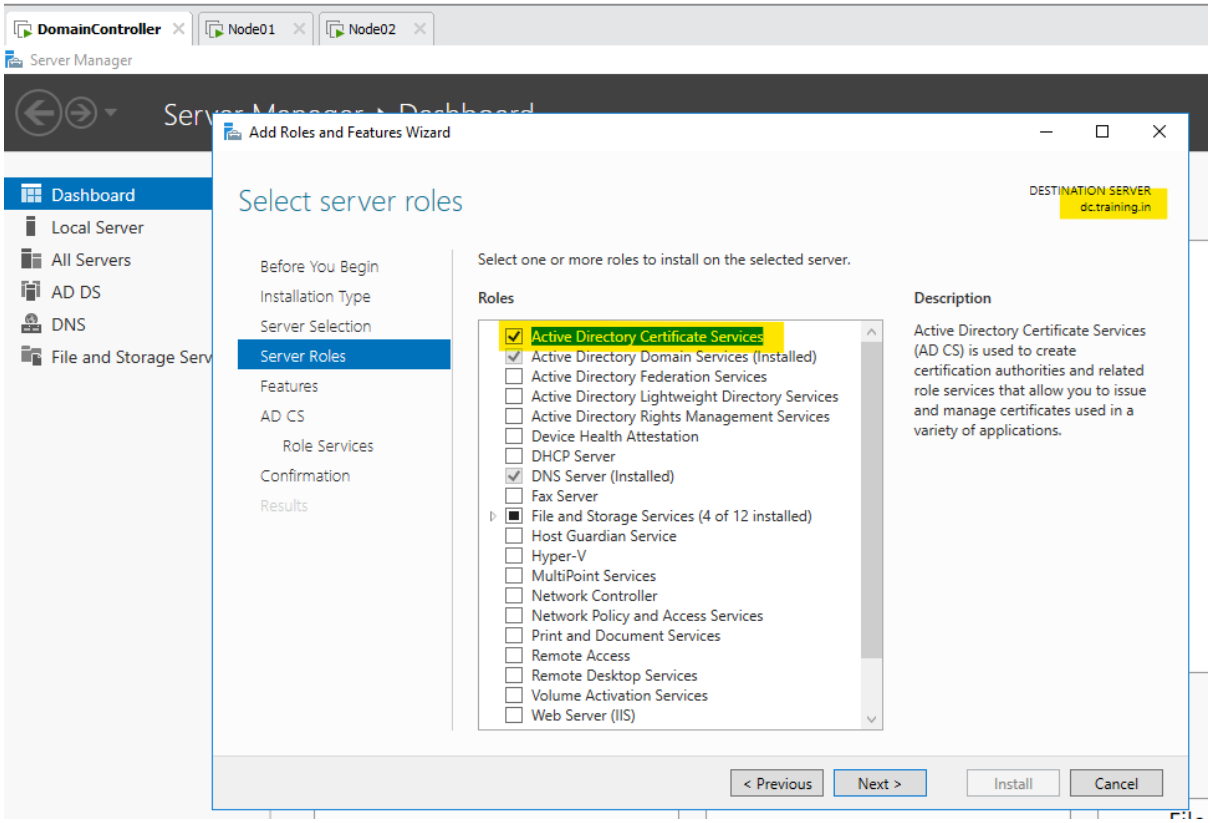
Area	Best Practice
Root CA	Keep offline, physically secured, and power on only when needed
Issuing CA	Secure and monitor; back up regularly
CRL and OCSP	Make CRLs highly available; use OCSP for real-time checking
Templates and Permissions	Limit who can request which types of certificates
Logging and Auditing	Enable auditing of certificate issuance and revocation

Installing and configuring AD CS (on DC)

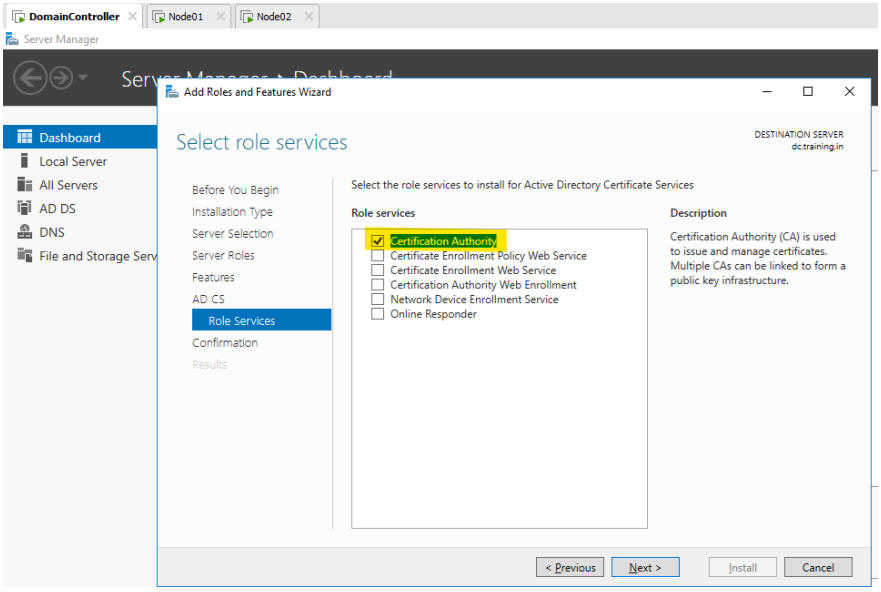
Step 1: Install the AD CS Role

Using Server Manager (GUI)

1. Open **Server Manager**.
2. Click **Manage > Add Roles and Features**.
3. Click **Next** on the Before You Begin page.
4. Select **Role-based or feature-based installation**, click **Next**.
5. Select your local server, click **Next**.
6. Under **Roles**, select **Active Directory Certificate Services**.
7. When prompted, click **Add Features**.
8. Click **Next** until you reach **Role Services**.

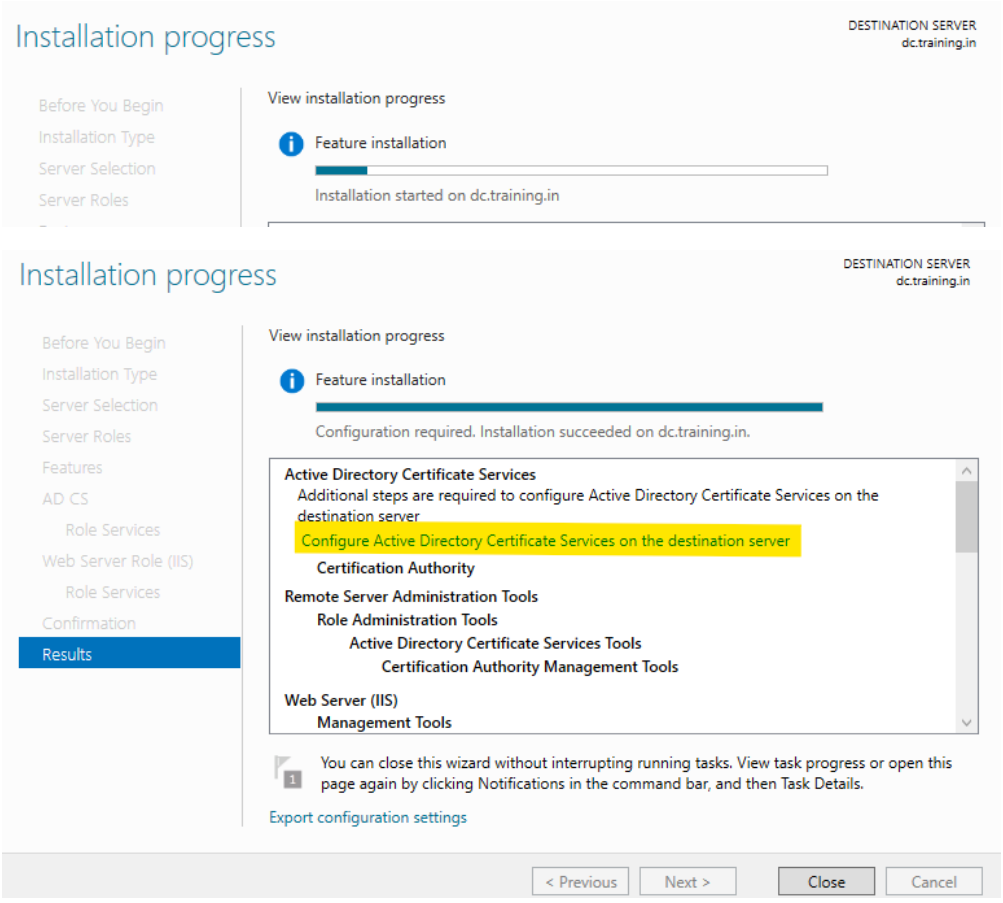


9. Select:
    - **Certification Authority**

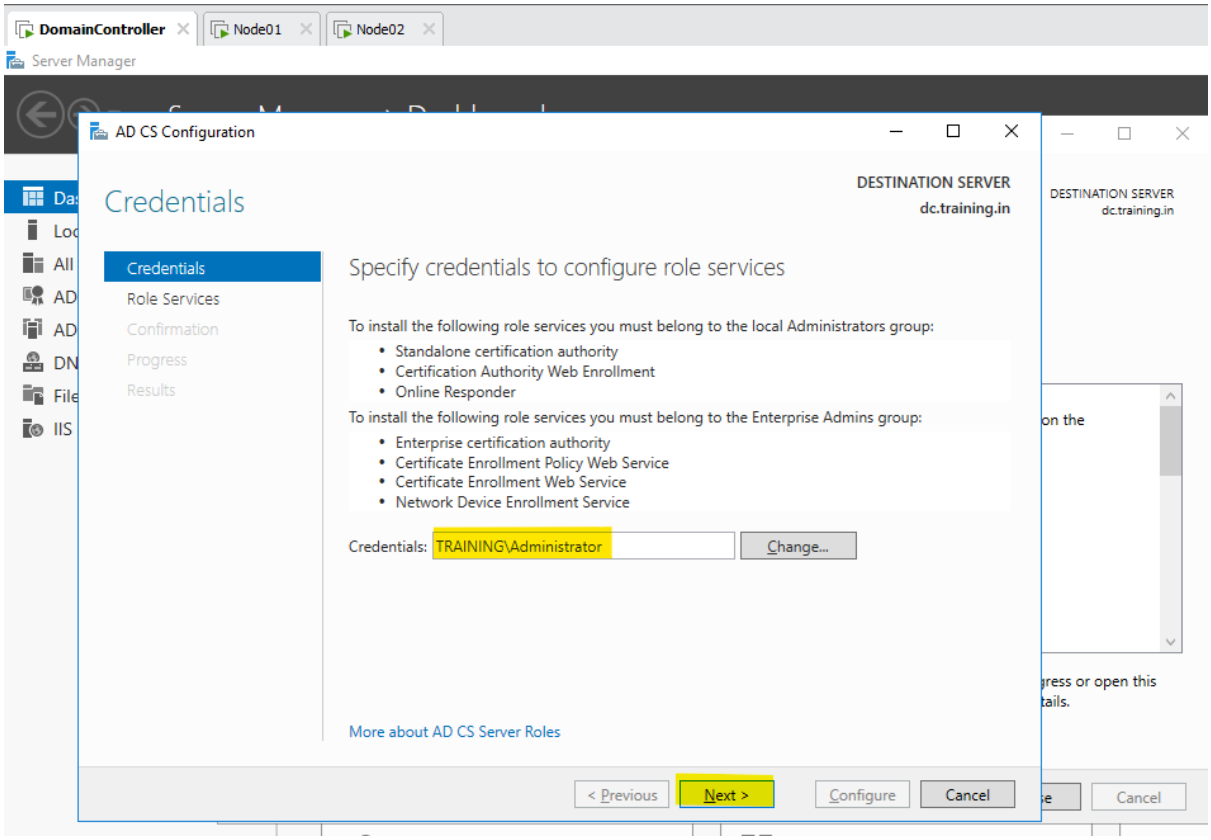


10. Click **Next**, then **Install**.

Wait for installation to finish, then click **Configure Active Directory Certificate Services on the destination server**.

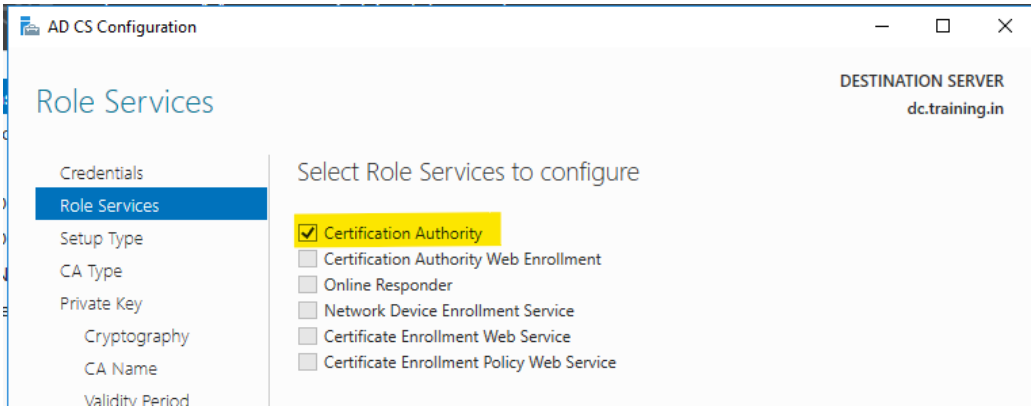


Step 2: Post-Installation Configuration



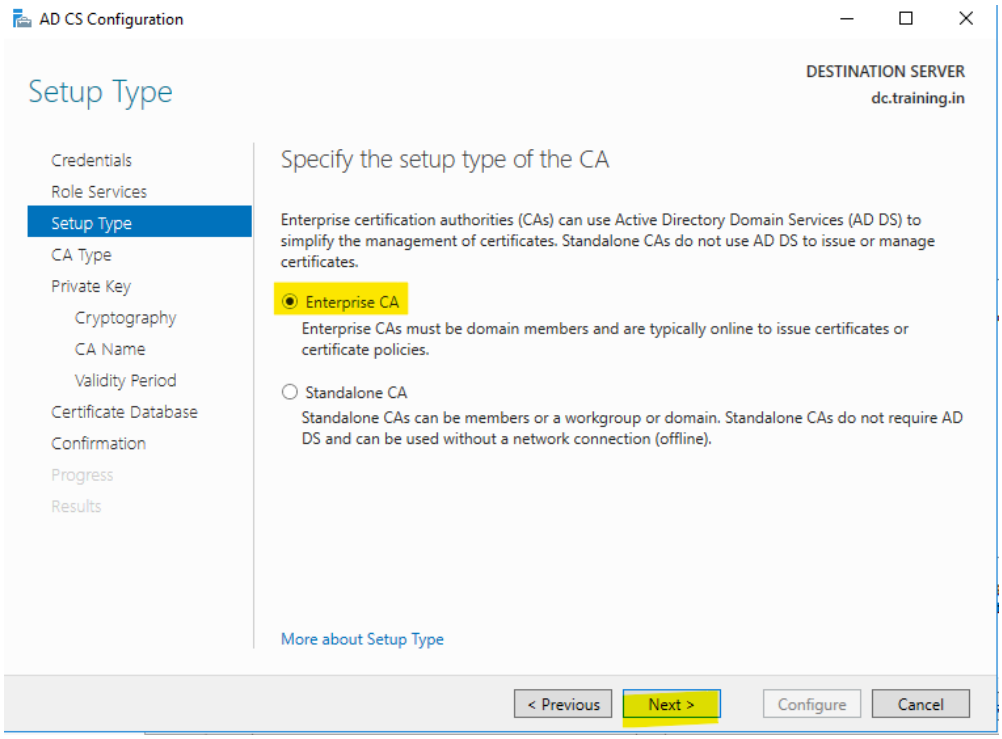
Using the AD CS Configuration Wizard

1. On the Role Services page, select:
    - Certification Authority



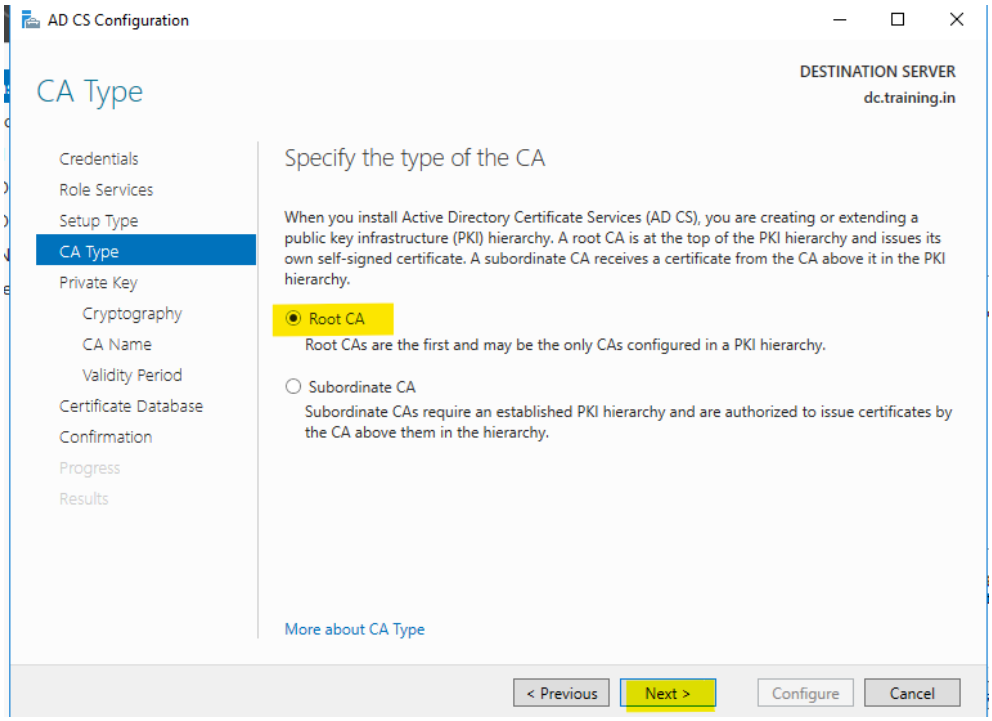
2. Click Next.

Select CA type:



Configure CA Type

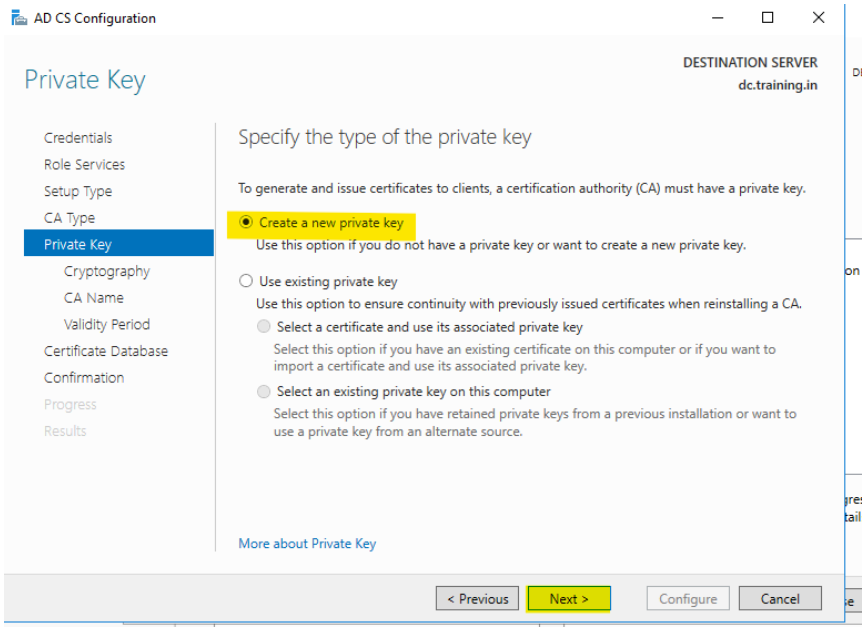
- Root CA: If this is the first CA in your PKI.
- Subordinate CA: If this CA will be signed by an existing Root CA (offline or external).

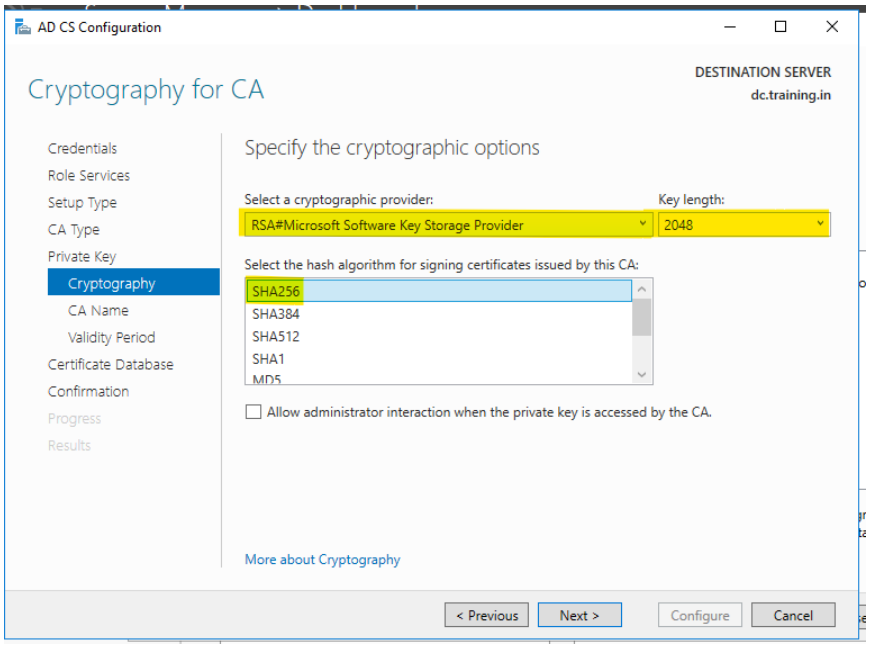


Note – In production, Root CA is offline, and Subordinate CA is online. For lab, Root CA can be online.

Configure Private Key

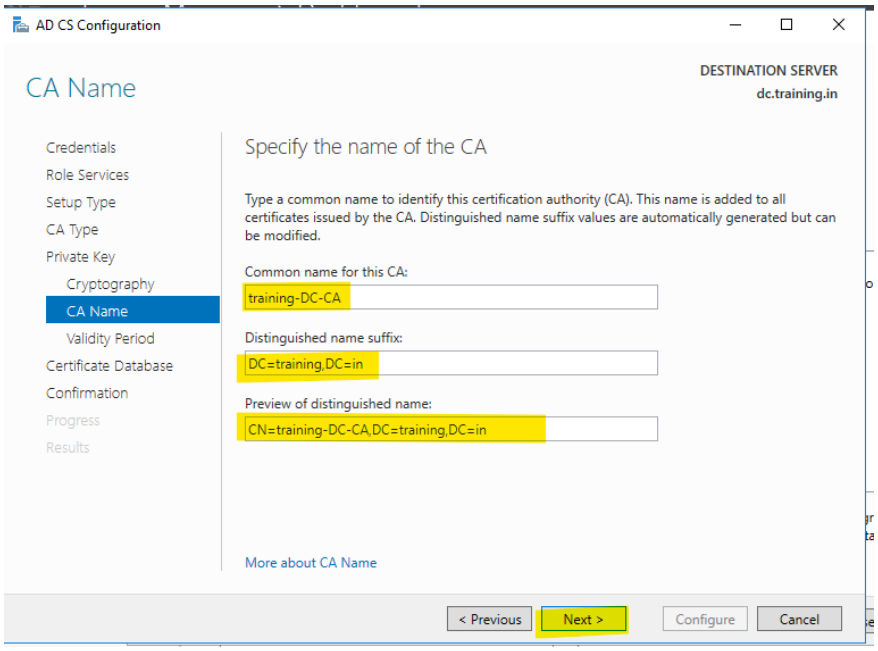
- Create a new private key (recommended for new installation)
- Key length: 2048 or 4096 bits
- Hash algorithm: SHA256





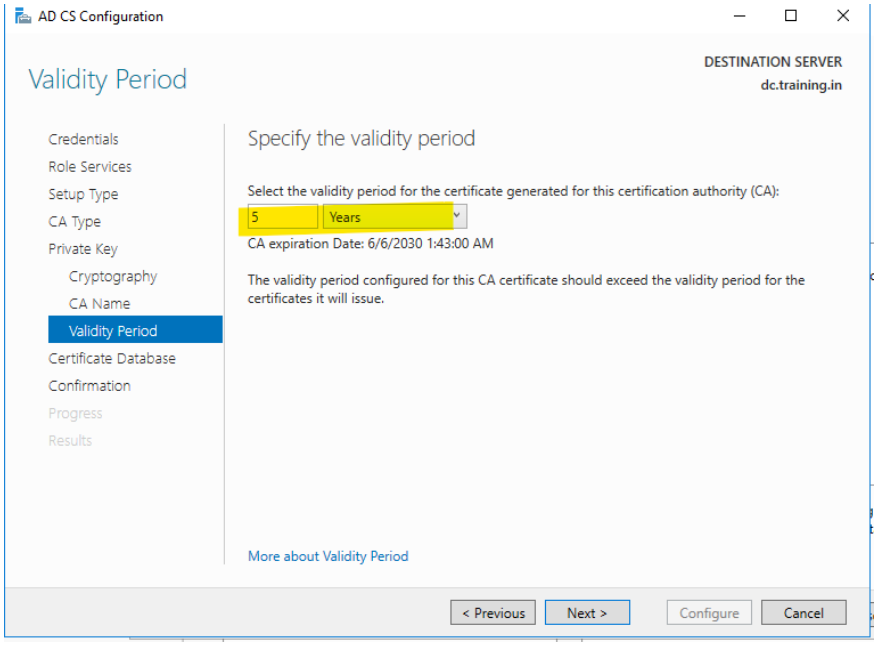
Configure CA Name

- Provide a Common Name for the CA (e.g., training-DC-CA).



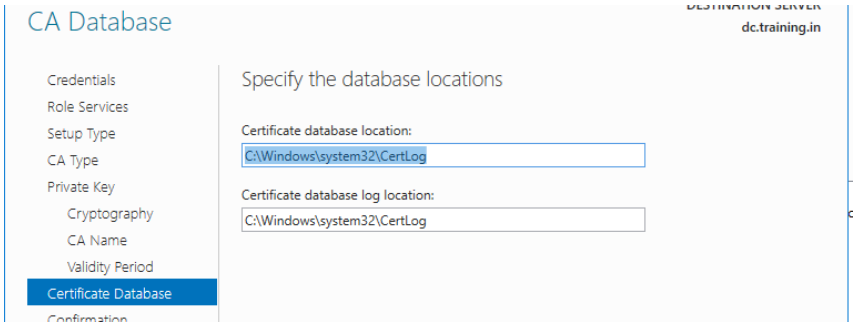
Validity Period

- Set validity period (e.g., 10 years for Root CA, 5 years for Subordinate CA).

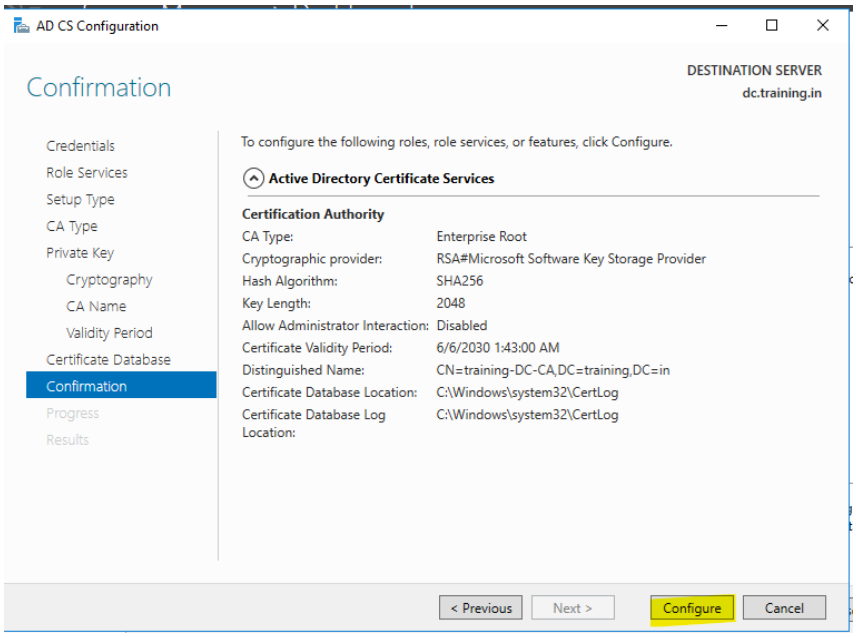


Configure Certificate Database

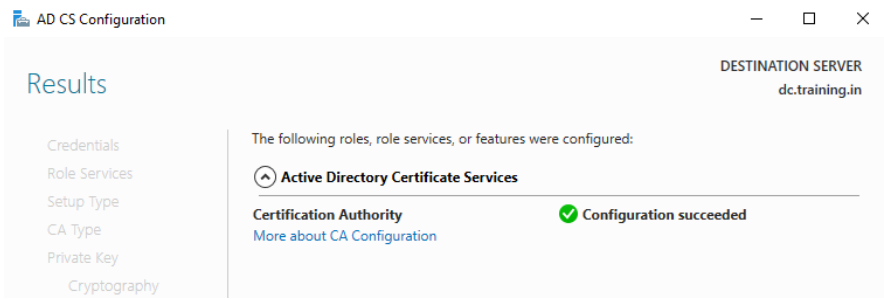
- Leave defaults or specify custom locations for the database and log files.



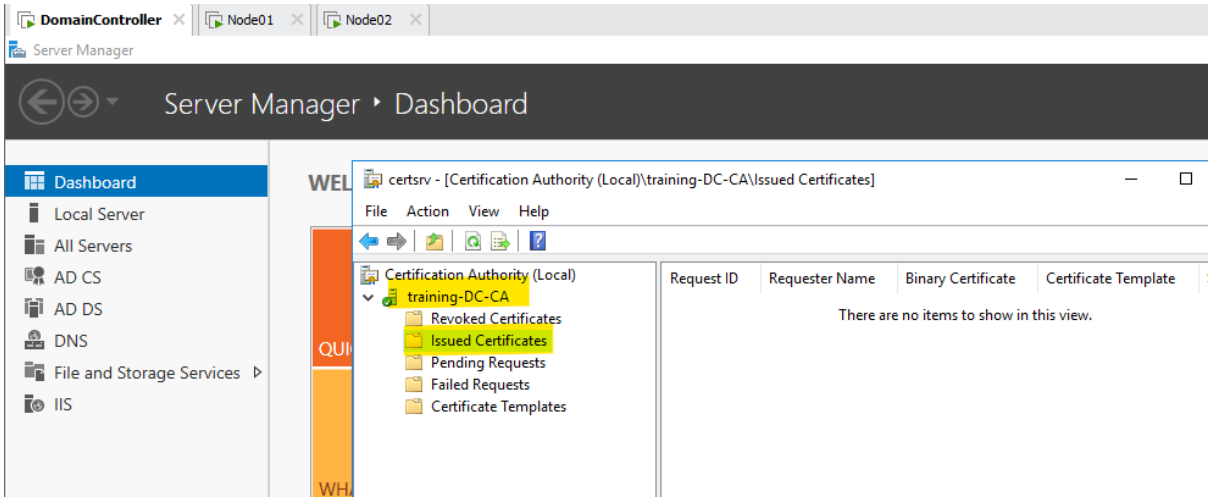
Click Configure,



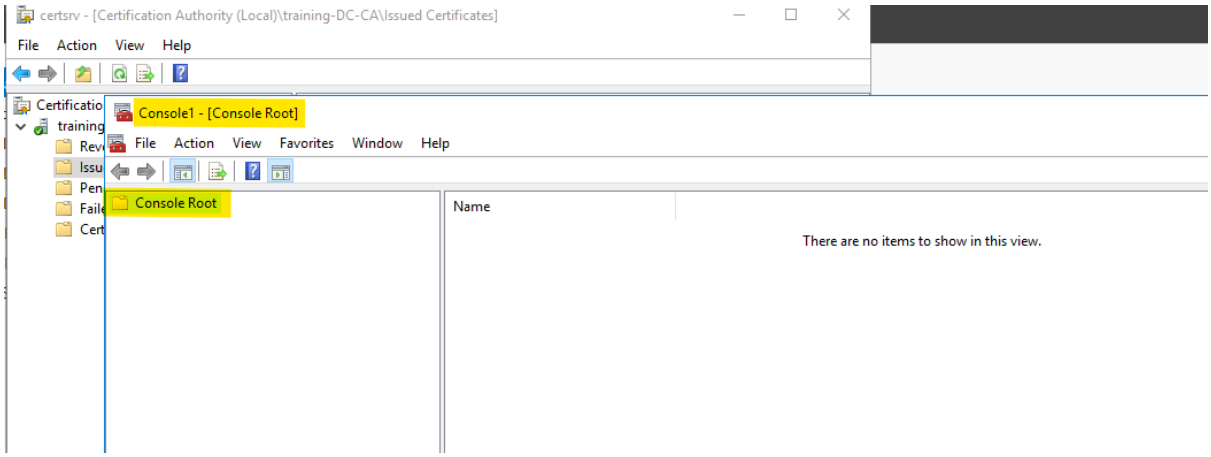
Wait for completion, and click Close.



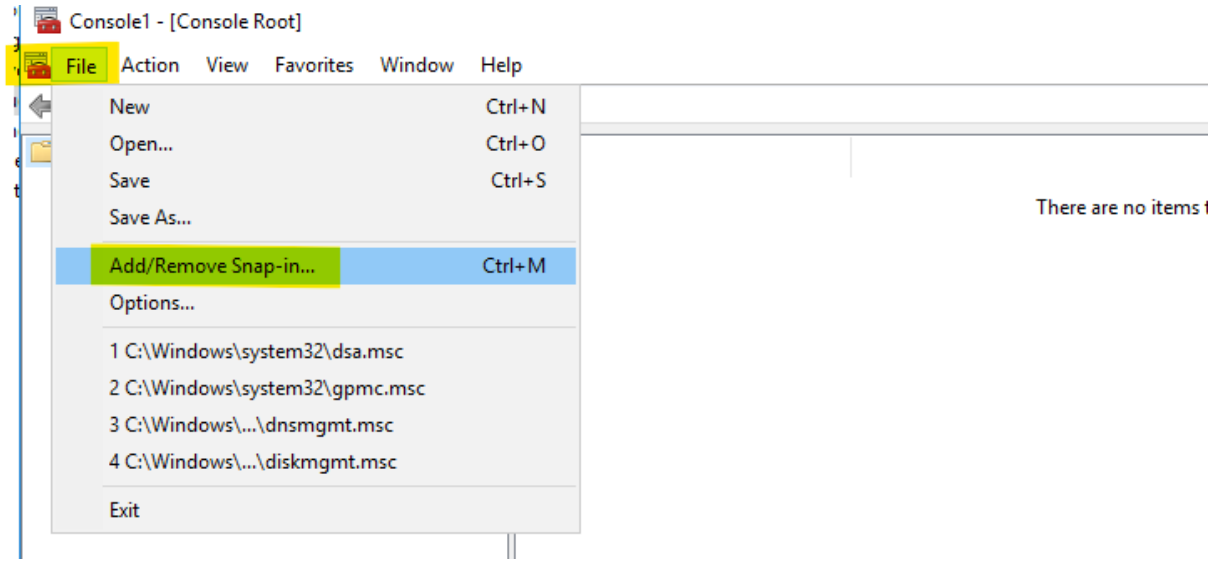
Go to: DC → Dashboard → Tools → Certification Authority → training-DC-CA → Issued Certificates



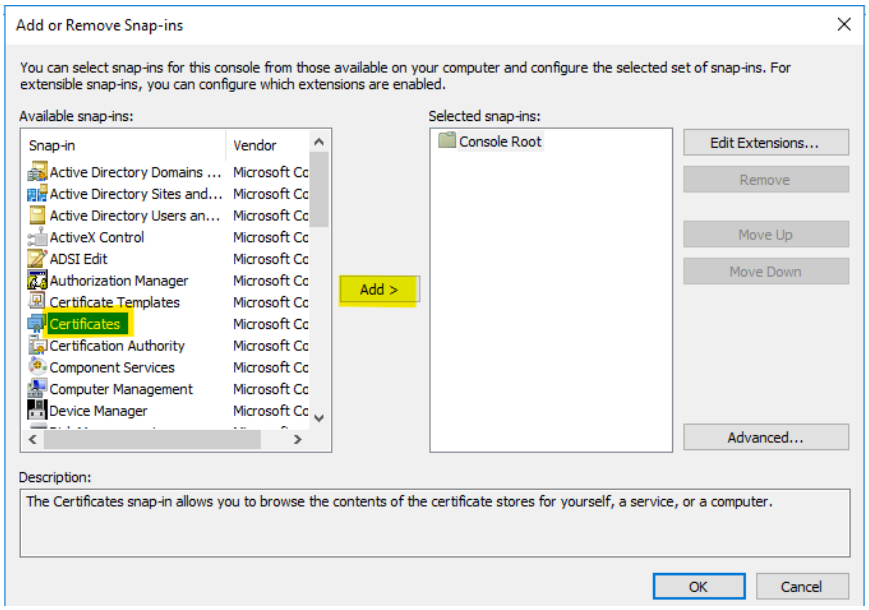
Next, Press “win+r” → run → type “mmc”



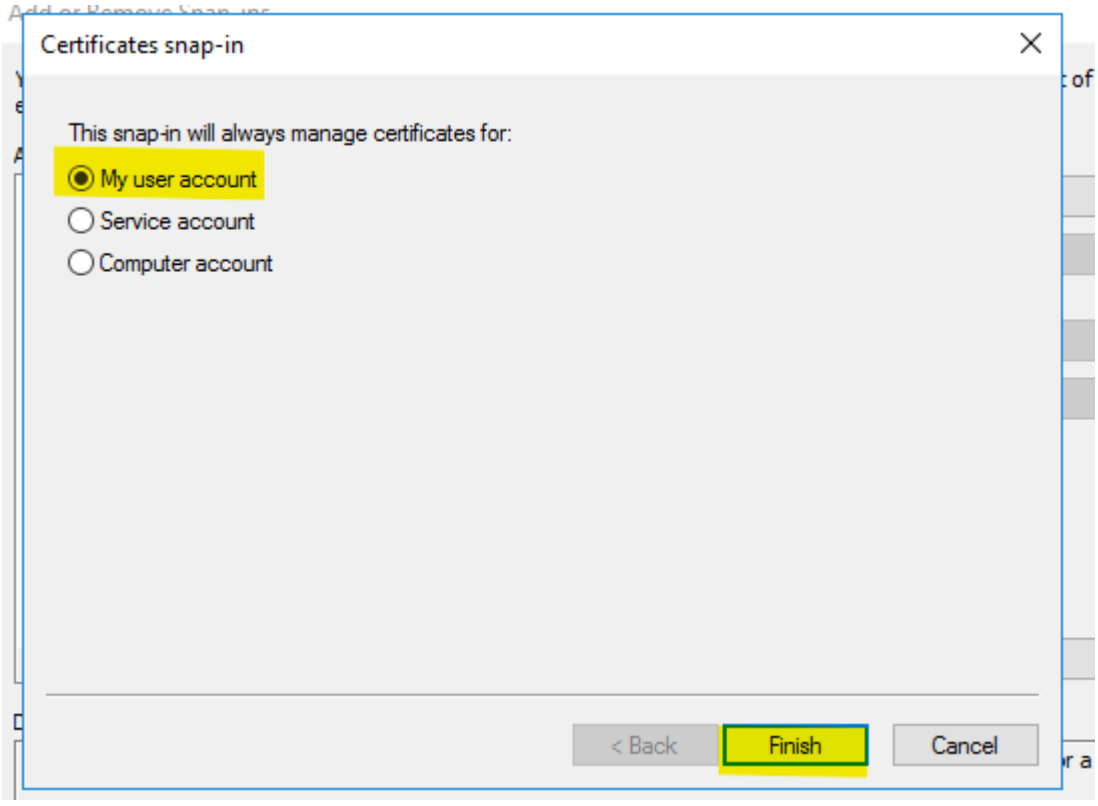
Go to File → Add/Remove snap-in…



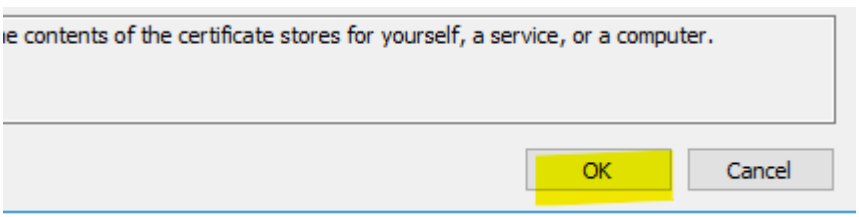
Click “Certificates” → “Add >”



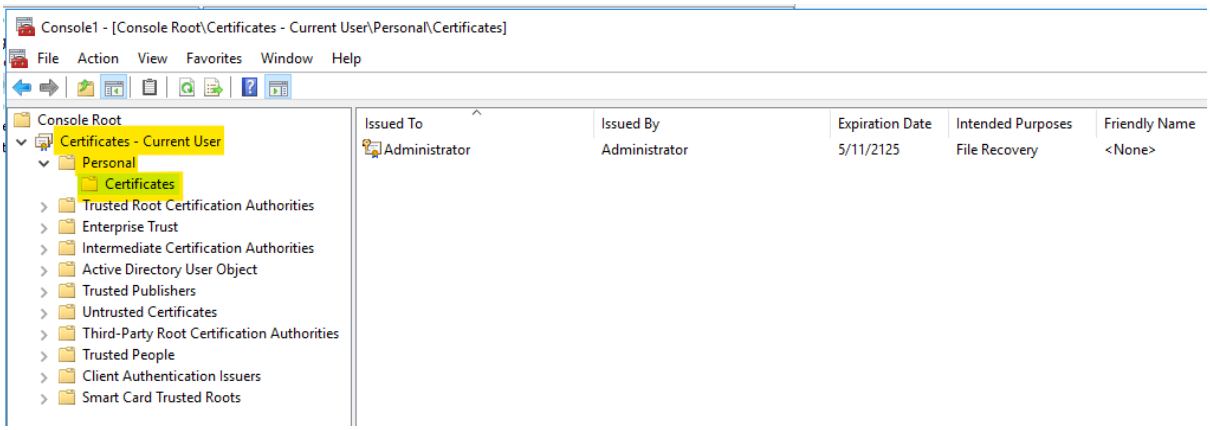
Select “My user Account” & then click Finish.



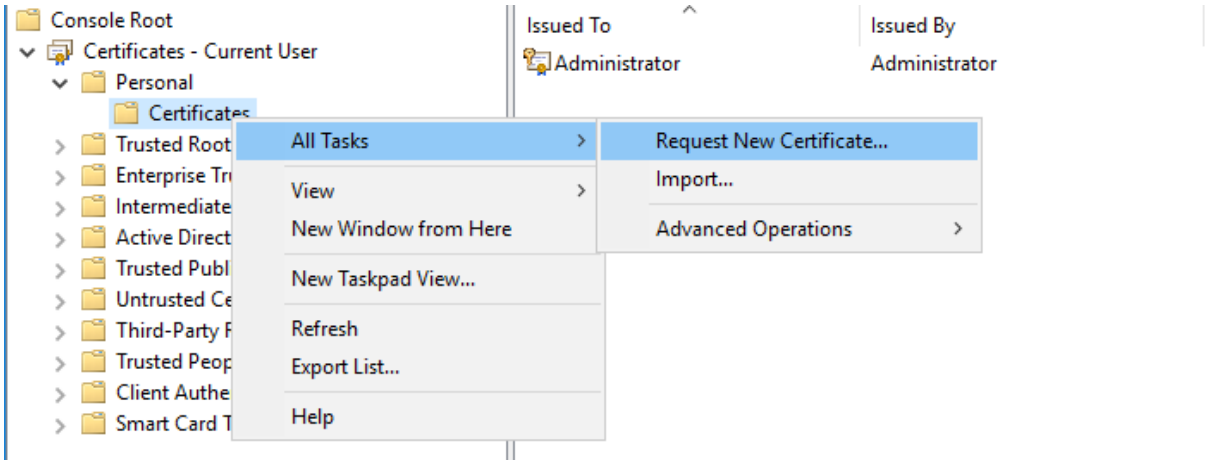
Then click OK.



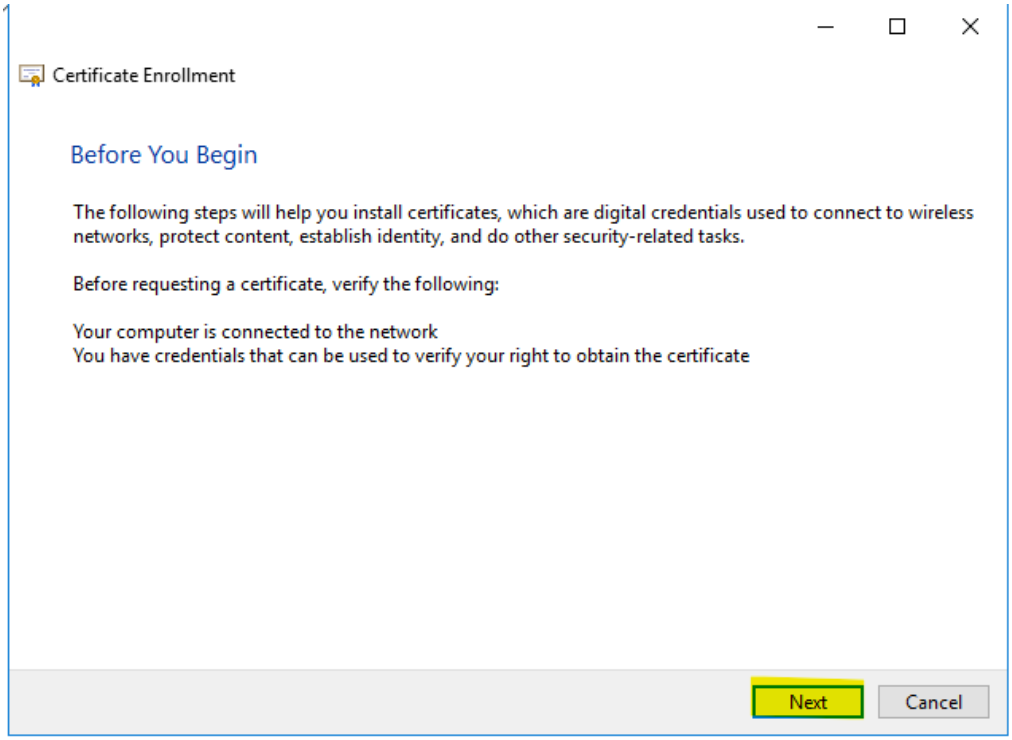
Now go to: Certificates – Current User →Personal → Certificates



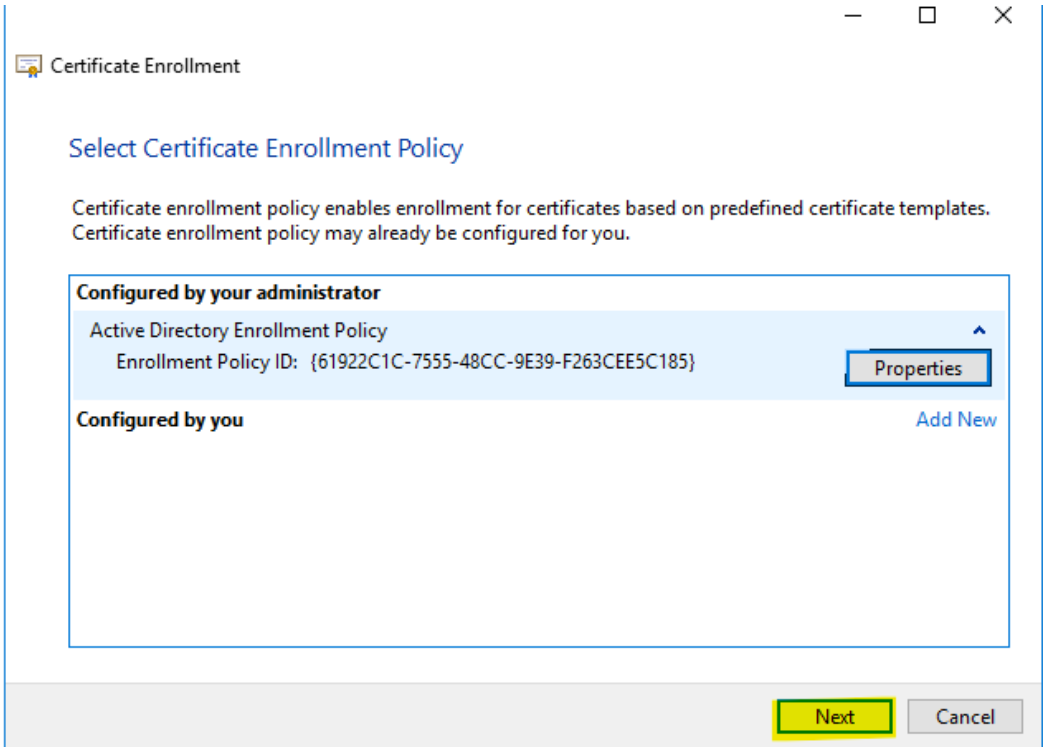
Now request for a new certificate:



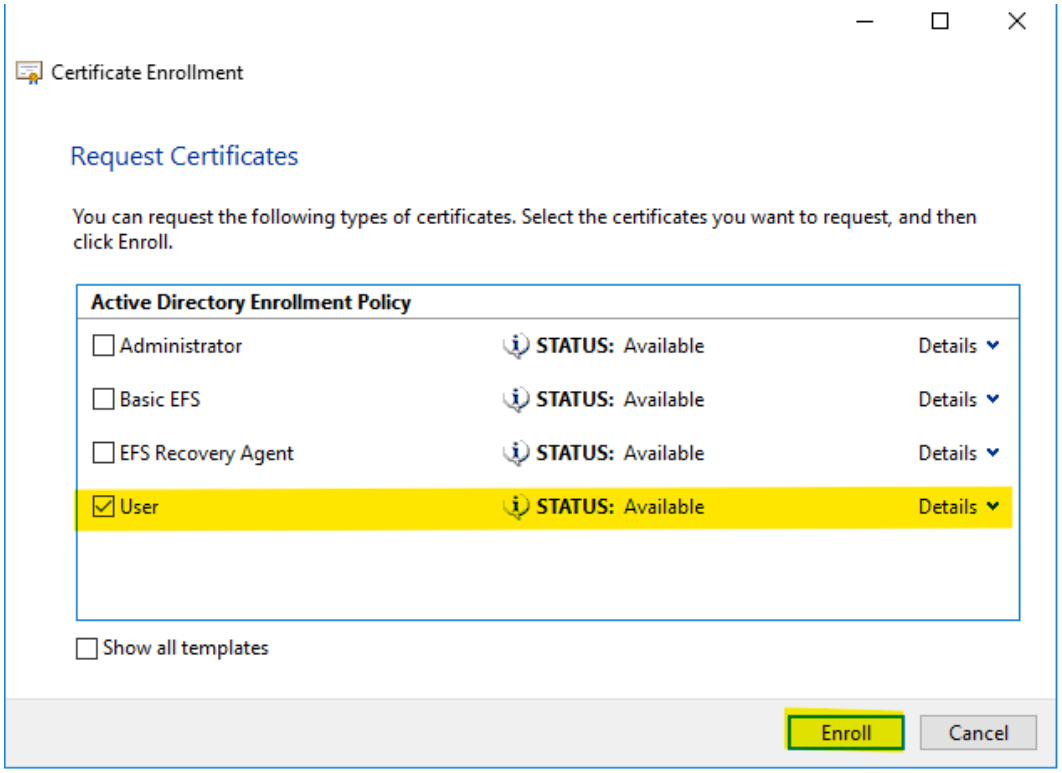
In Before you Begin,



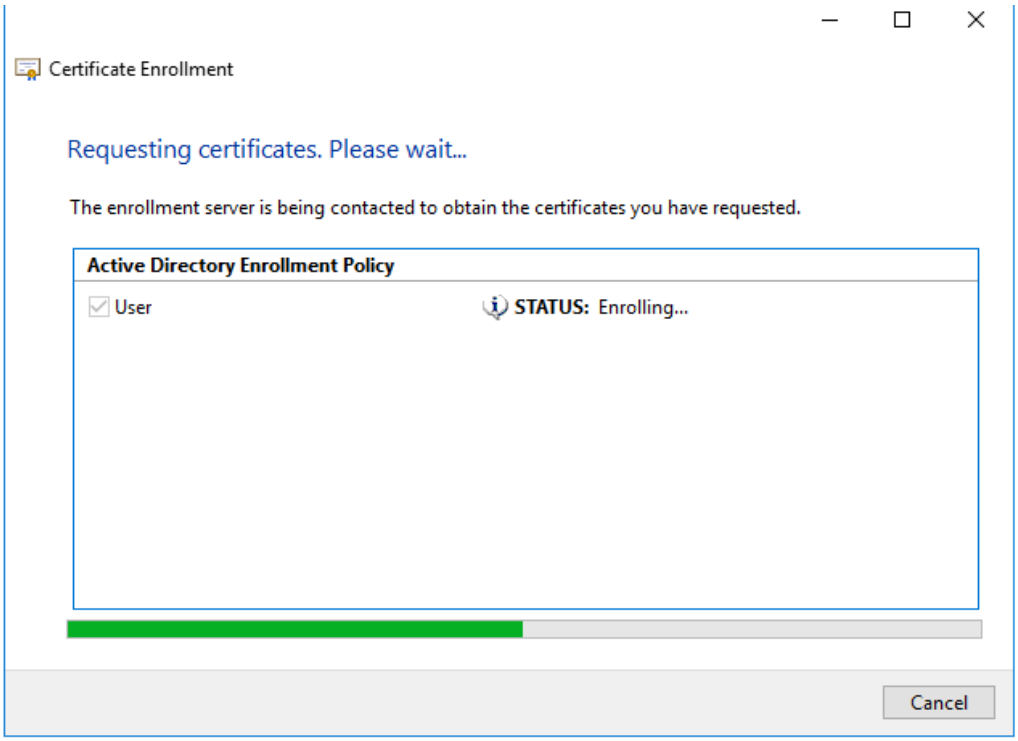
Click “Next” on certificate enrollment policy:

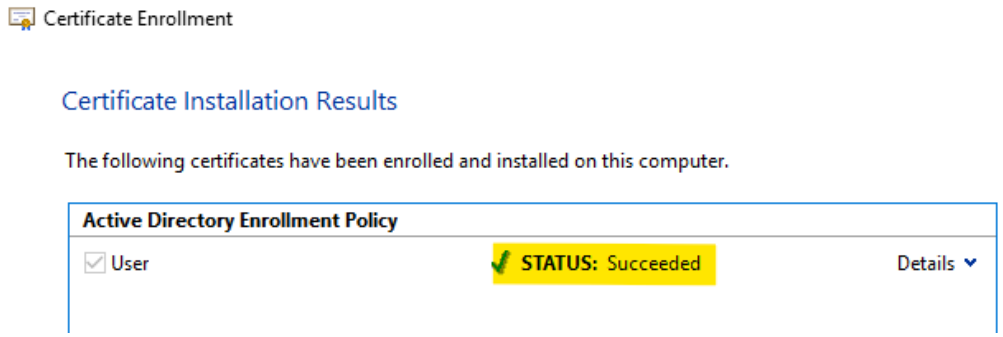


Select any request certificate:

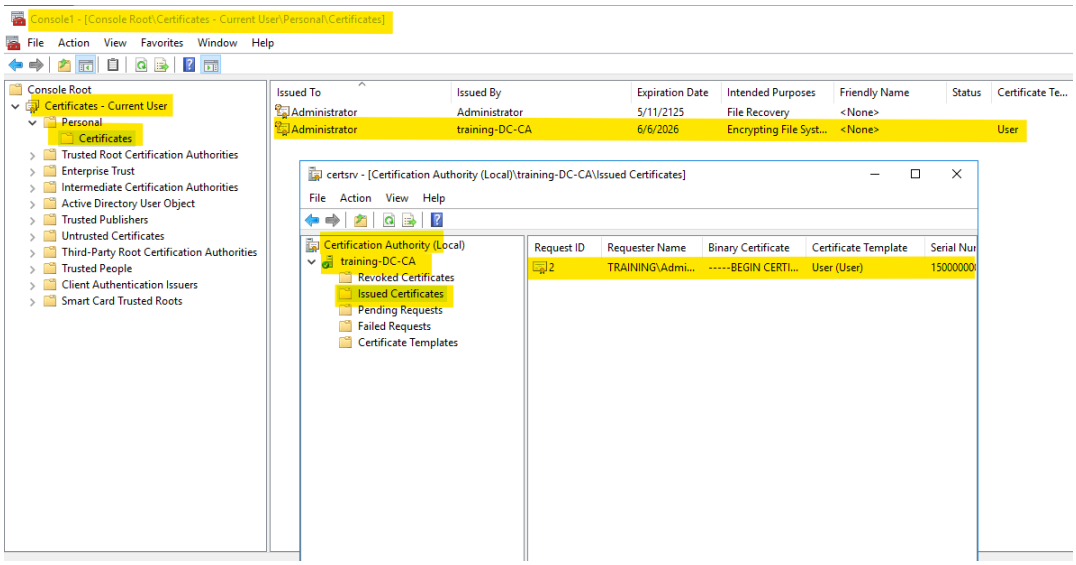


Wait…





To verify, go to Certification Authority and MMC:



Note – That's all for Certification Authority

Active Directory Federation Service (ADFS)

What is ADFS?

Active Directory Federation Services (ADFS) is a Single Sign-On (SSO) and web-based authentication solution developed by Microsoft. It allows users to access multiple applications (on-premises and cloud-based) using a single set of credentials from Active Directory (AD).

Key Features of ADFS

Feature	Description
Single Sign-On (SSO)	Users log in once and gain access to multiple systems
Federation	Trust relationship between multiple domains or organizations
Claims-Based Authentication	Uses security tokens with user identity data (claims)
Multi-Factor Authentication	Supports MFA for enhanced security
Access Control Policies	Define who can access what, when, and how
Integration with Azure AD	Extend on-prem SSO to Microsoft 365 and other cloud services

How ADFS Works (Authentication Flow)?

1) User accesses an application (relying party).
2) Application redirects user to ADFS for authentication.
3) ADFS authenticates the user against Active Directory.
4) ADFS issues a security token (containing claims).
5) The token is passed back to the application.
6) The application validates the token and grants access.

ADFS Architecture

1. ADFS Server

- The main component that authenticates users and issues tokens.

2. Web Application Proxy (WAP)

- Deployed in DMZ, Publishes ADFS to external users, Acts as a reverse proxy.

3. Active Directory

- Identity provider storing user accounts and group memberships.

4. Relying Party Trusts

- External or internal applications that trust ADFS to authenticate users.

5. Claims Provider Trusts

- External identity providers trusted by your ADFS to provide user identities.

ADFS Components

Component	Description
Claims	User attributes (e.g., email, UPN, group) sent in the token
Relying Party Trust (RP)	Application that uses ADFS to authenticate users
Claims Provider Trust	External identity providers (e.g., another ADFS, Azure AD)
Attribute Store	Source of claim values (usually AD)
Security Token Service (STS)	Issues, signs, and validates tokens

Supported Protocols

Protocol	Use Case
SAML 2.0	Federation with external apps (Salesforce)
WS-Federation	Legacy apps
OAuth 2.0	Modern apps and APIs
OpenID Connect	Web apps and mobile apps

Multi-Factor Authentication (MFA)

- ADFS supports:
    - Windows Hello for Business
    - Certificate-based auth
    - OTP (one-time password)
    - 3rd-party MFA (Duo, RSA)
- Configured via Access Control Policies

ADFS Management Tools

Tool	Use
ADFS Management Console (adfsmgmt.msc)	GUI tool to configure ADFS
PowerShell	Scripting and automation
Event Viewer	Logs under **Applications and Services Logs > ADFS**
Performance Monitor	Track token requests, sign-ins, etc.

Step by step setup of ADFS:

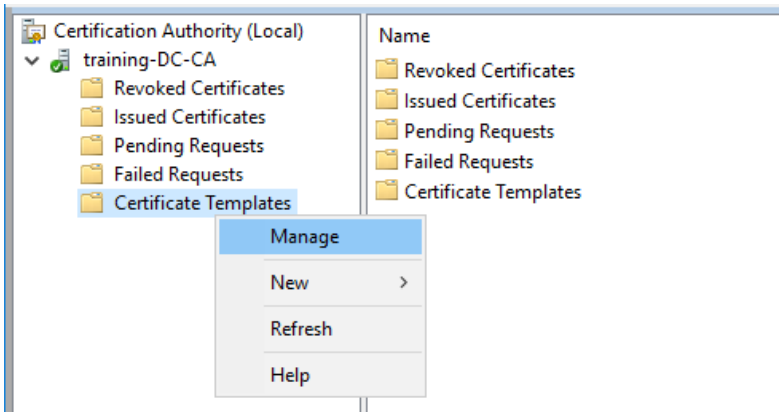
STEP 1: PREREQUISITES

1. Domain Membership
    - Ensure ADFS server (Node01) is joined to the domain.
2. Static IP Address
3. DNS Configuration
    - Make sure ADFS server can resolve DC and vice versa.
4. Service Account
    - Create a domain user account (e.g., svc_adfs or training\administrator) with a strong password.
    - Give it permission to log on as a service (optional step).

STEP 2: CREATE / OBTAIN AND CONFIGURE SSL CERTIFICATE

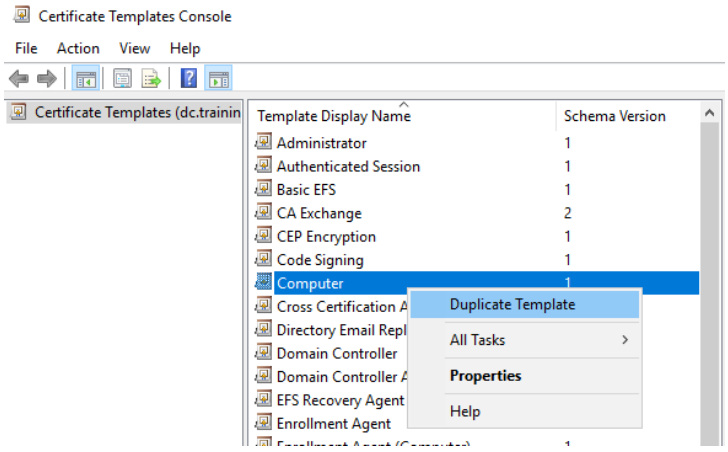
Creating an SSL certificate using internal Certification Authority (CA):

On the DC machine → Dashboard → Tools → Certification Authority → Certificate Template → right-click → Manage

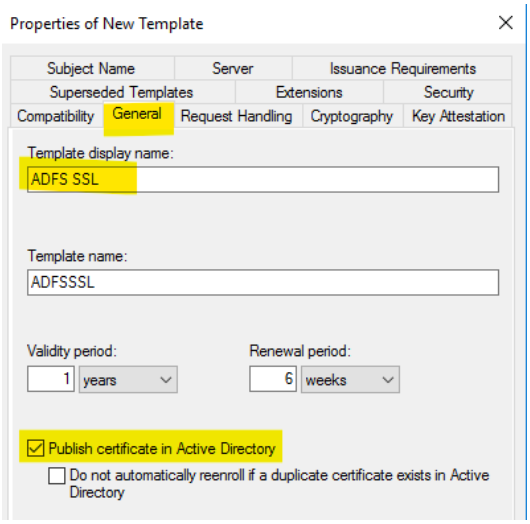


Here, we will create a template with the help of which we will create SSL certificate later.

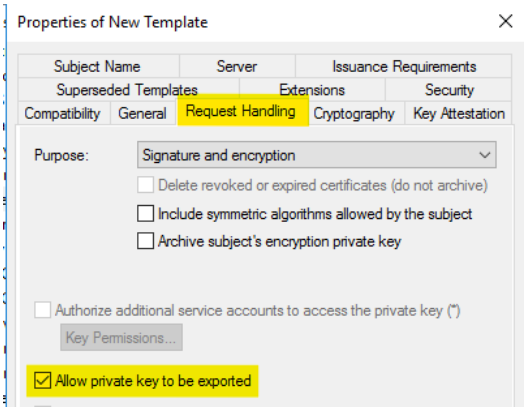
Right-Click on “Computer” display name and click on “Duplicate Template”



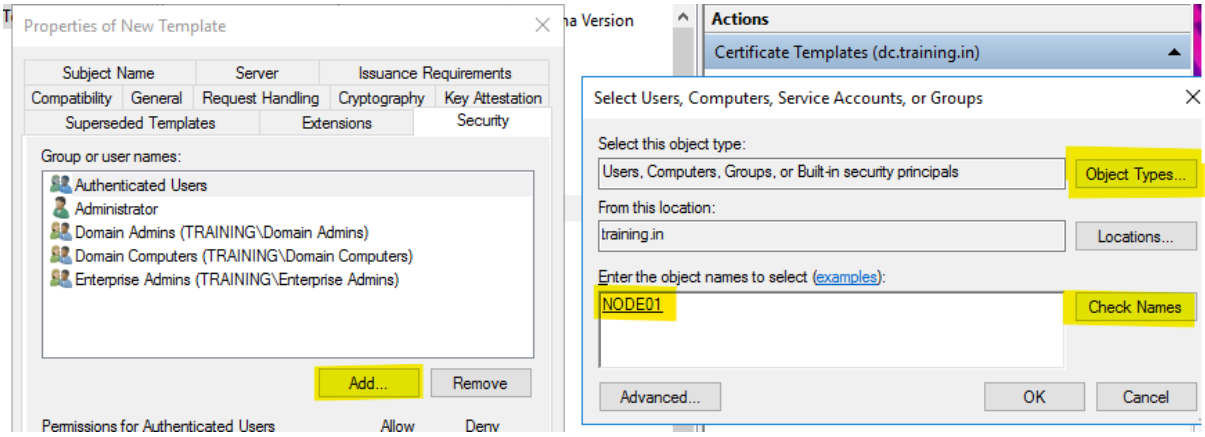
Now go to “General” tab and type “ADFS SSL” in template display name:



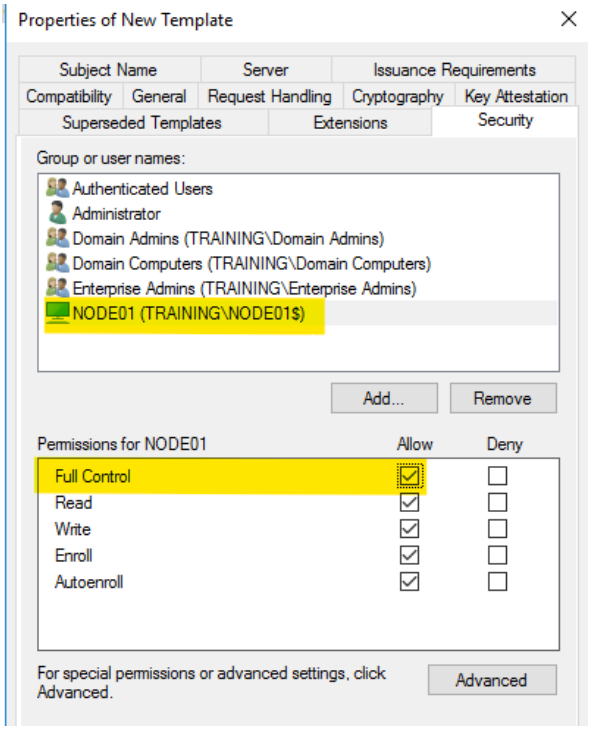
Now go to “Request Handling”, check “Allow private key to be exported”.



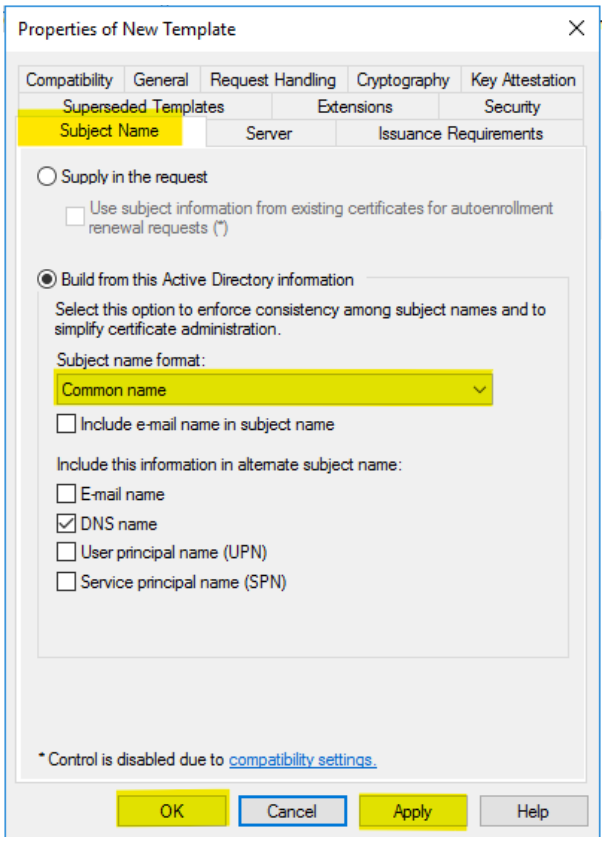
Now go to “Security” tab and add the machine on which you will install ADFS role (Node01 in my case). If the computer name is not present after search, click in “Object Types…” and check ‘computer’ field.



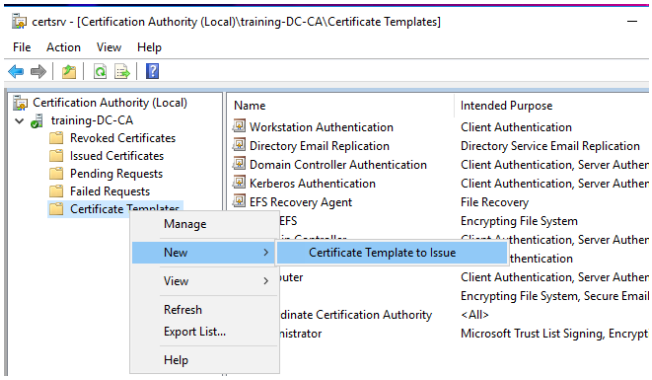
Allow full control for Node01.



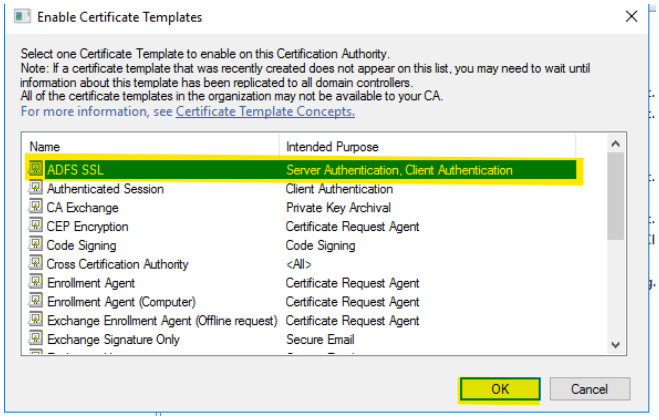
Now go to “Subnet Name” tab, select “Common Name” and Apply and OK.



Now again go to Certificate Template, right-click → New → Certificate Template to Issue.

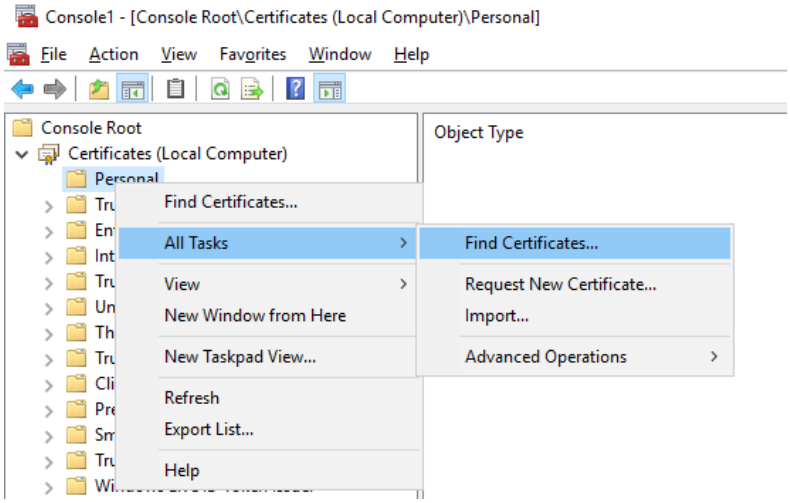


Select the template you created and click OK.

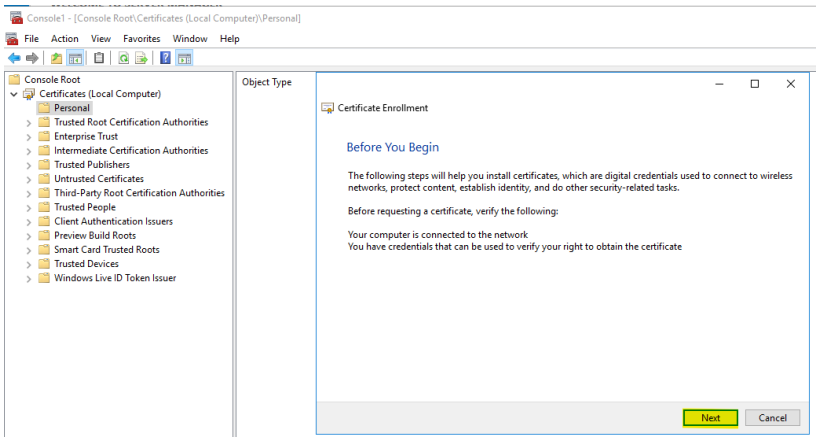


Now switch to machine where ADFS is installed (in my case Node01).

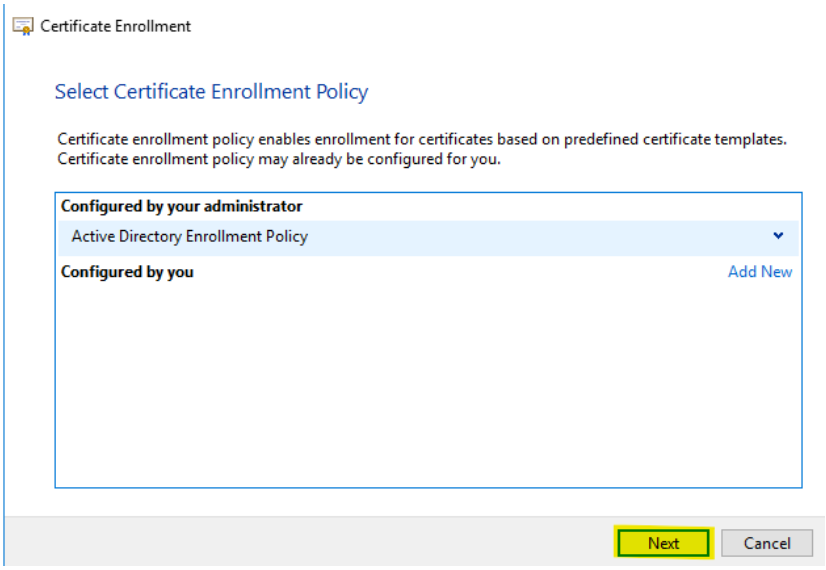
Run → mmc → File → Add/remove snap-in… → Certificate → "Add" → Computer account → OK → Certificates (Local Computer) → Personal → All Task → Request New Certificate…



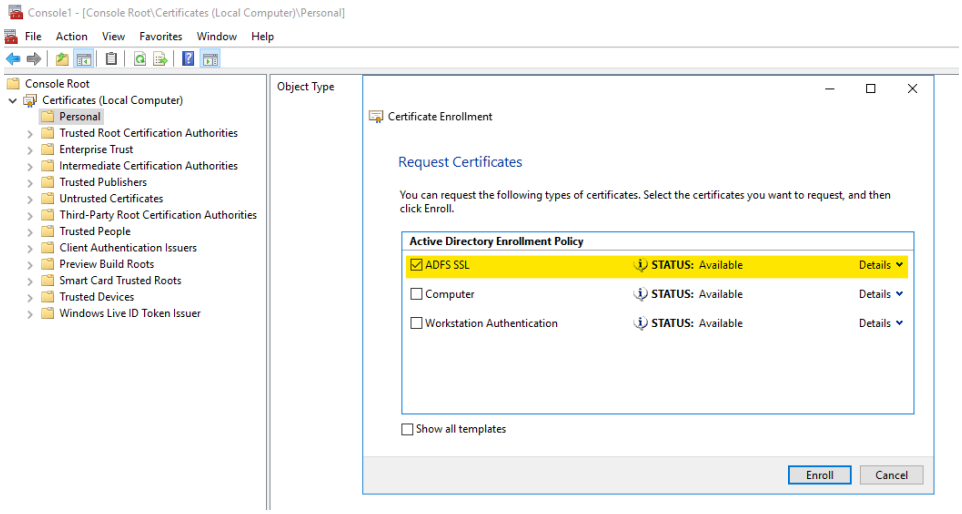
Click Next on “Before you Begin”



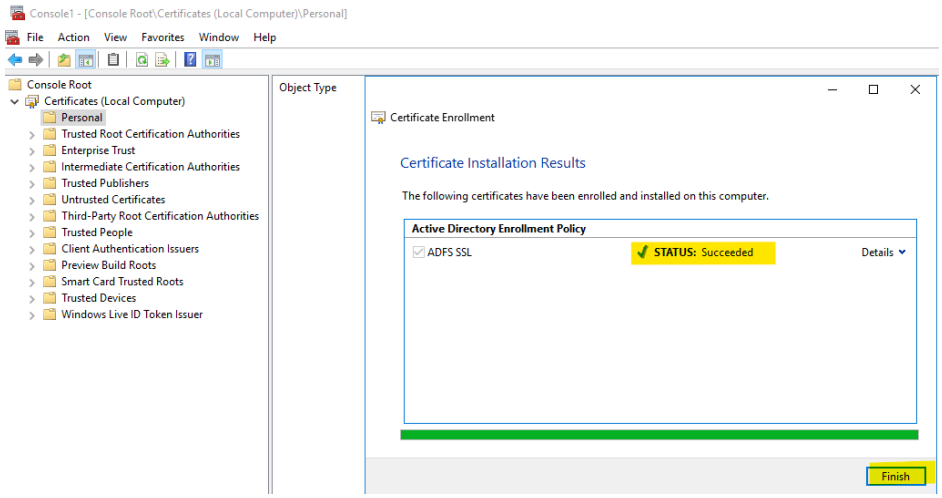
Click Next on Certificate Enrollment Policy



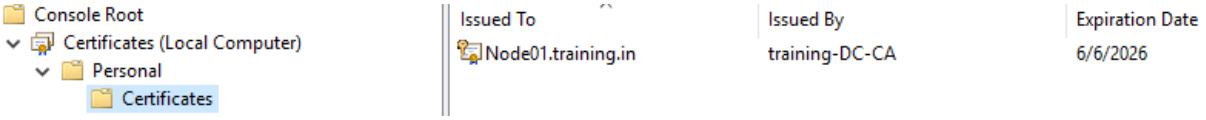
Select the custom created SSL certificate & click on Enroll



Verify if it’s successful and click on “Finish”



Personal → Certificate



Steps:

1. Add Certificates snap-in > for Computer Account.

   Click “Finish”

2. Request a certificate:
   - Right-click Personal > Certificates > All Tasks > Request New Certificate.
   - Use your internal CA to request a Web Server certificate.
   - Common Name (CN): Node01.training.in (match DNS name).

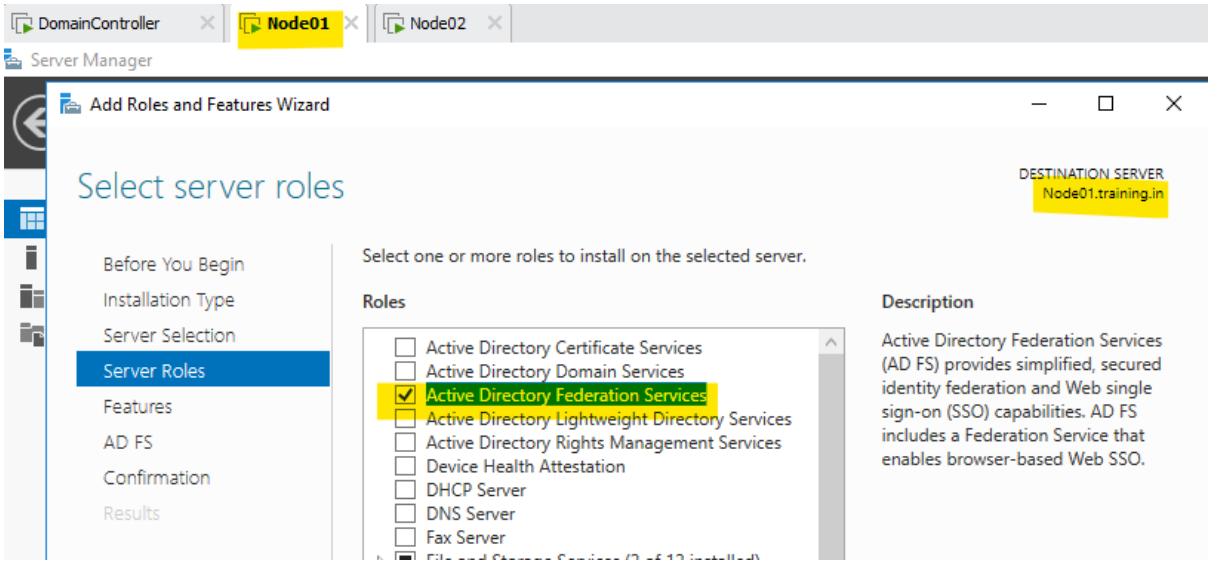
   After Requesting → Next, under Certificate Enrollment Policy → Next:

3. After installing, verify the certificate is under Personal > Certificates.

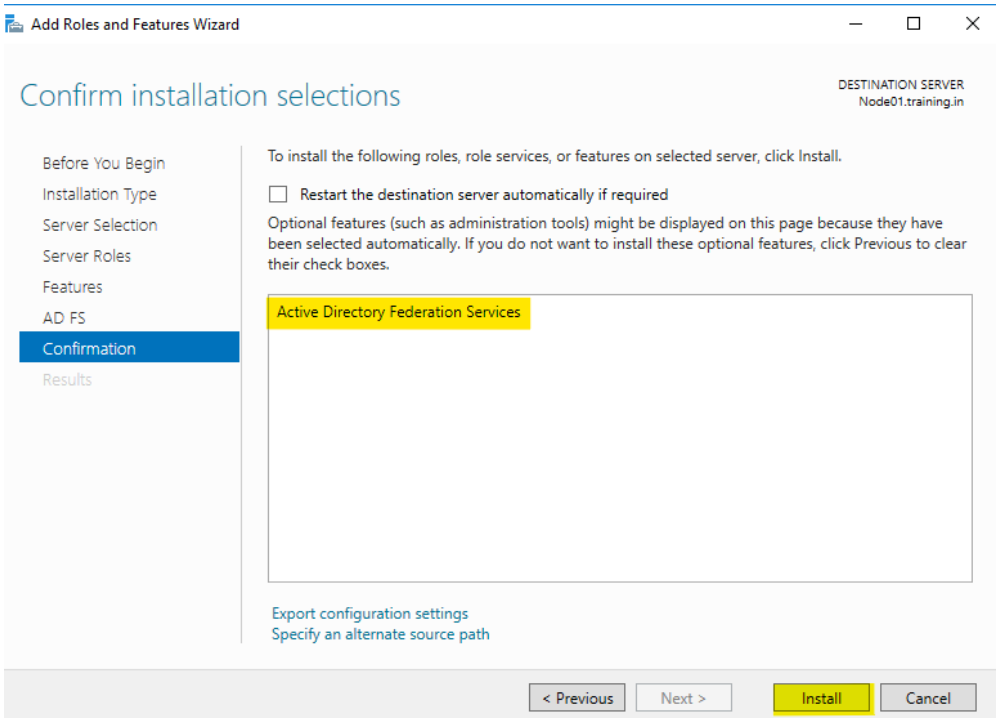
Now you can install ADFS role on Node01.training.in

STEP 3: INSTALL ADFS ROLE ON ADFS SERVER

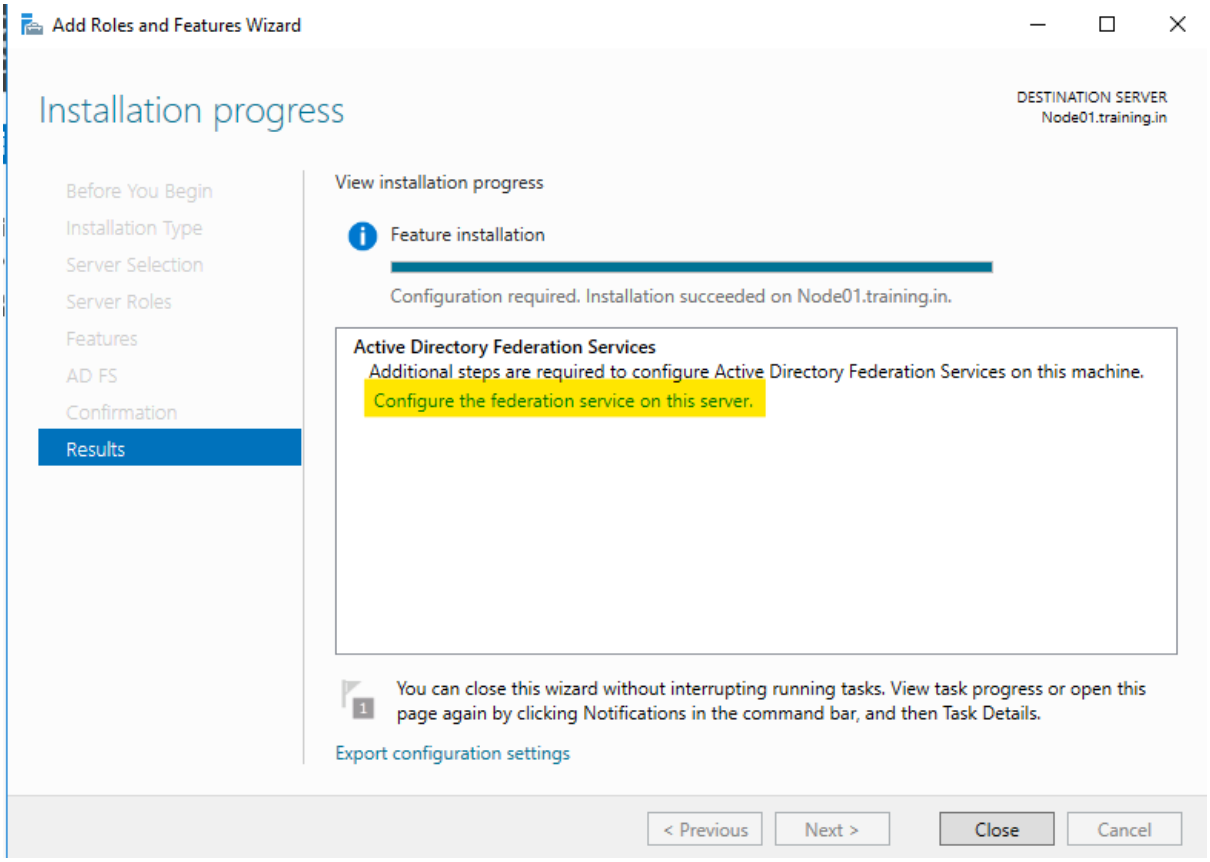
1. Log in to *Node01.training.in* using a domain administrator account.
2. Open Server Manager.
3. Click on Manage > Add Roles and Features.
4. Click Next until you reach Server Roles.
5. Select Active Directory Federation Services, click Next.
6. Click Next again and install.



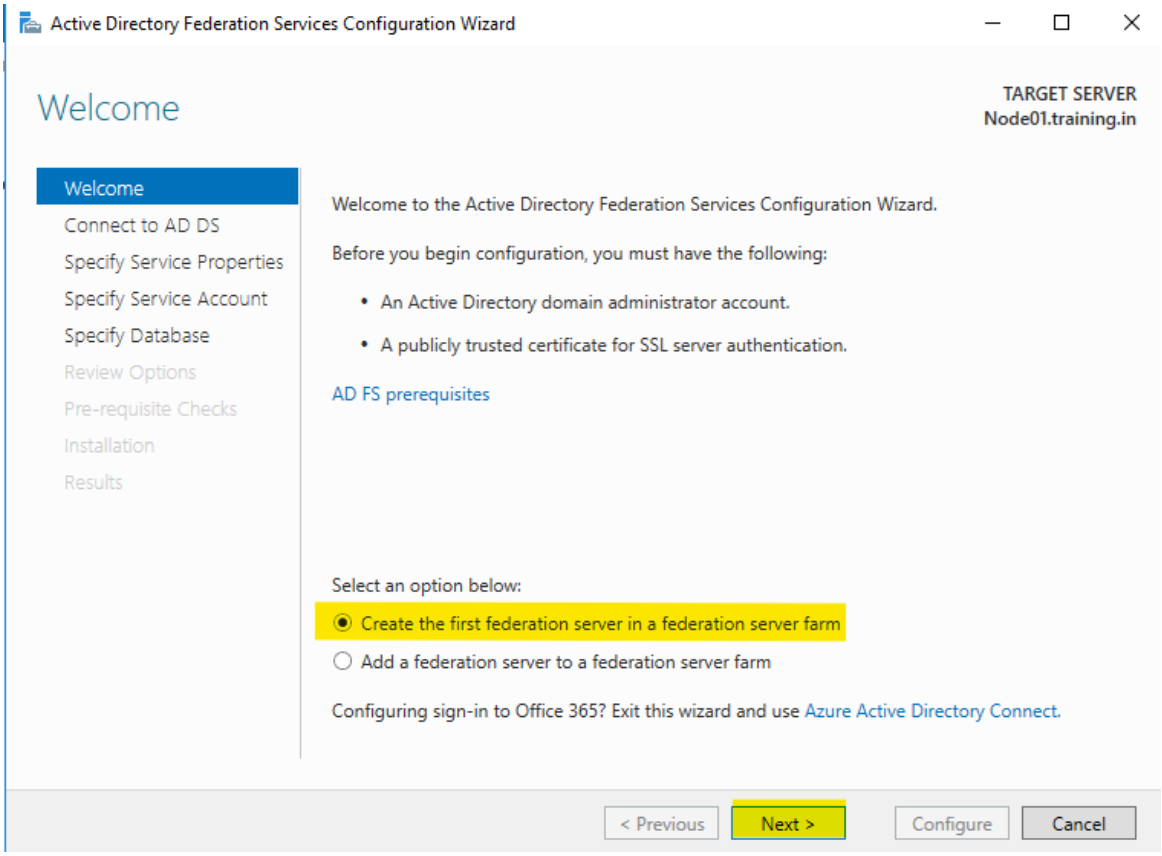
Click Install:



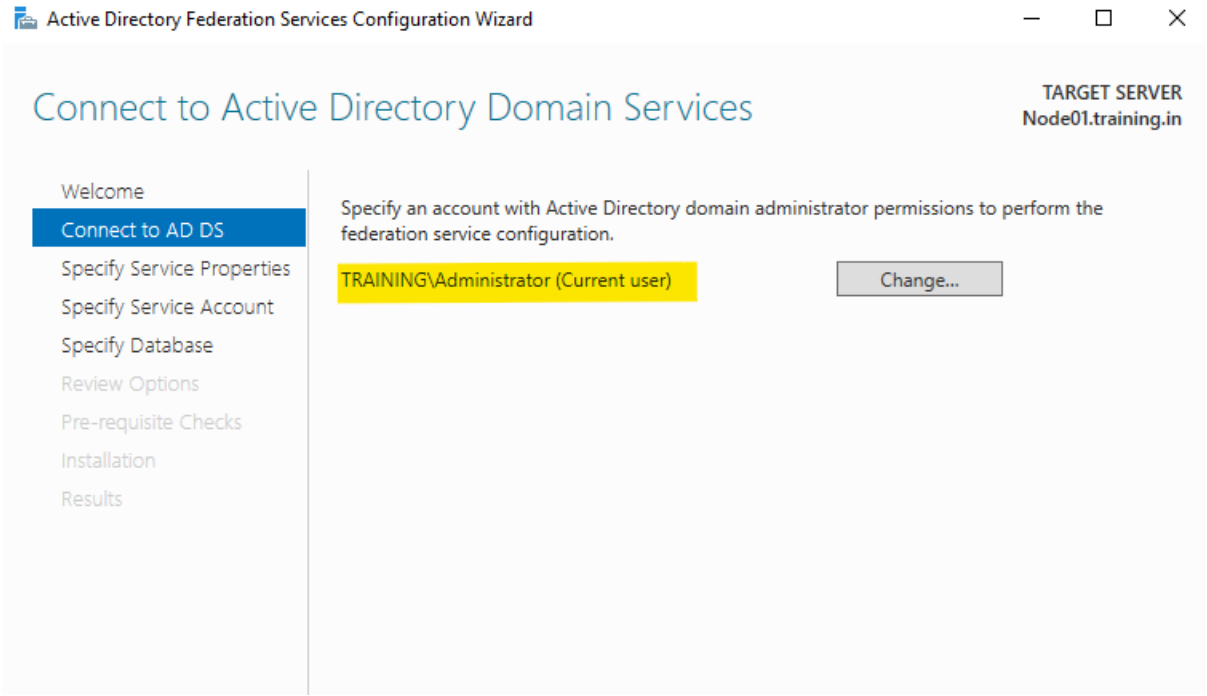
Wait on this page & switch to next step.



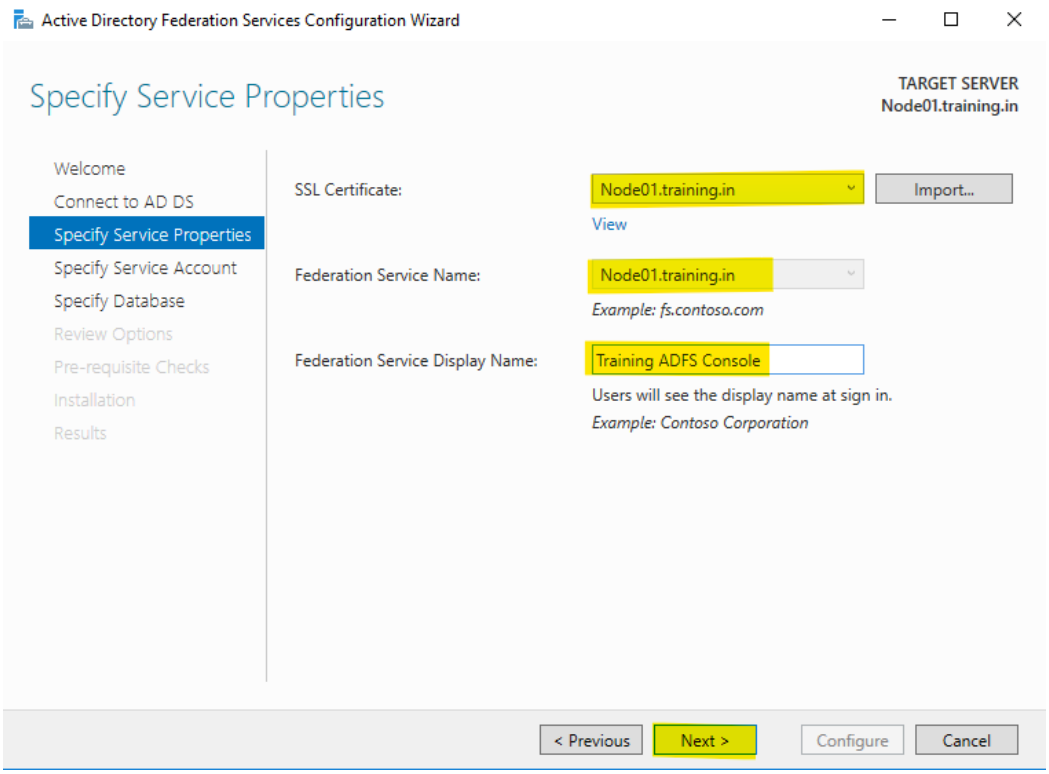
After installation, now configure ADFS server on Node01



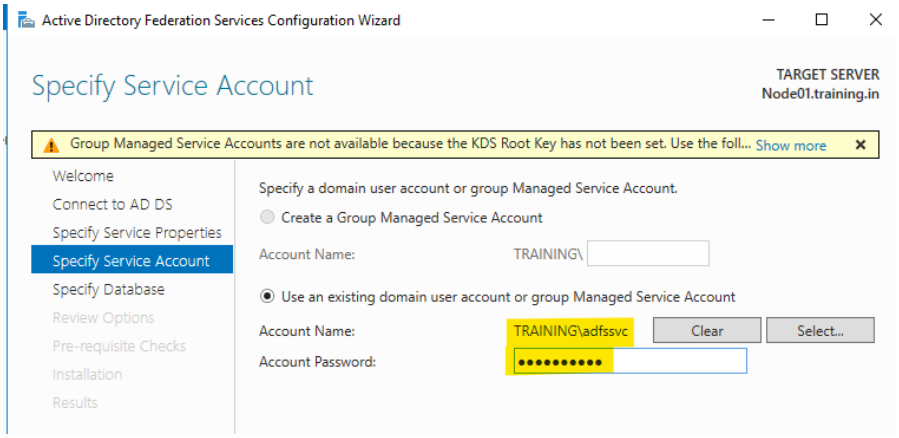
Either login with a service account that has proper permissions or login with domain Admin.



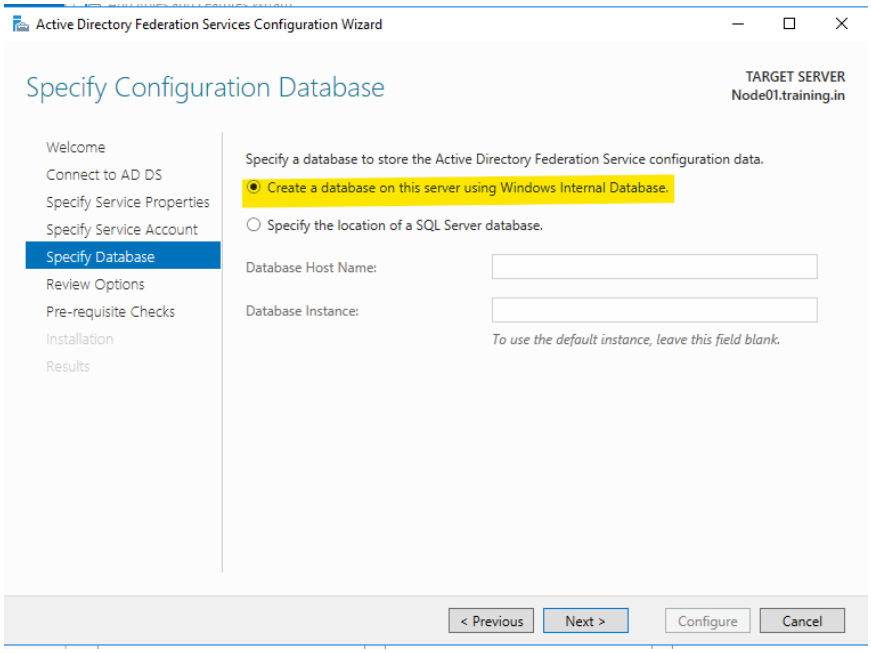
Select the SSL certificate using drop down.



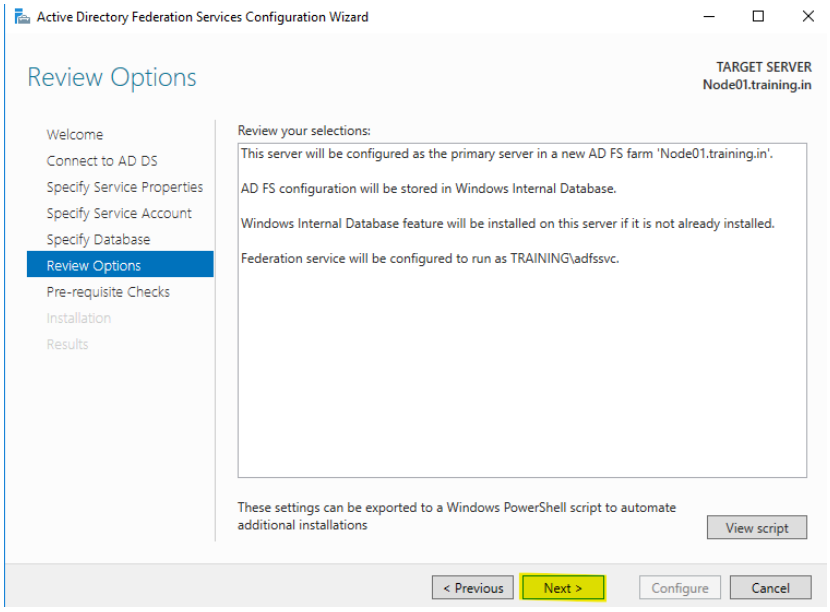
Now, ADFS needs credentials of any user/service to login. I replicated user named “Demouser1”, that we created earlier. And allocated credentials of that user.



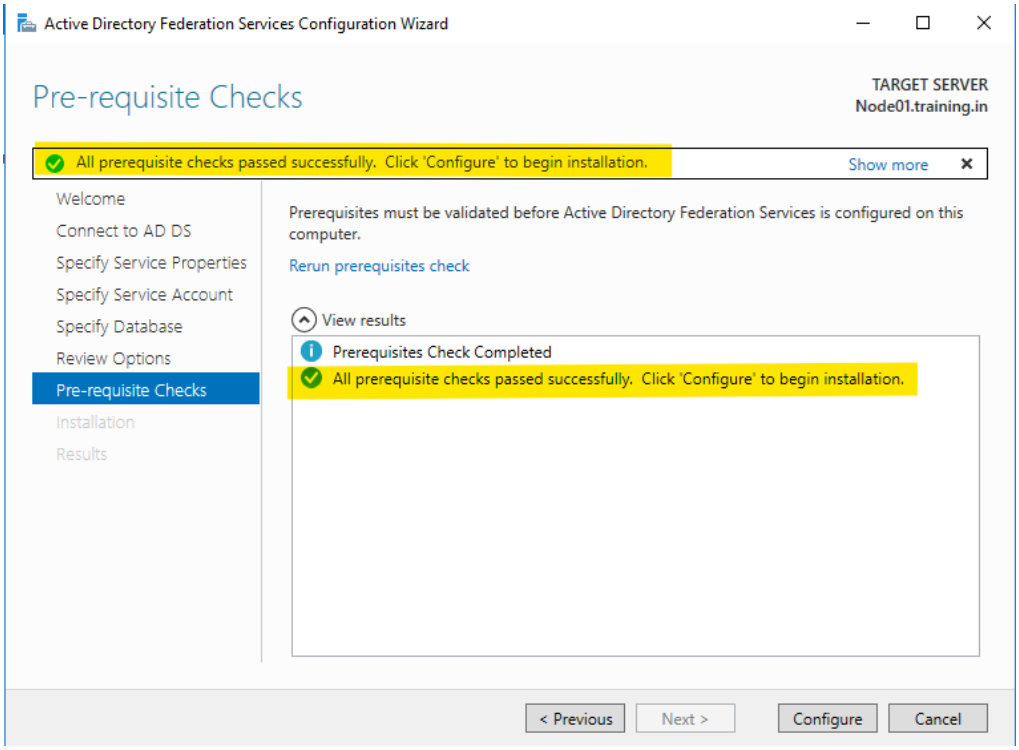
Use Windows Internal Database (WID).



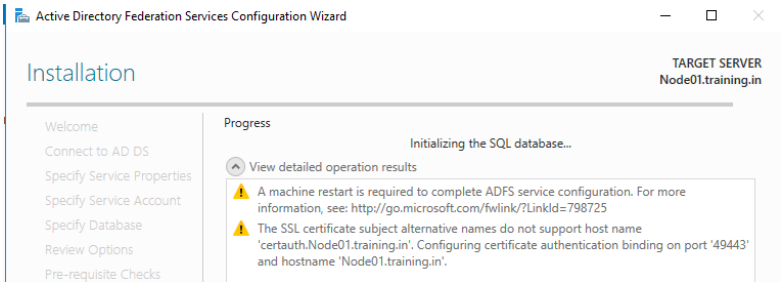
Review all:



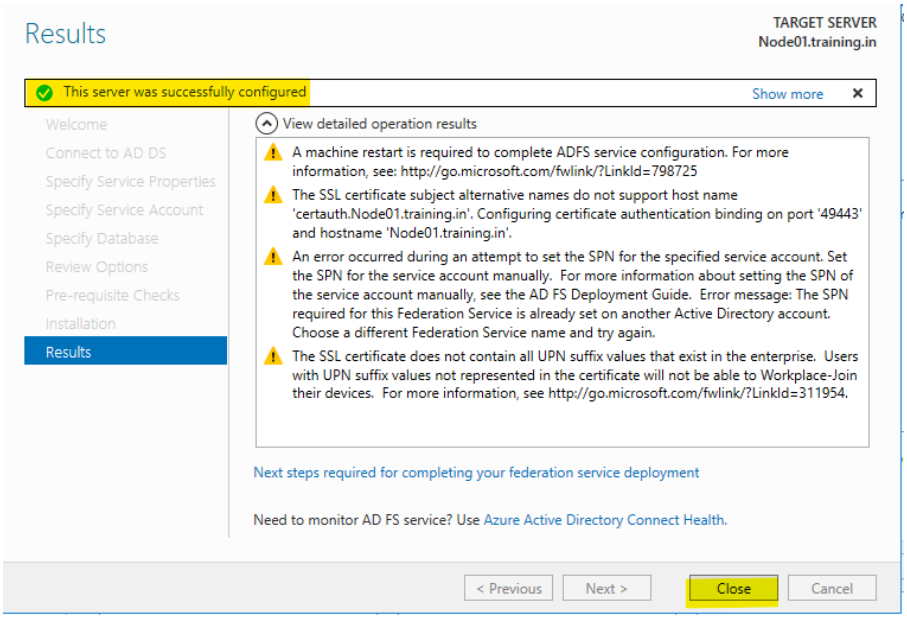
Once all pre-requisites are done & successful. Click on “Configure”



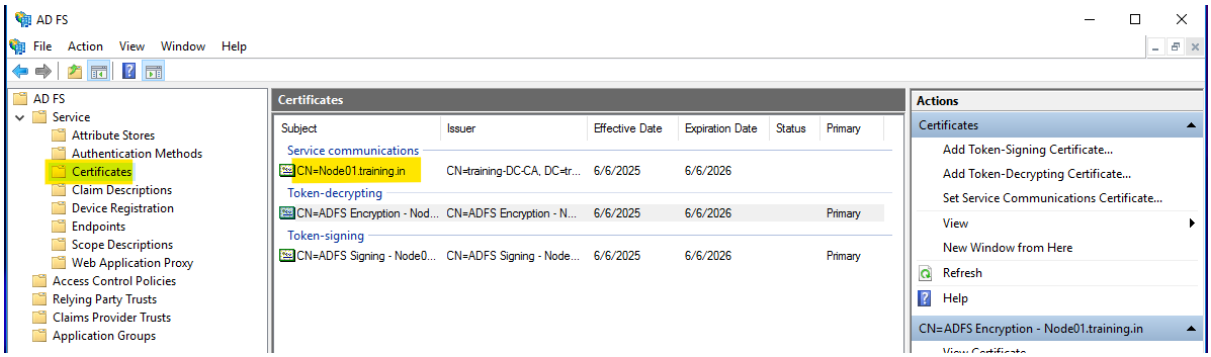
Wait until it’s done.



Close after completion.



Now Node01 → Dashboard → Tools → ADFS Management & just verify.



To check if the ADFS is working properly or not, we need to access IDP initiated Sign on page.

```
PS C:\Users\administrator.TRAINING> Get-AdfsProperties | fl *enableidp*

EnableIdpInitiatedSignonPage : False
```

Cmd: **Get-AdfsProperties | fl *enableidp***

To enable, run this command given below.

Cmd: **Set-AdfsProperties -EnableIdPInitiatedSignonPage $true**

```
PS C:\Users\administrator.TRAINING> Set-AdfsProperties -EnableIdPInitiatedSignonPage $true
PS C:\Users\administrator.TRAINING>
PS C:\Users\administrator.TRAINING> Get-AdfsProperties | fl *enableidp*

EnableIdpInitiatedSignonPage : True
```

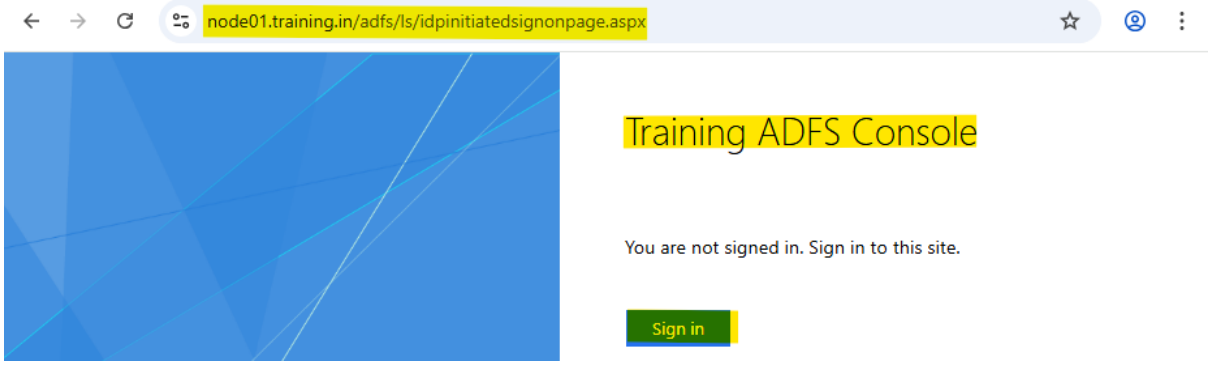
To list for the endpoint to ADFS services

Cmd: **Get-AdfsEndpoint | fl *fullurl*** → search for the URL ends with "**/ls/**"

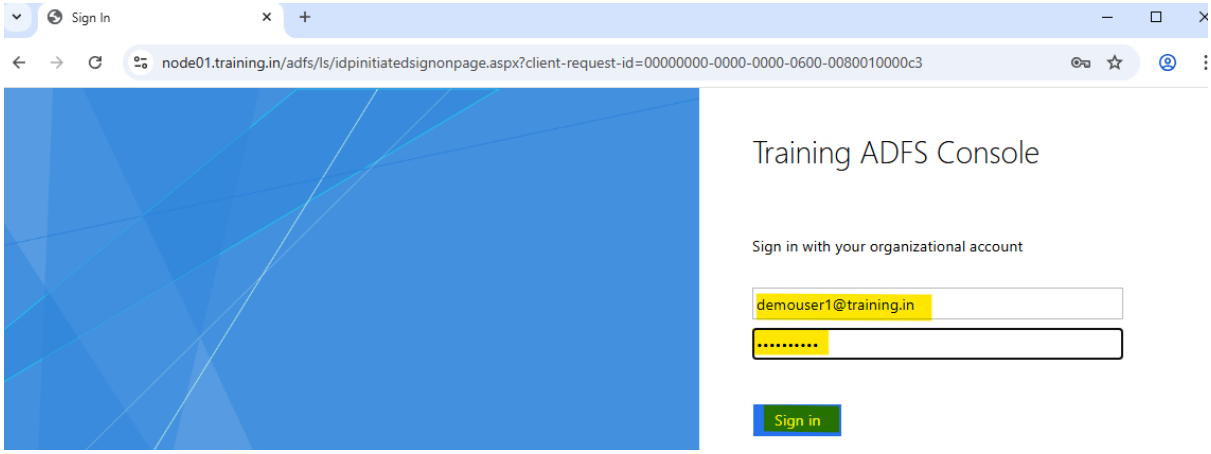
```
PS C:\Users\administrator.TRAINING> Get-AdfsEndpoint | fl *fullurl*

FullUrl : https://node01.training.in/adfs/services/trust/mex
FullUrl : https://node01.training.in/adfs/ls/
FullUrl : http://node01.training.in/adfs/services/trust/2005/windows
```

Copy this URL and add '**idpinitiatedsignonpage.aspx**'

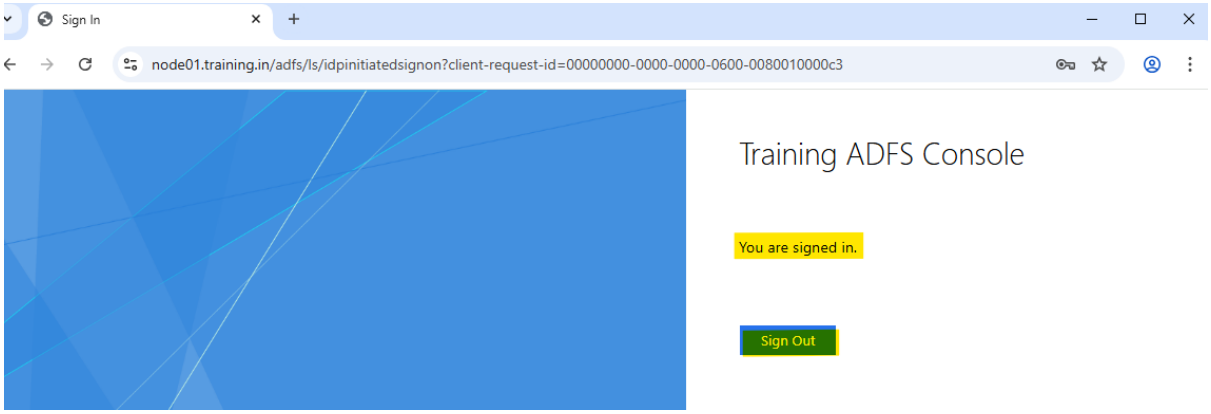
And make the URL like this → https://node01.training.in/adfs/ls/**idpinitiatedsignonpage.aspx**



Try signing on with a user by clicking on “Sign in” button and type credentials



If you get the output “You are signed in.”, means all good and ADFS is working.



After verifying, you can sign-out.

Note – That’s all for ADFS

Thank You