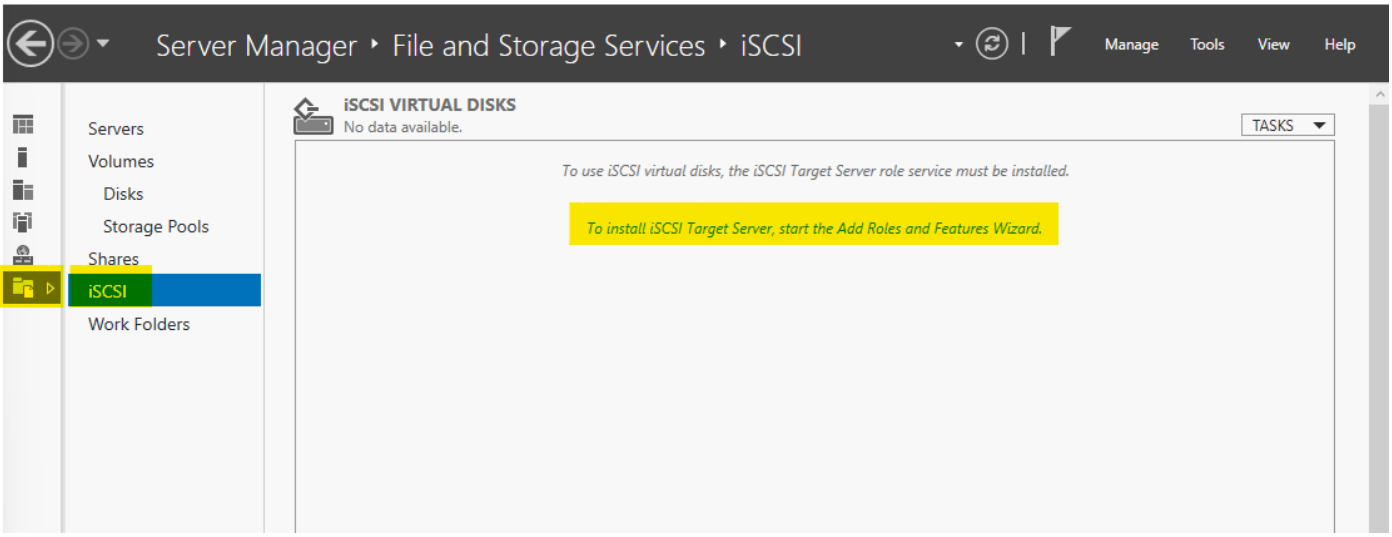
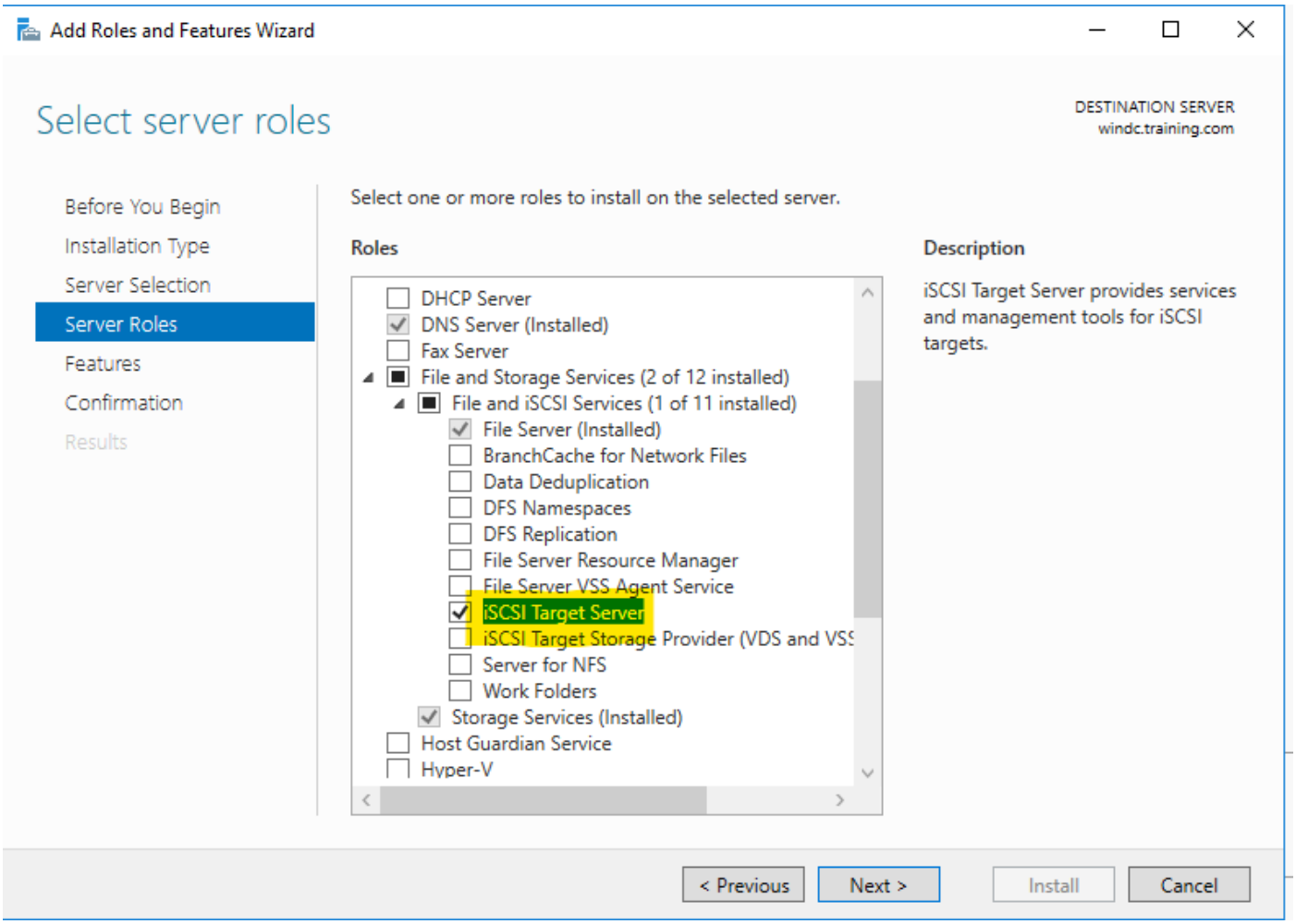
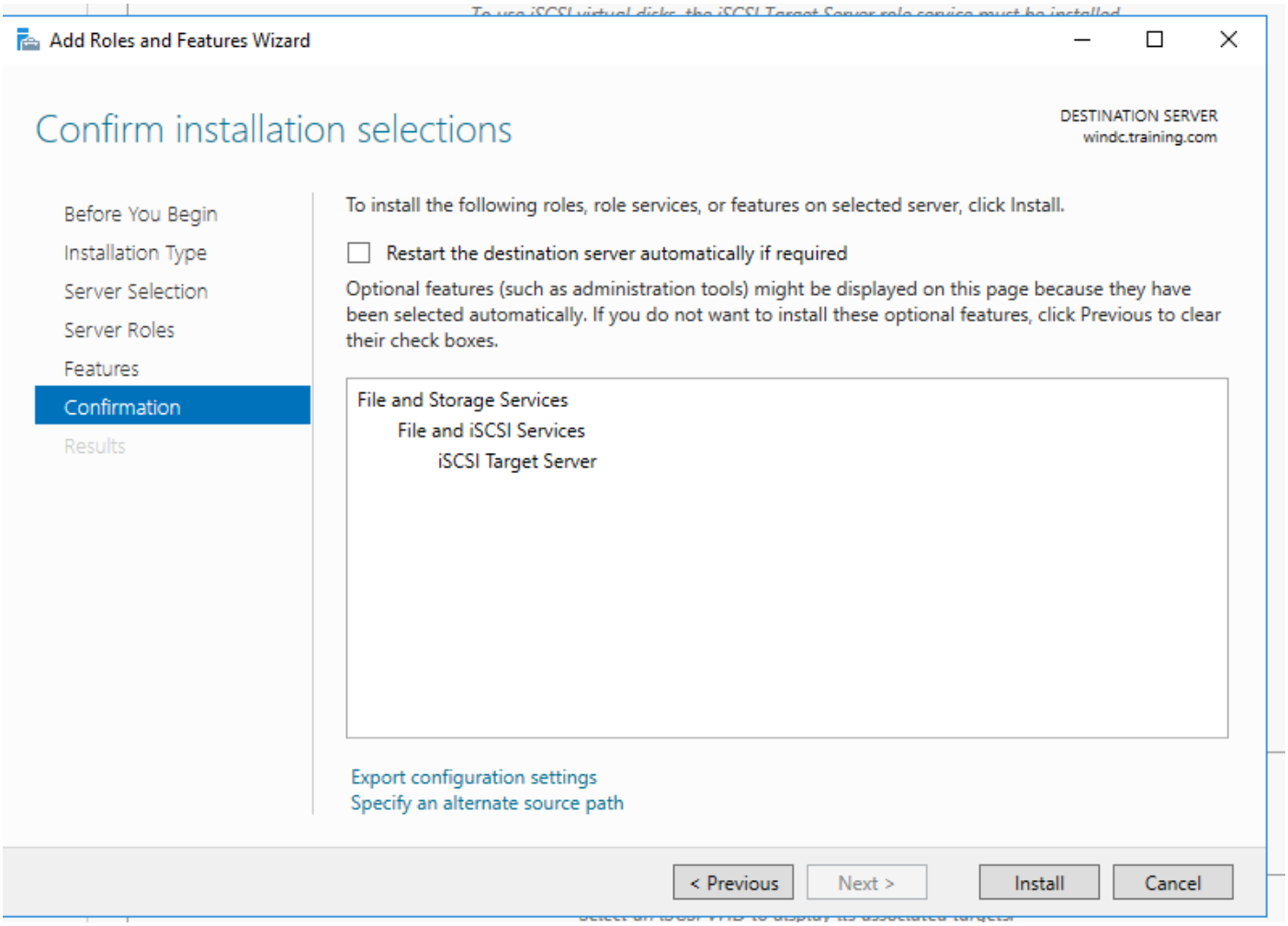
Installing iSCSI:

Installing iSCSI on DC

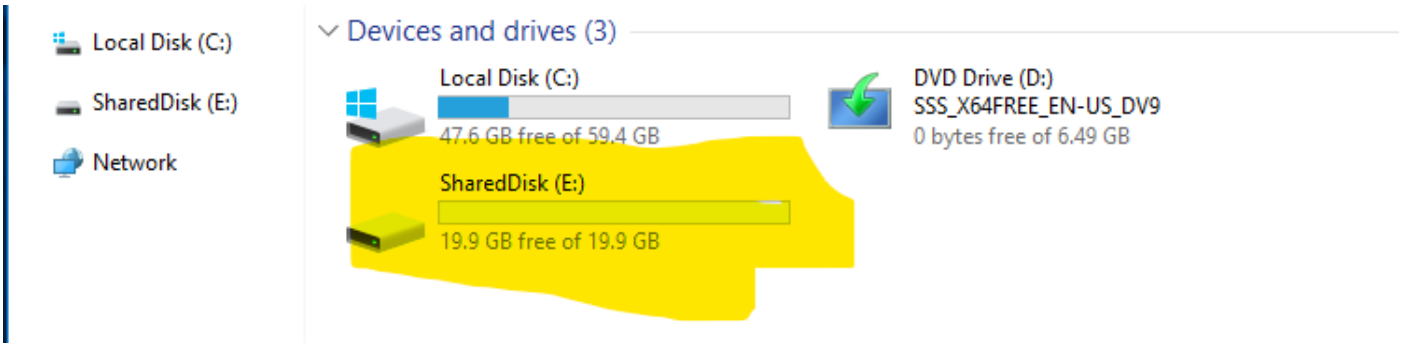




Install:

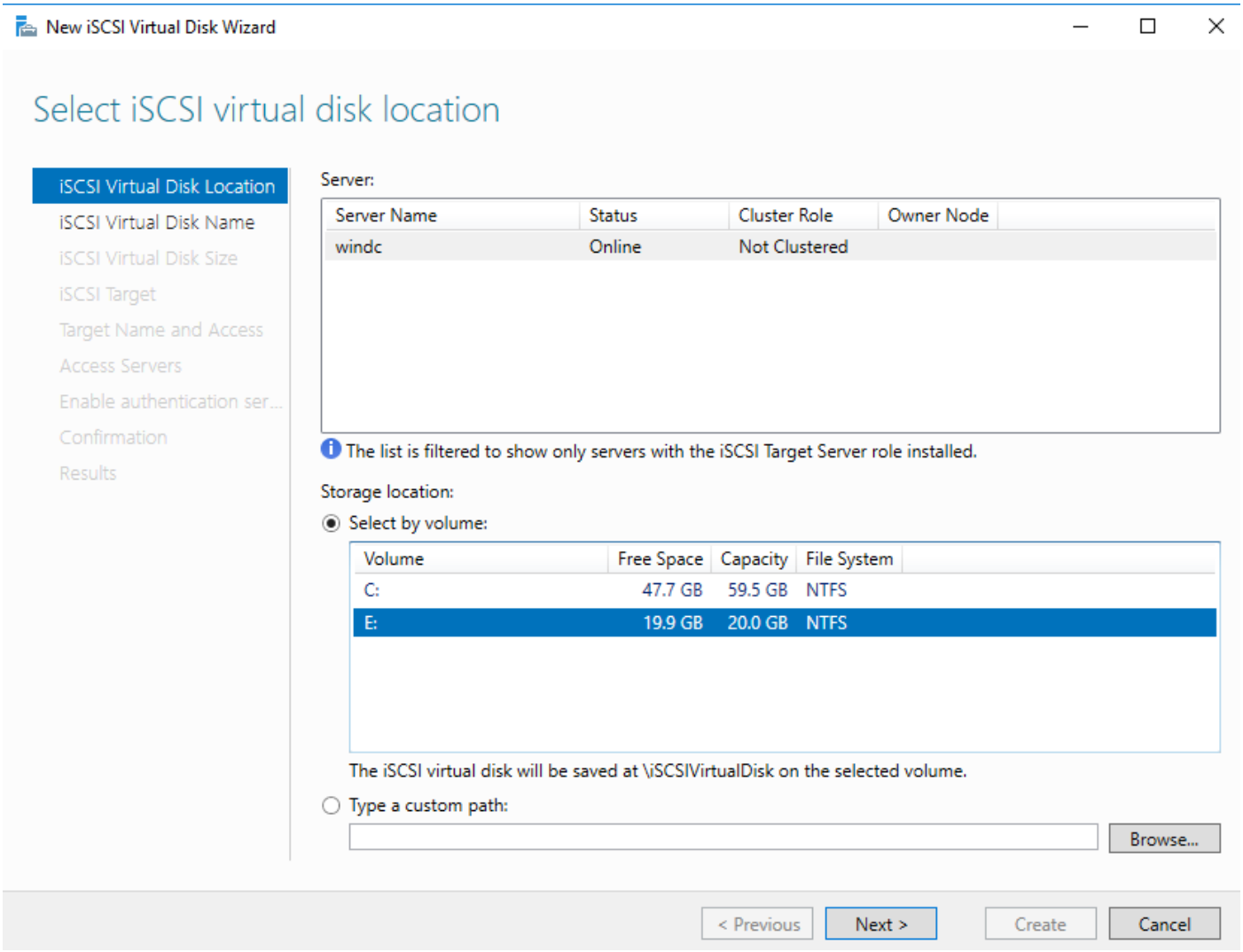


Adding a new 20GB disk:

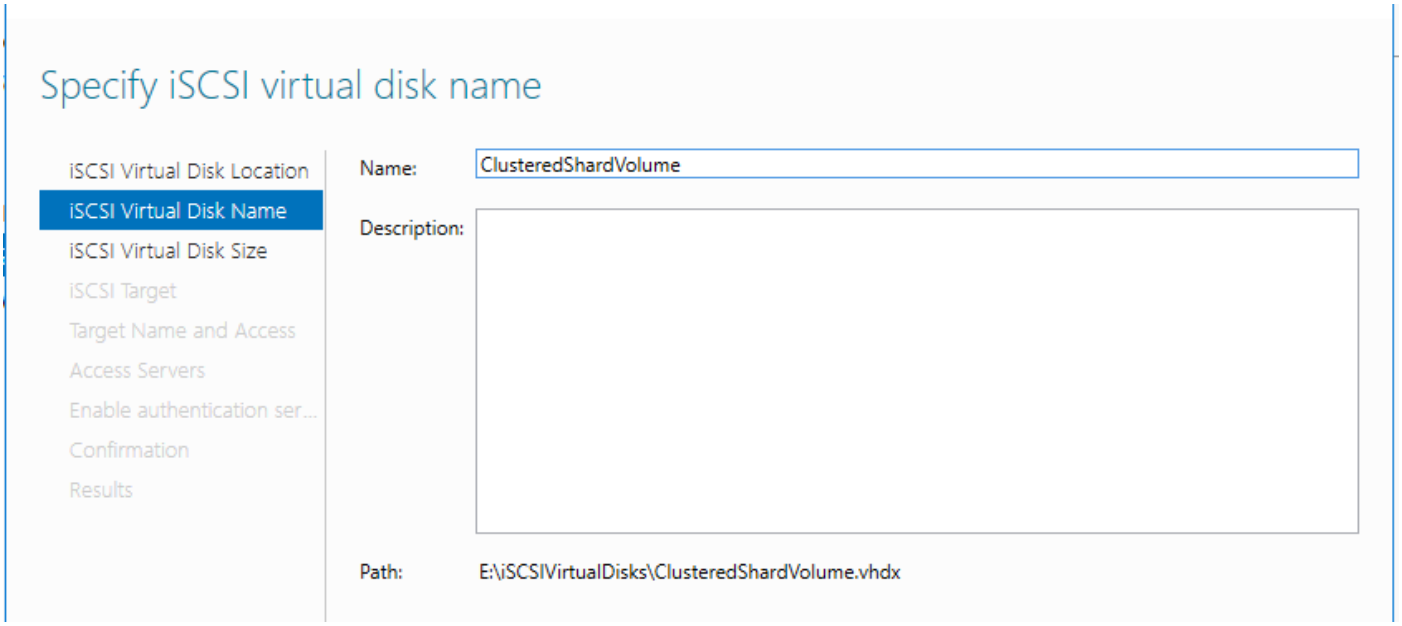


Creating iSCSI virtual disk:

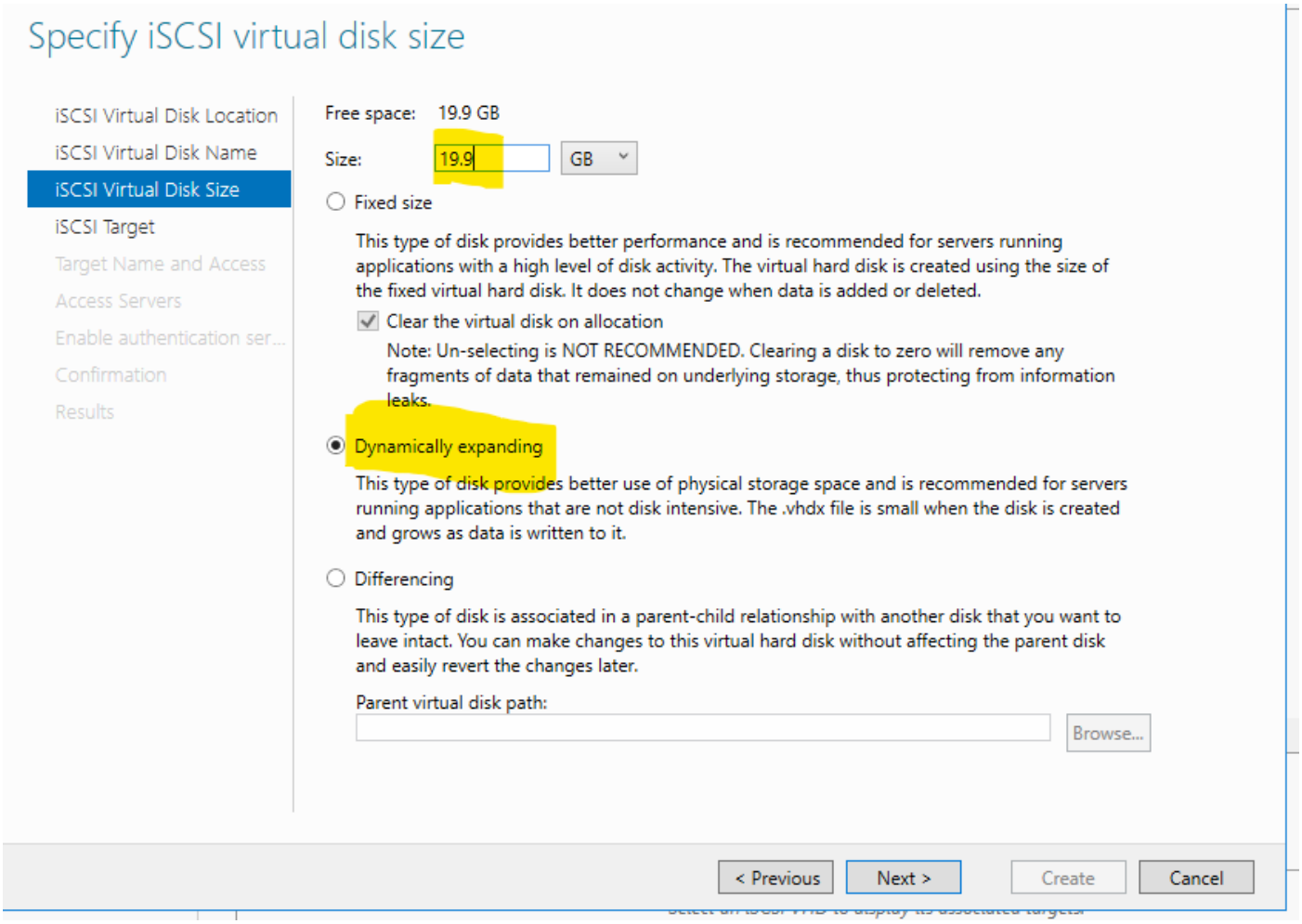
Selecting the disk:



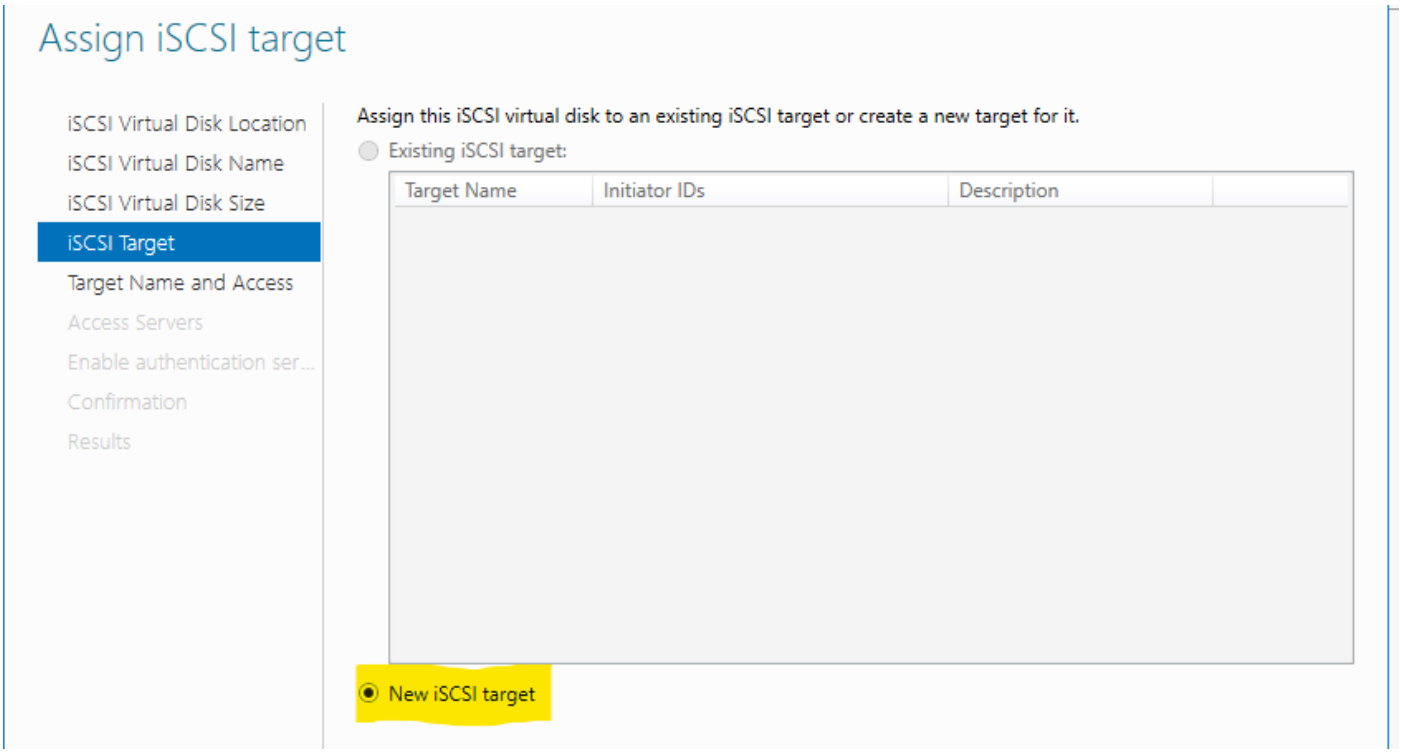
Creating a name for the volume:



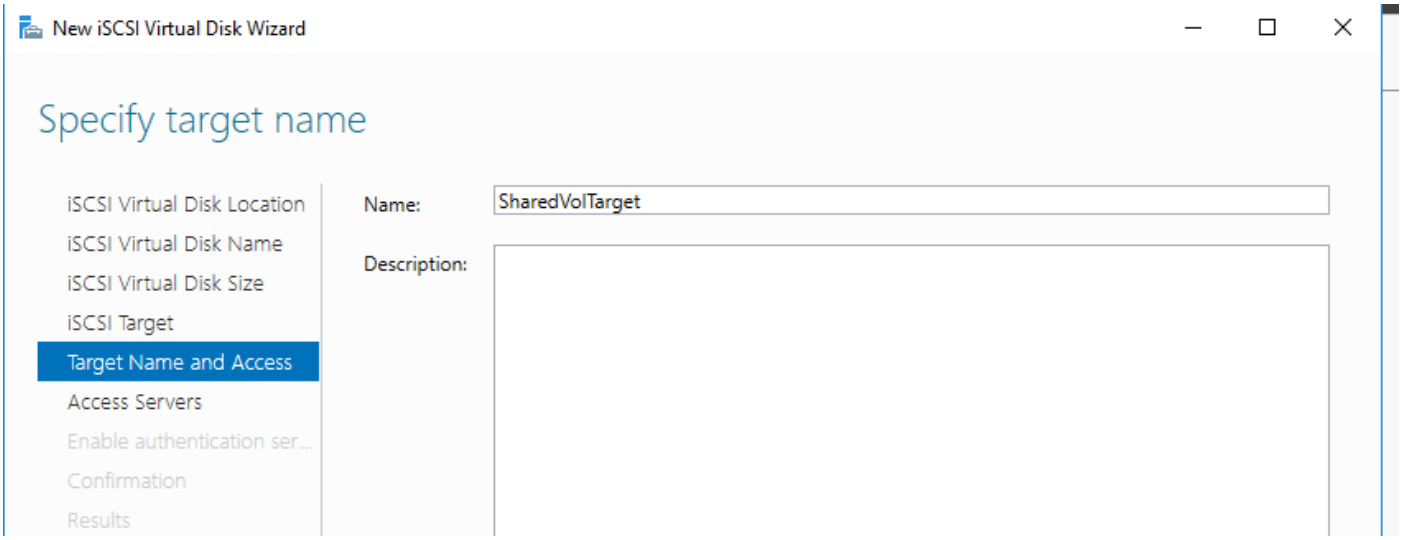
Specifying the disk type:



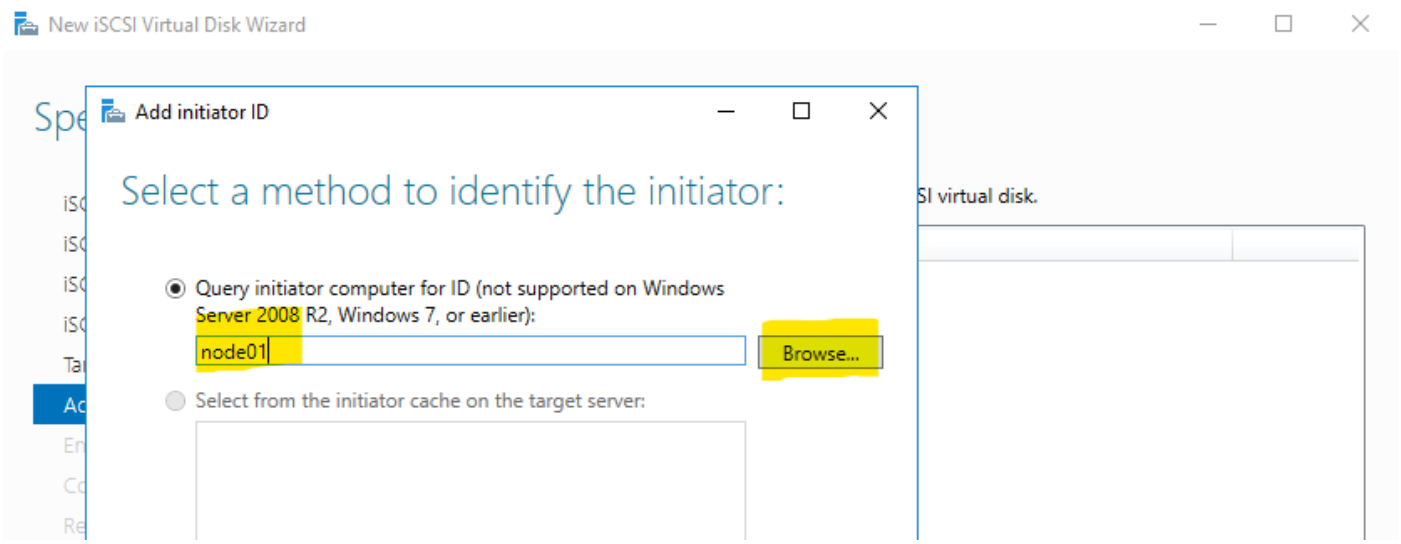
Assigning a new iSCSI target:

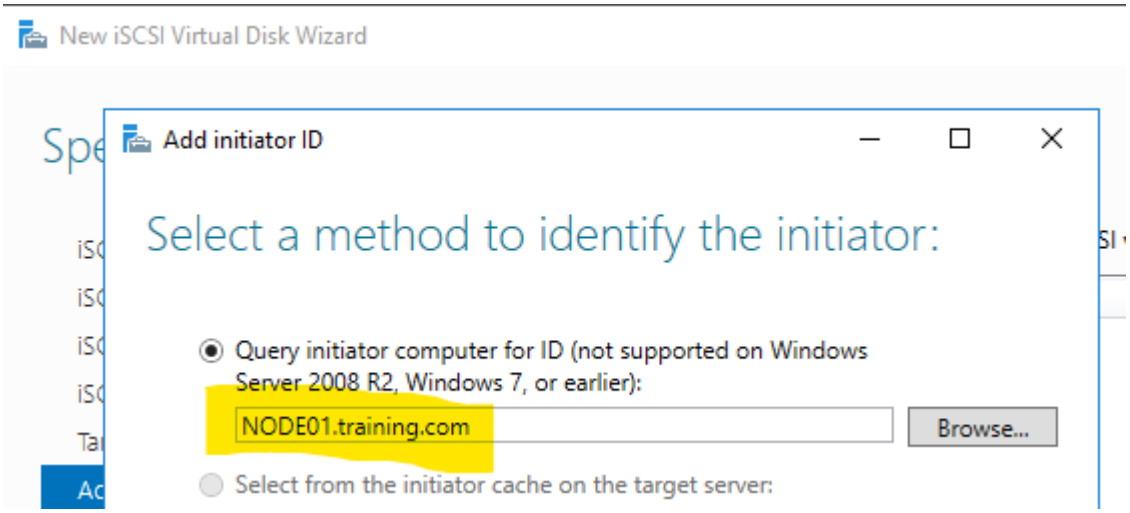


Adding target name:

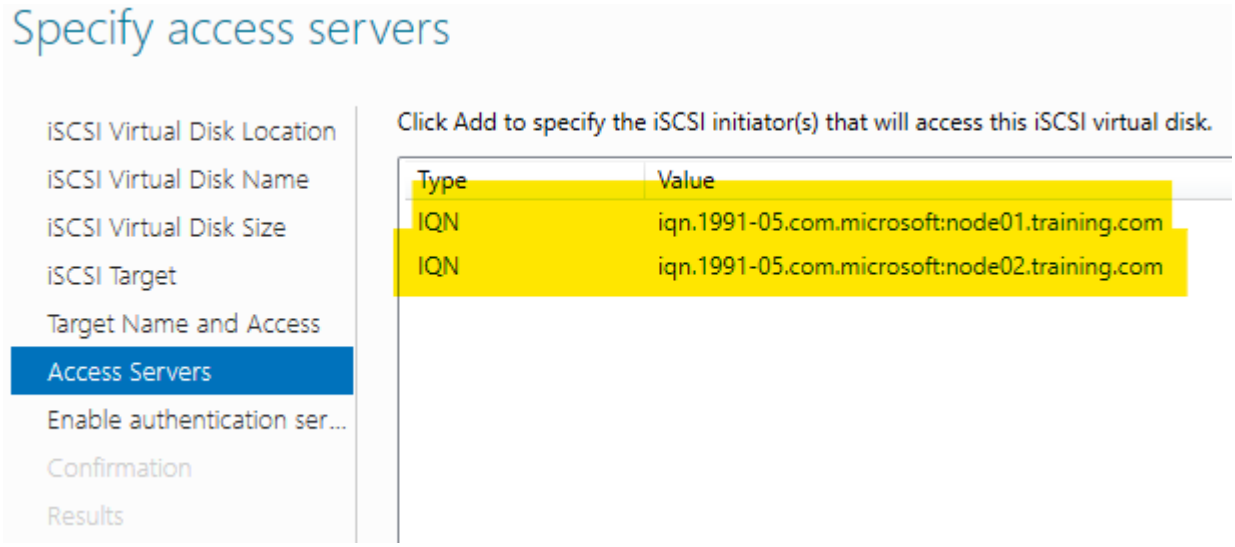


Adding access server:

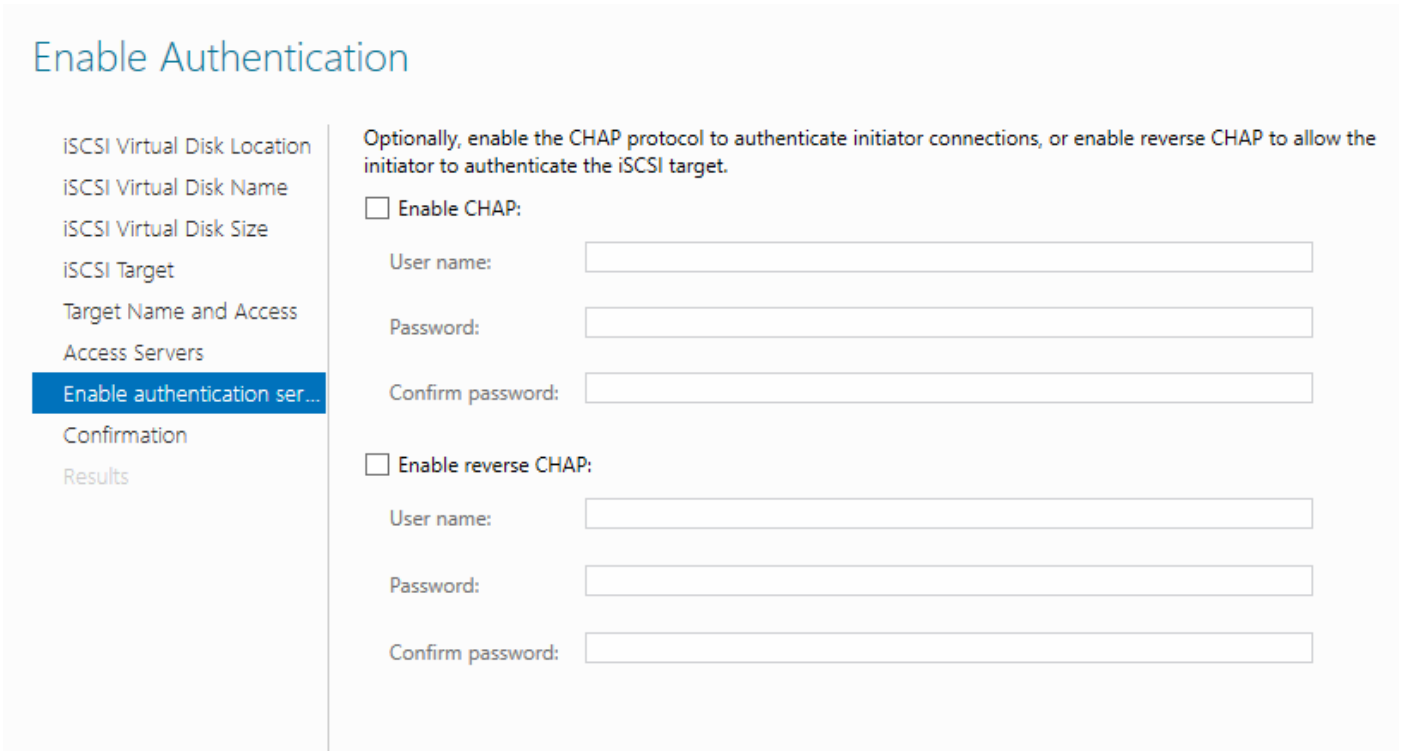




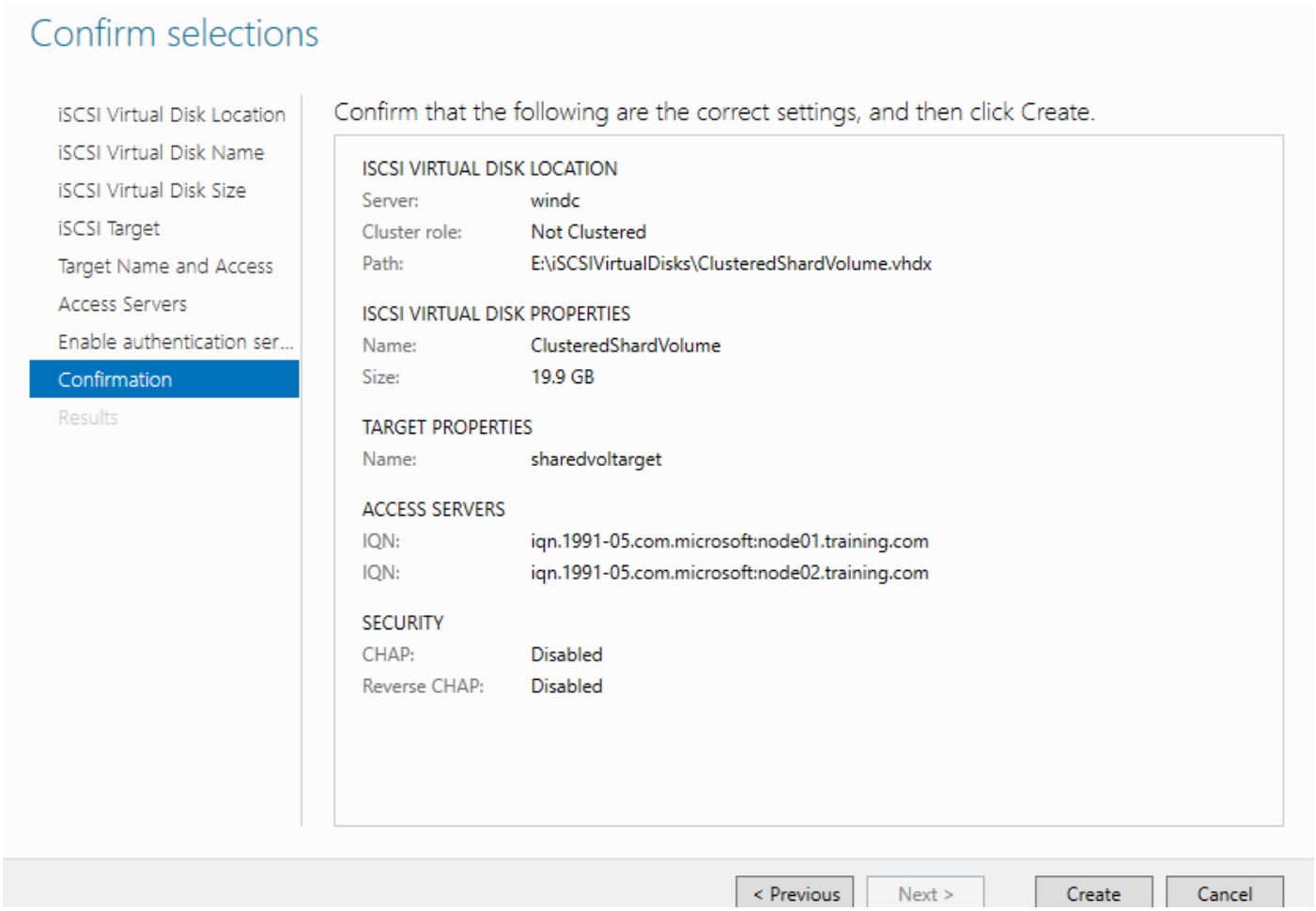
Adding both nodes:

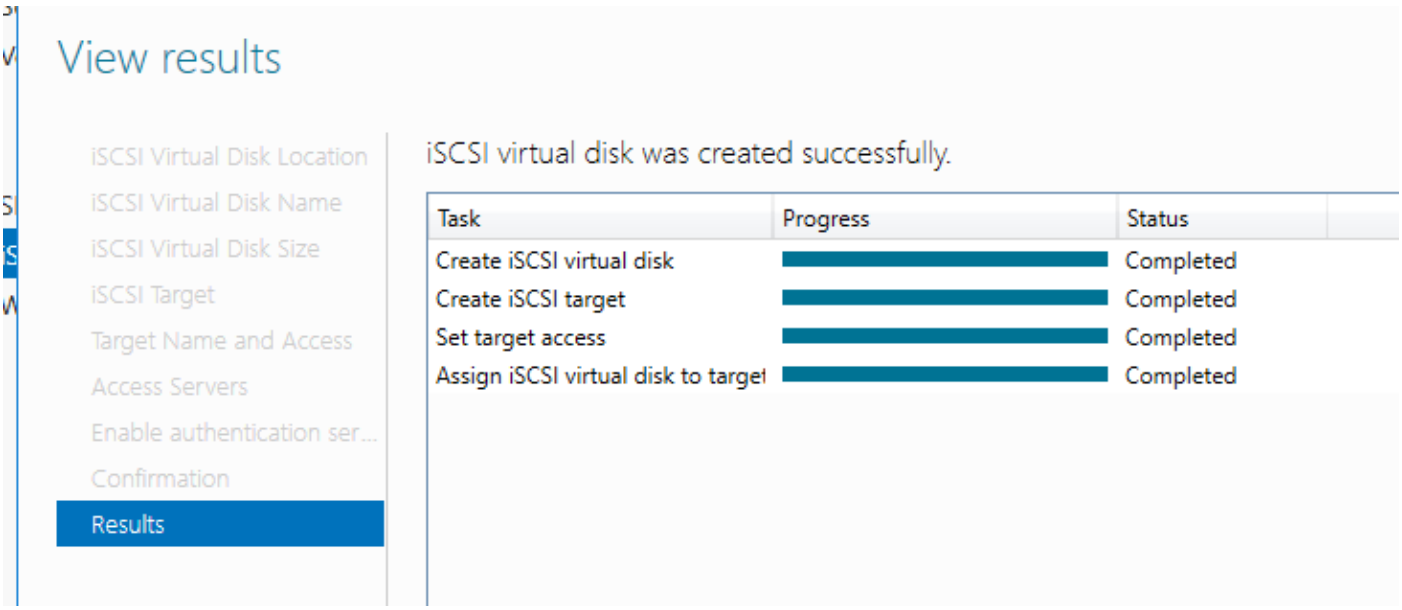


Leave CHAP:

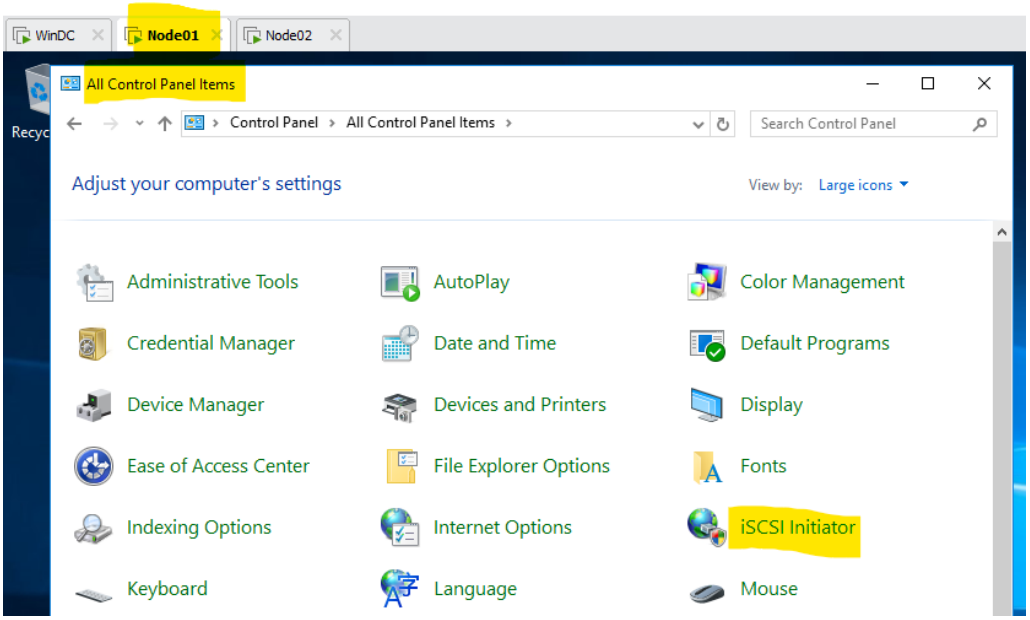


Verify:

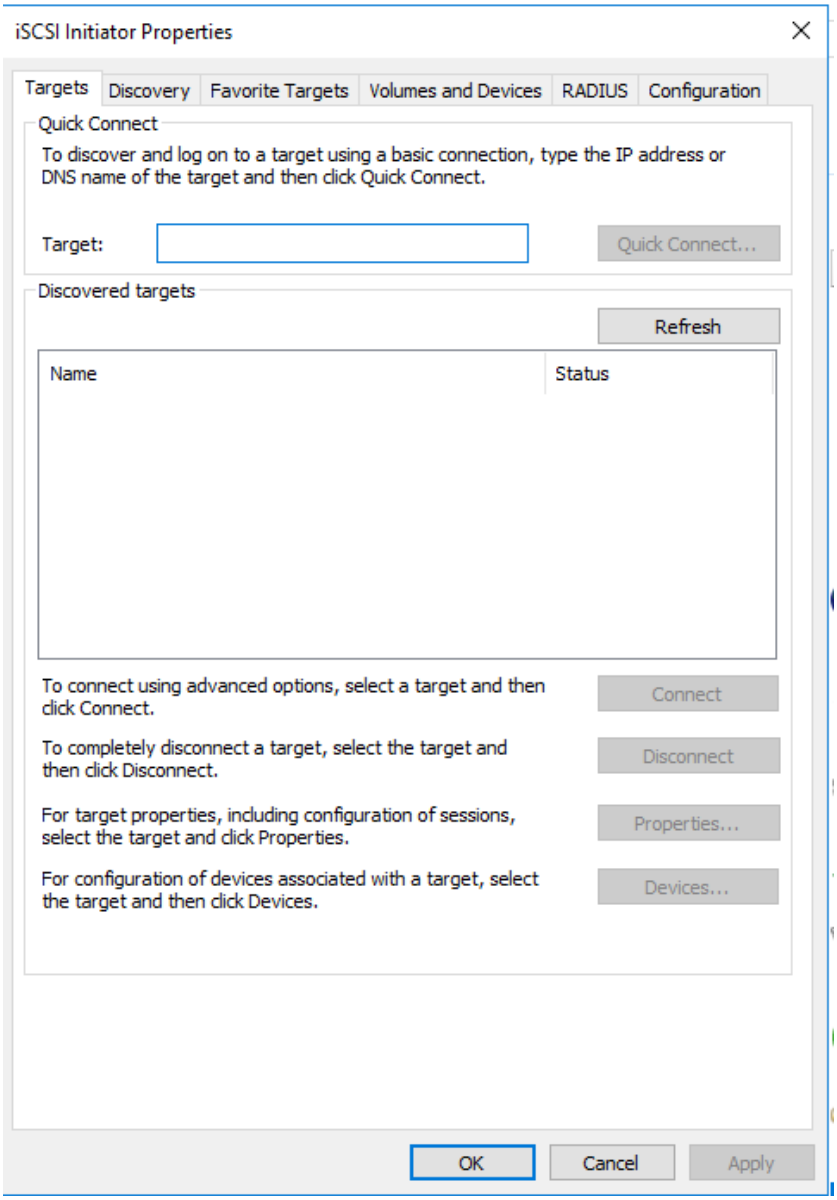

Confirm selections
iSCSI Virtual Disk Location
iSCSI Virtual Disk Name
iSCSI Virtual Disk Size
iSCSI Target
Target Name and Access
Access Servers
Enable authentication ser...
Confirmation
Results
Confirm that the following are the correct settings, and then click Create.
ISCSI VIRTUAL DISK LOCATION
Server: windc
Cluster role: Not Clustered
Path: E:\iSCSIVirtualDisks\ClusteredShardVolume.vhdx
ISCSI VIRTUAL DISK PROPERTIES
Name: ClusteredShardVolume
Size: 19.9 GB
TARGET PROPERTIES
Name: sharedvoltarget
ACCESS SERVERS
IQN: iqn.1991-05.com.microsoft:node01.training.com
IQN: iqn.1991-05.com.microsoft:node02.training.com
SECURITY
CHAP: Disabled
Reverse CHAP: Disabled
< Previous
Next >
Create
Cancel


View results
iSCSI Virtual Disk Location
iSCSI Virtual Disk Name
iSCSI Virtual Disk Size
iSCSI Target
Target Name and Access
Access Servers
Enable authentication ser...
Confirmation
Results
iSCSI virtual disk was created successfully.
Task
Progress
Status
Create iSCSI virtual disk
Completed
Create iSCSI target
Completed
Set target access
Completed
Assign iSCSI virtual disk to target
Completed

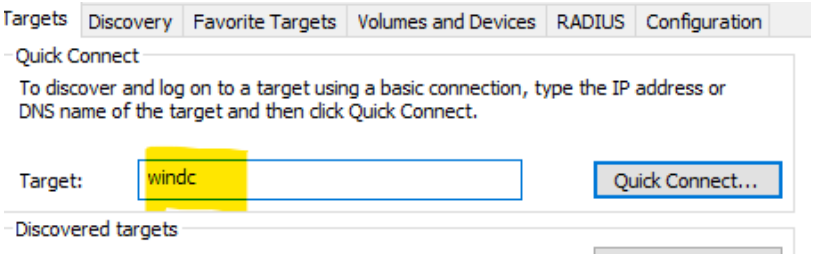
Switch to Node01 and configure iSCSI:



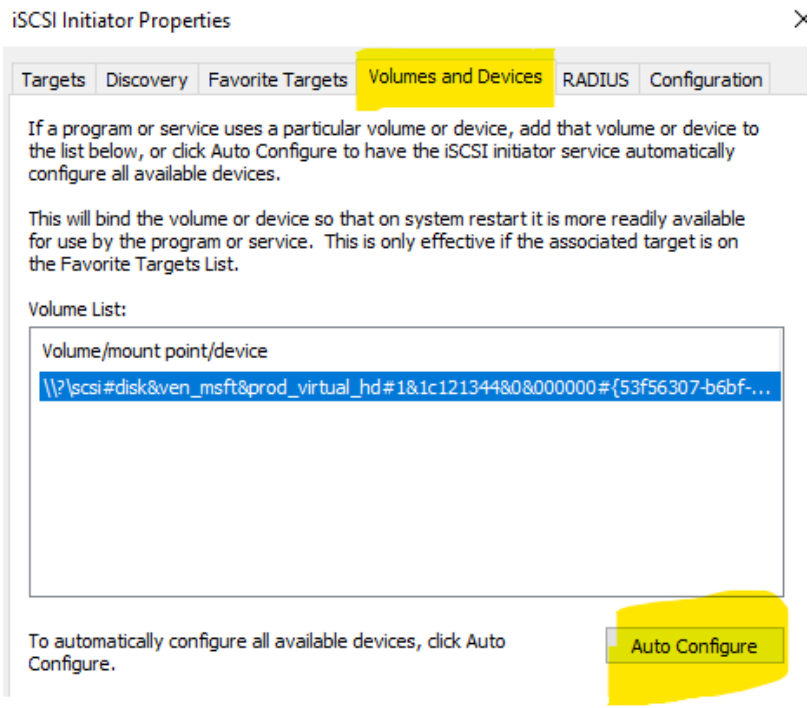
Start the service, if it shows error.



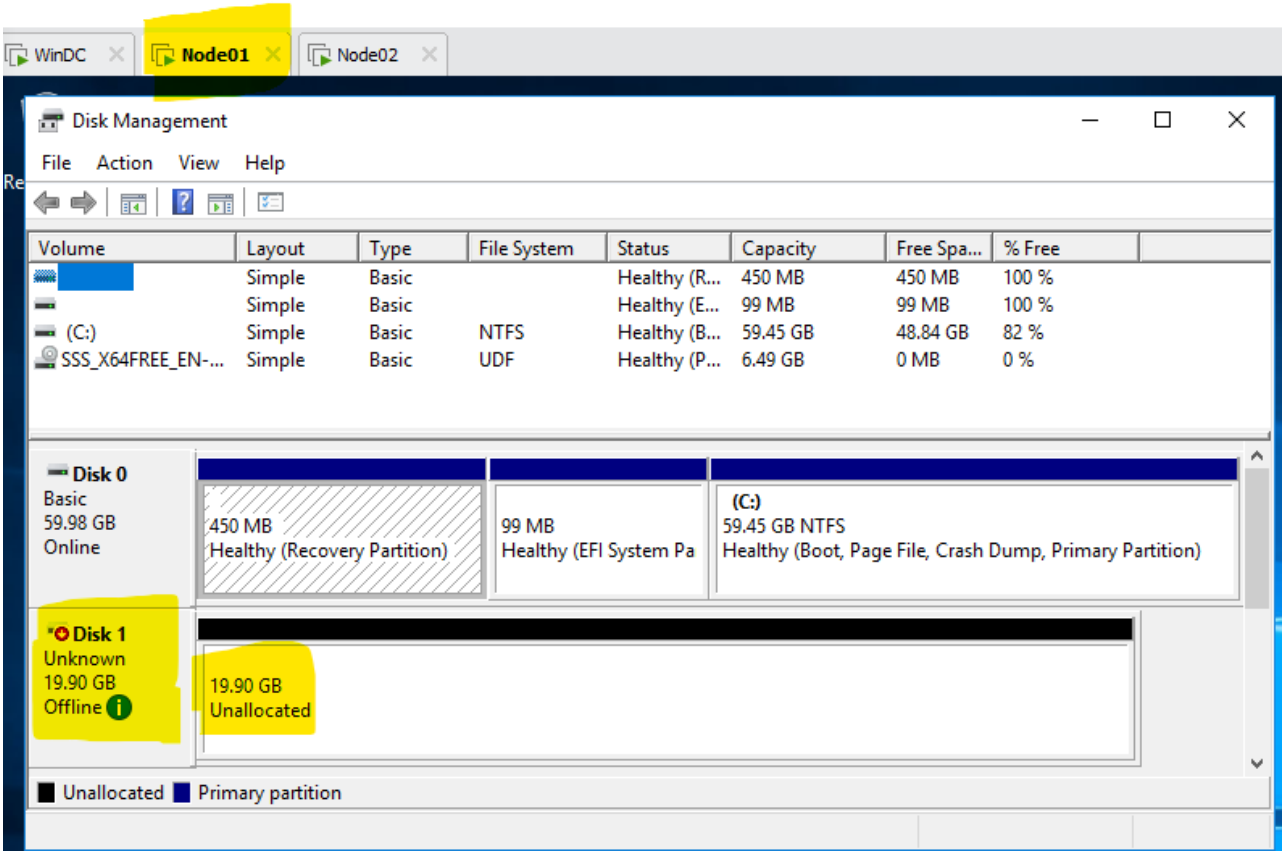
Go to target and fill the iSCSI target source on both nodes (01 & 02) & click on quick connect:



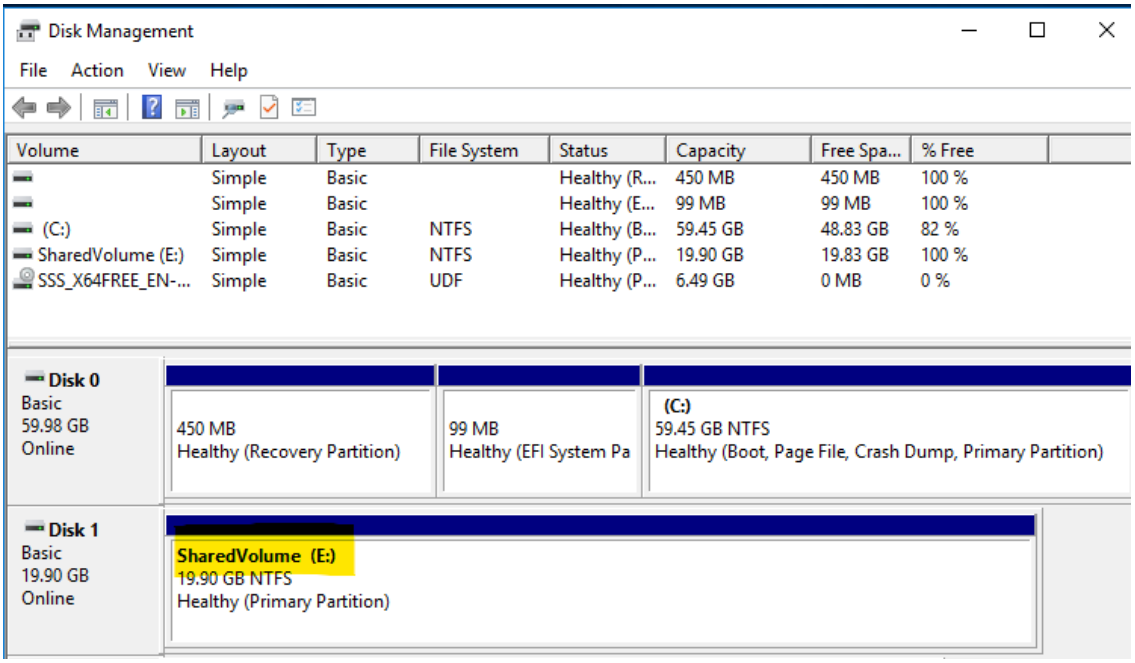
Switch volume & device tab & clock auto-configure:



Open “disk management portal” and create disk:



Just initialize the disk on Node02:



Preparation Steps for Upgrades and Migrations

1. Assessment and Planning

- Inventory existing environment (hardware, software, OS versions, roles/features).
- Identify incompatible hardware, drivers, or applications.
- Decide between:
  - *In-place upgrade* (same hardware).
  - *Migration* (new hardware or virtual platform).
- Create a detailed migration plan and timeline.
- Ensure compliance with Windows Server upgrade paths (e.g., 2012 → 2016 → 2019 → 2022).

2. Understand Upgrade/Migration Paths

- In-place upgrade: OS is upgraded on the same server.
- Migration: Data and roles moved to a new server (preferred for clean setup).
- Cluster OS Rolling Upgrade: For upgrading failover clusters with minimal downtime.
- Cross-Forest/Domain Migration: For AD, Exchange, or file services between domains.

3. Testing

- Set up a test environment that mirrors production.
- Validate applications, services, and custom scripts.
- Perform a pilot upgrade/migration on a non-critical system.

4. Backup and Recovery Planning

- Take full system and data backups (bare-metal or VSS-based).
- Document current IP configurations, DNS settings, roles.
- Validate restore procedures before beginning the upgrade.

5. Prepare the Target Environment

- Install and patch the target Windows Server version.
- Join the domain, configure roles/services.
- Ensure hardware drivers and firmware are updated.
- Install required migration tools (e.g., Windows Server Migration Tools).

6. Perform the Upgrade or Migration

- Follow a step-by-step checklist (based on role being moved).
- Use tools like:
  - Windows Server Migration Tools, Active Directory Migration Tool (ADMT), Storage Migration Service (SMS) for file servers, Hyper-V Live Migration for VMs
- Monitor logs and events closely.

7. Post-Migration Tasks

- Validate that all services, DNS, DHCP, AD replication are functioning.
- Update Group Policy Objects, scripts, monitoring tools.
- Remove old server roles and decommission gracefully.
- Communicate with stakeholders and document changes.

Useful Microsoft Tools

- Windows Server Migration Tools (WSMT)
- Microsoft Assessment and Planning Toolkit (MAP)
- ADMT (Active Directory Migration Tool), Storage Migration Service, Sysinternals Suite for diagnostics

Windows Server activation models

Windows Server supports several activation models to ensure that the operating system is genuine and properly licensed. These models vary depending on whether you're using

- retail,
- volume licensing, or
- cloud environments.

Retail Activation (MAK – Multiple Activation Key)

- Used for individually purchased Windows Server licenses.
- Each product key can be used only a limited number of times.
- Activation is done via Microsoft's activation servers.
- Ideal for: Small businesses or standalone servers.

Volume Activation (for large organizations)

Volume Activation is used in enterprise environments and includes two main methods:

- MAK (Multiple Activation Key)
  - One-time activation per device via Microsoft servers.
  - No need for continuous connectivity.
  - Best for: Dispersed or offline environments.
- KMS (Key Management Service)
  - Local server (KMS host) activates Windows clients on the network.
  - Requires minimum number of systems (25 clients or 5 servers).
  - Clients must reactivate every 180 days.
  - Best for: Large, connected enterprise networks.

Active Directory-Based Activation

- Integrates with Active Directory Domain Services (AD DS).
- Clients are activated automatically when they join the domain.
- No need to configure each machine individually.
- Activation lasts for 180 days, auto-renewed if connected to the domain.
- Best for: Domain-joined environments with Windows Server 2012 or later.

Automatic Virtual Machine Activation (AVMA)

- Used in Hyper-V environments.
- Allows VMs to activate automatically if the Hyper-V host is activated with a Datacenter edition.
- No internet or KMS/MAK needed for the VMs.
- Best for: Datacenter deployments with many VMs.

Understanding iSNS, DCB, and MPIO

What is iSCSI?

- iSCSI (Internet Small Computer System Interface)
- iSCSI is a storage networking protocol that allows data transfer over IP (TCP/IP) networks.
- It enables SCSI commands (used by traditional storage devices) to be sent over Ethernet.
- Primarily used to connect servers (initiators) to storage devices (targets) in a SAN (Storage Area Network).

Features of iSCSI

- Runs over standard Ethernet – no special hardware needed.
- Cost-effective alternative to Fibre Channel.
- Supports block-level access to storage.
- Works over existing IP infrastructure (LAN/WAN).
- Compatible with Windows, Linux, VMware, etc.

Use Cases

- Storage Area Networks (SANs) in small to medium-sized businesses.
- VMware and Hyper-V shared storage for virtual machines.
- Clustered environments where shared block storage is needed.
- Disaster recovery using iSCSI replication.

What is FCIP (Fibre Channel over IP)?

- FCIP is a protocol that tunnels Fibre Channel (FC) data over IP networks. AKA “IP Storage tunnelling”.
- Allows geographically dispersed Fibre Channel SANs to connect via standard IP networks (like the Internet or WAN).

Purpose

- To extend Fibre Channel SANs across distances using TCP/IP infrastructure.
- Enables business continuity, replication, and disaster recovery between data centres.

Use Cases

- Remote SAN extension (data center interconnect).
- Backup over long distances using existing IP networks.
- Connecting remote sites to centralized storage arrays.

Comparison with iSCSI

Feature	FCIP	iSCSI
Base Technology	Fibre Channel	SCSI over TCP/IP
Primary Use	Extending existing FC SANs	IP-based SANs
Hardware Requirement	FC switches & gateways	Ethernet + iSCSI-capable NICs
Performance	High (depends on IP network)	Moderate to high

iSNS (Internet Storage Name Service)

- Purpose:
  - Helps discover, manage, and configure iSCSI and FCIP devices in a large IP-based SAN.
- Key Features:
  - Provides naming and discovery for iSCSI targets and initiators.
  - Centralized management of iSCSI SANs.
  - Maintains a database of devices, allowing automatic updates and device status monitoring.
- Use Case:
  - Useful in large iSCSI SANs where dynamic discovery and registration of devices is needed. Not essential for small setups.

DCB (Data Center Bridging)

- To make Ethernet lossless and suitable for storage traffic (iSCSI, FCoE) in data centers.
- Ensures high reliability and zero data loss over Ethernet.
- Allows storage and data traffic to share the same network using Quality of Service (QoS).
- Critical for converged network architectures.
- Helps prevent packet drops, which can cause iSCSI session resets.

MPIO (Multipath I/O)

- To provide redundancy, high availability, and performance for storage paths.
- Maintains continuous access to storage in case of a path failure.
- Load balances I/O traffic across multiple active paths.
- Ensures fault tolerance and performance optimization.
- Essential for mission-critical applications and SAN environments.

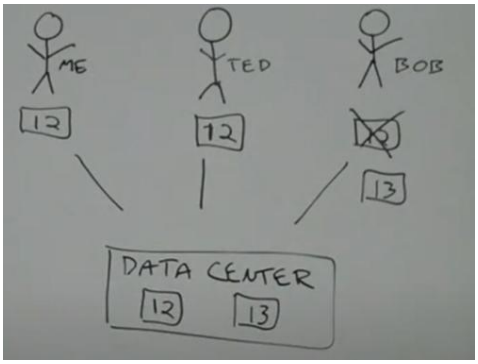
Real-World Analogy:

- **iSNS** is like a phonebook for storage—helps devices find each other.
- **DCB** is like traffic rules that give priority to important vehicles (e.g., ambulances = storage traffic).
- **MPIO** is like having multiple roads to a destination—if one road is blocked, you still get there.

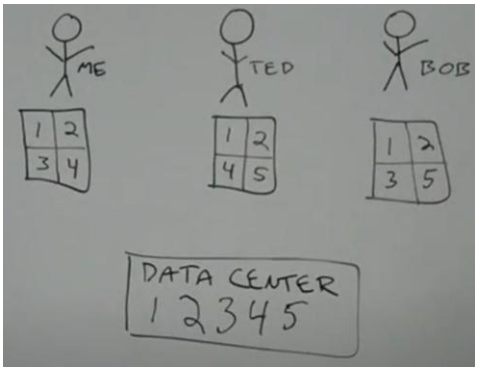
Data Deduplication in Windows Server 2016

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

Step 2: Enable on a Volume

- Using Server Manager:
- Go to File and Storage Services → Volumes
- Right-click the volume → Configure Data Deduplication
- Choose usage type (e.g., General Purpose File Server)
- Set deduplication schedule and minimum file age (default: 3 days)

Step 3: Monitor and Manage

Check status: Get-DedupStatus

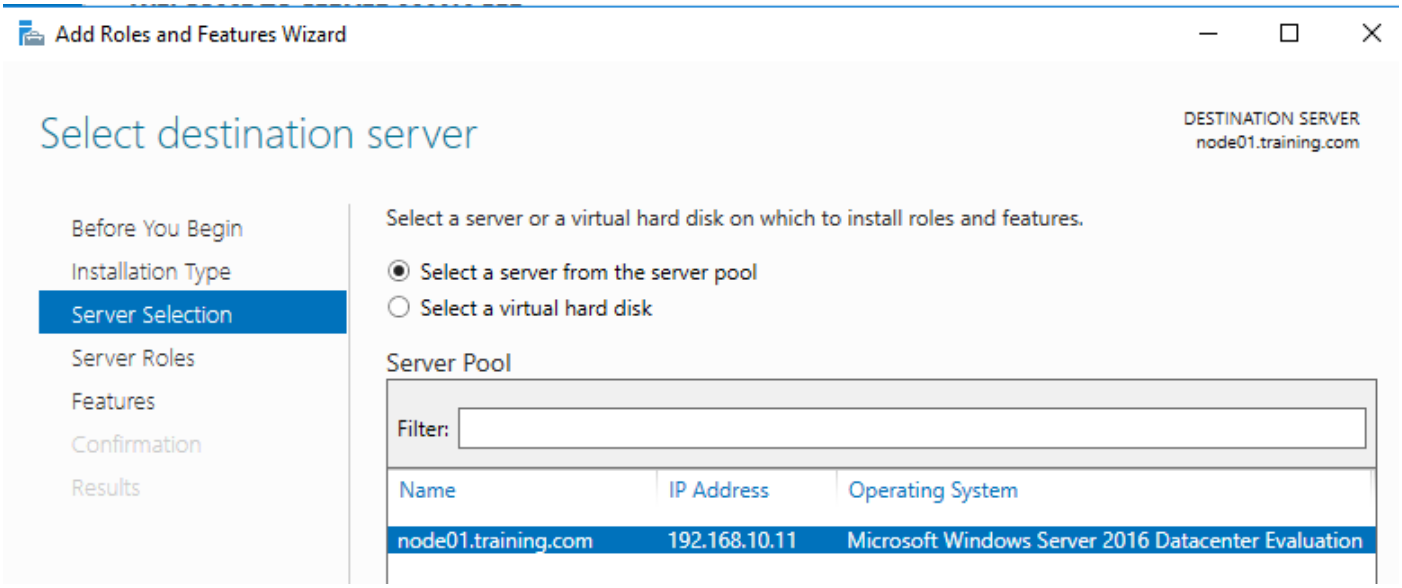
Start deduplication job manually:

```
Start-DedupJob -Volume "D:" -Type Optimization
```

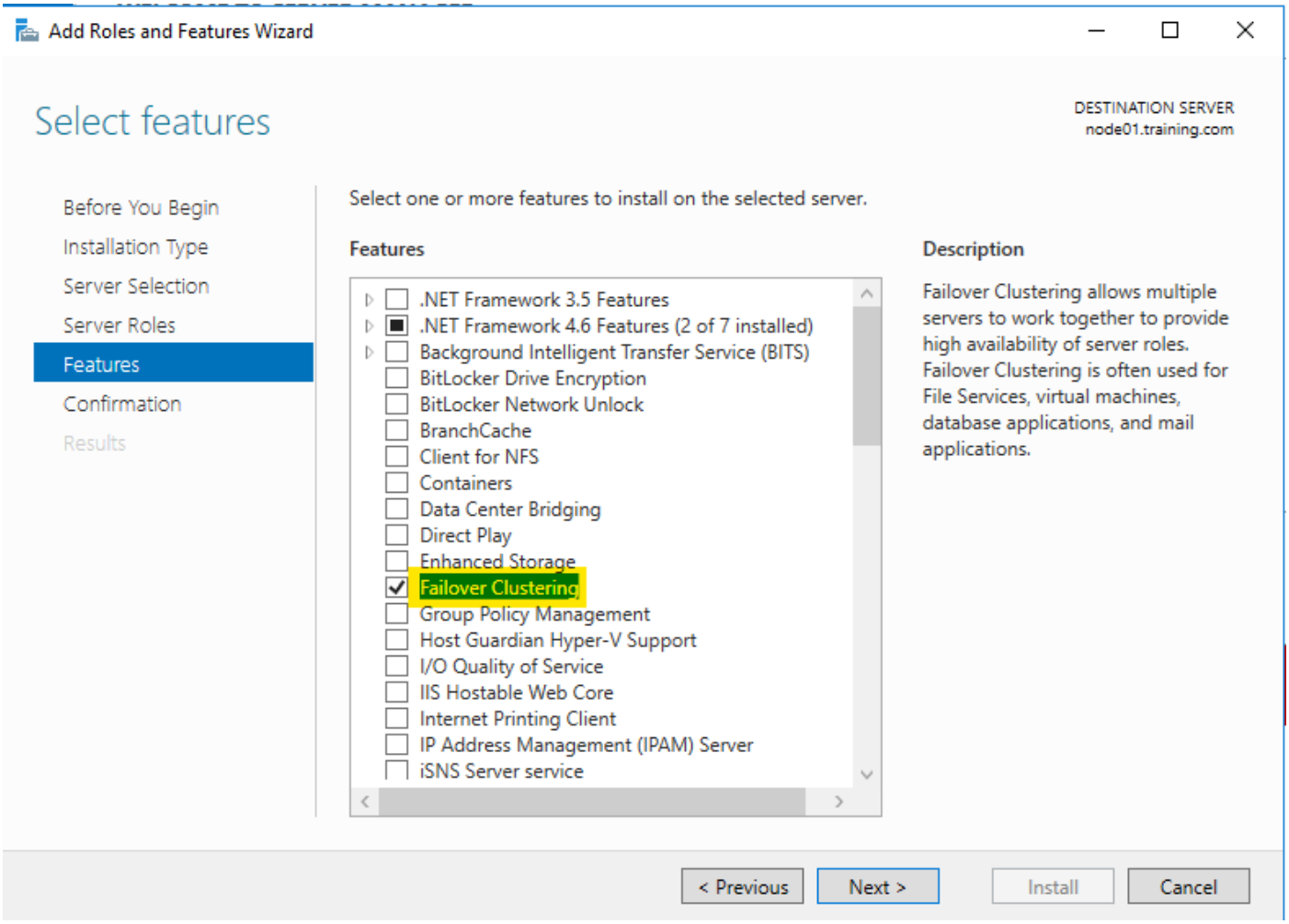
Install failover cluster role on both Node 1 & 2

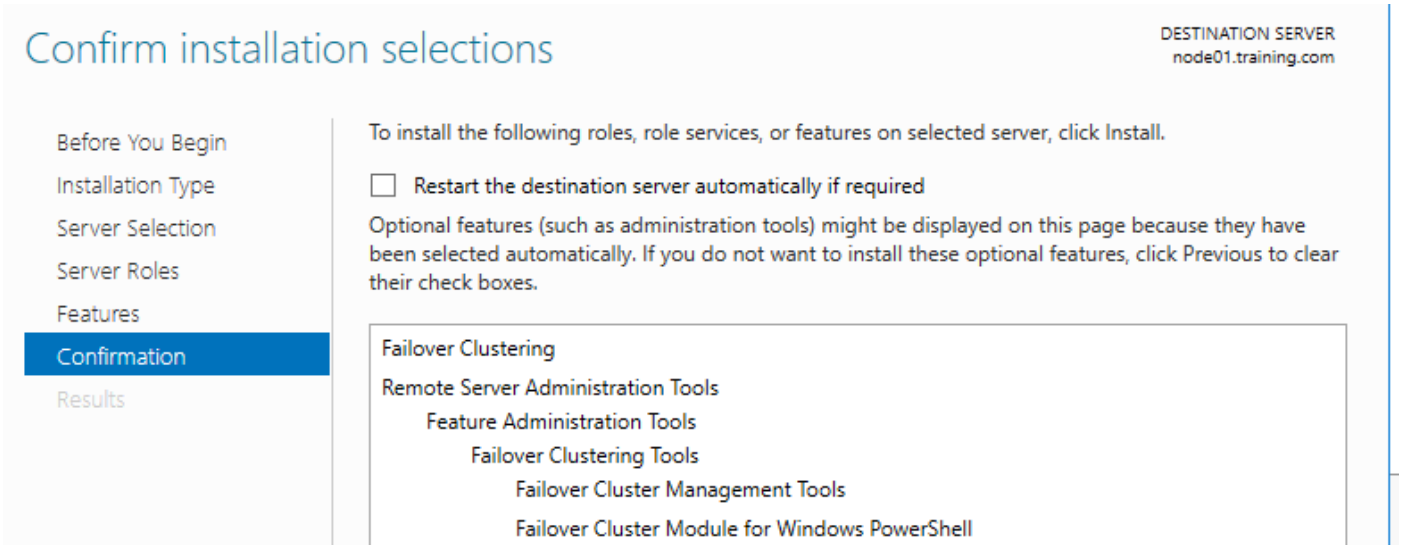
TAKE SNAPSHOT for all 3 VMS

Node01:

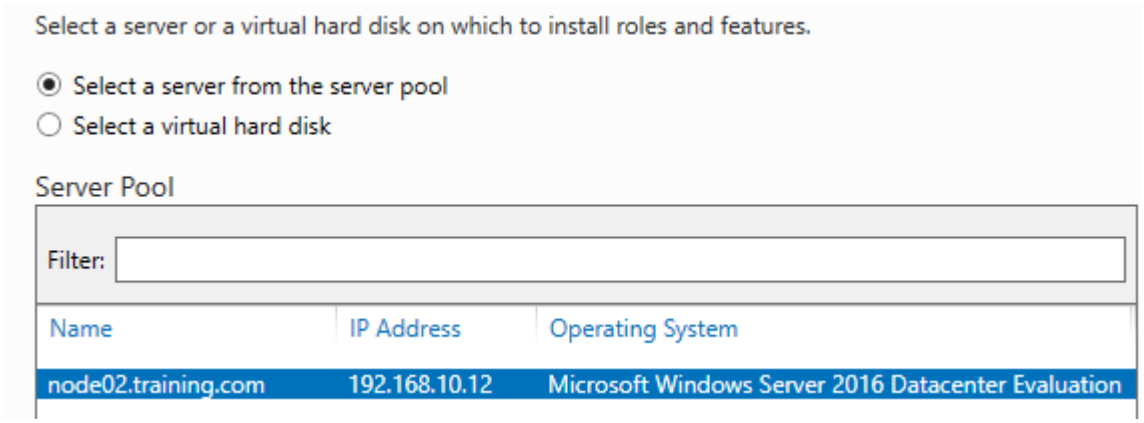


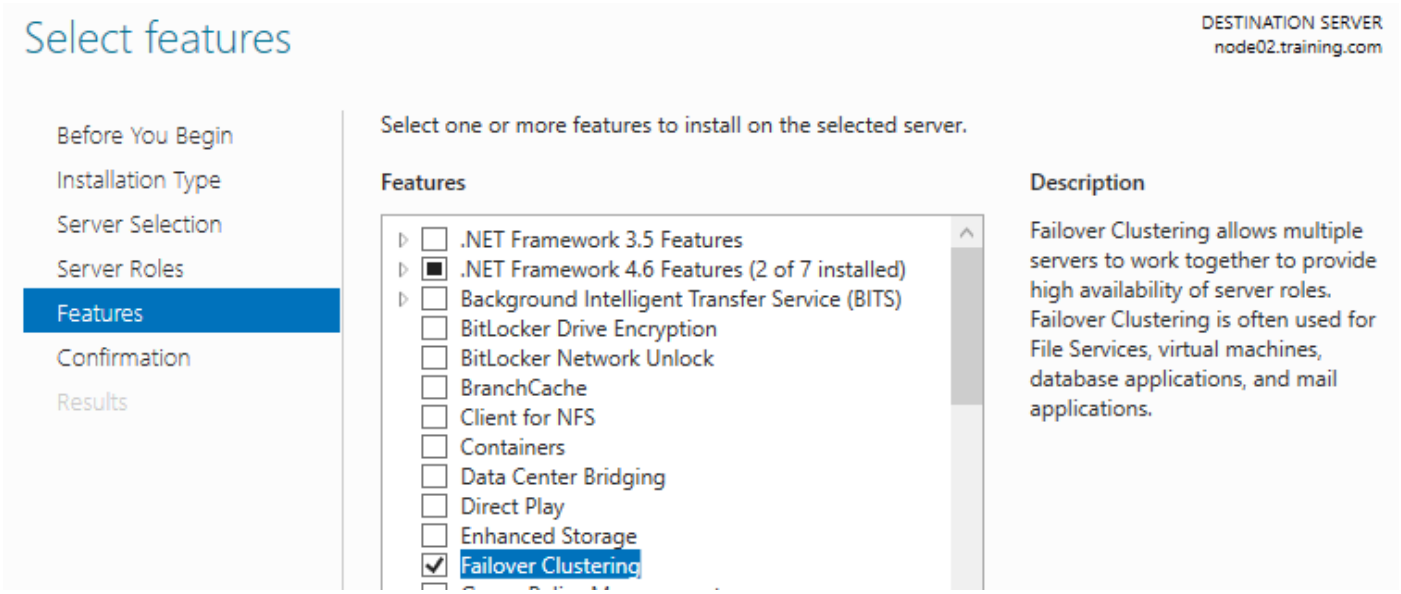
Installing feature:





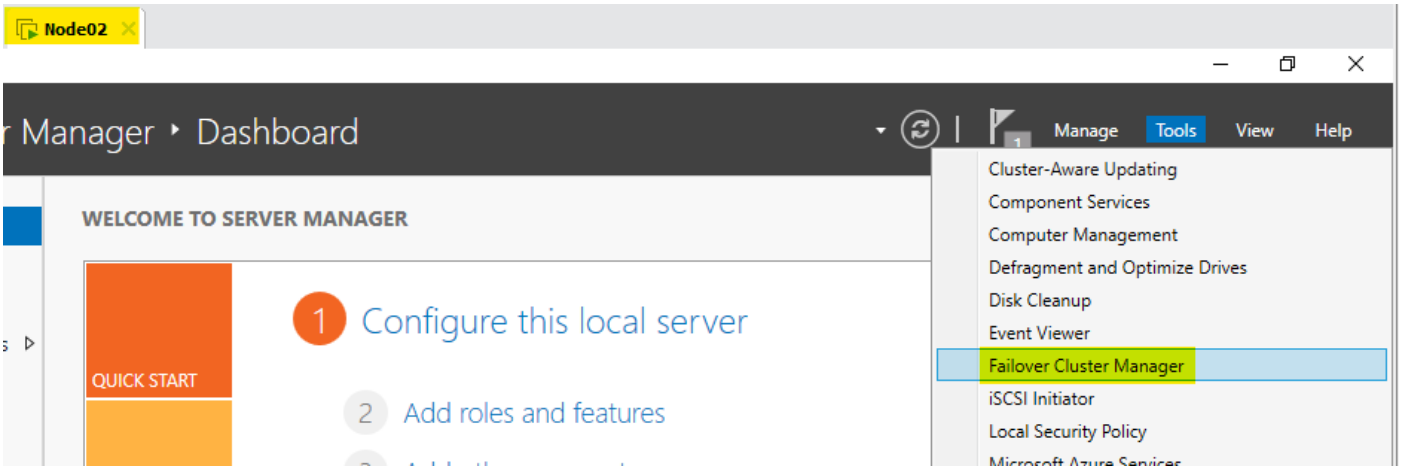
Performing the same on Node02:



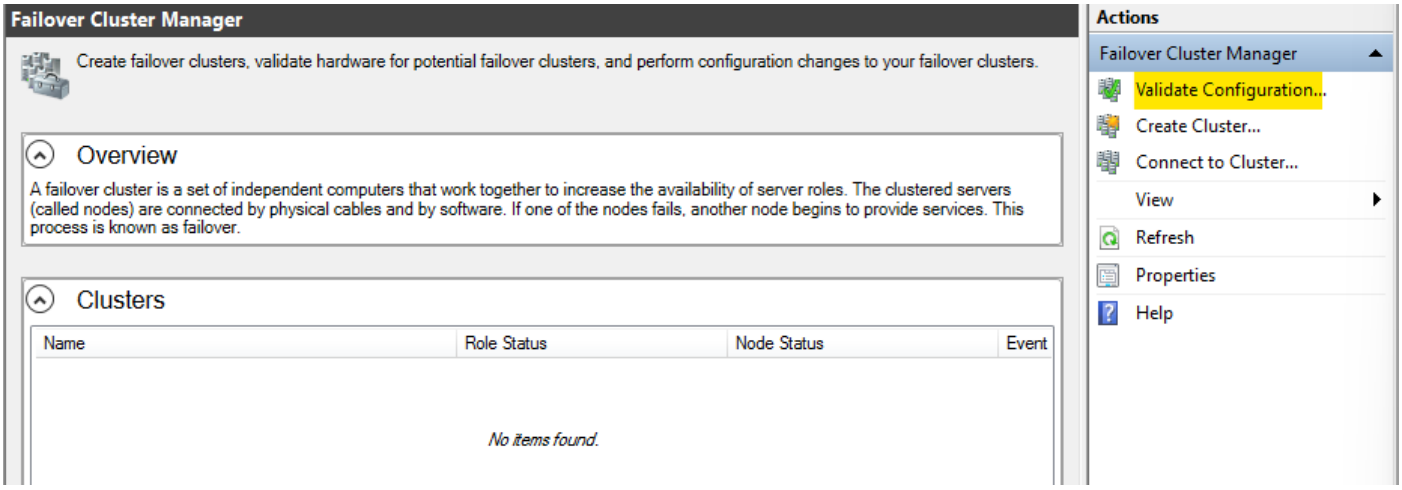


Testing the failover clustering:

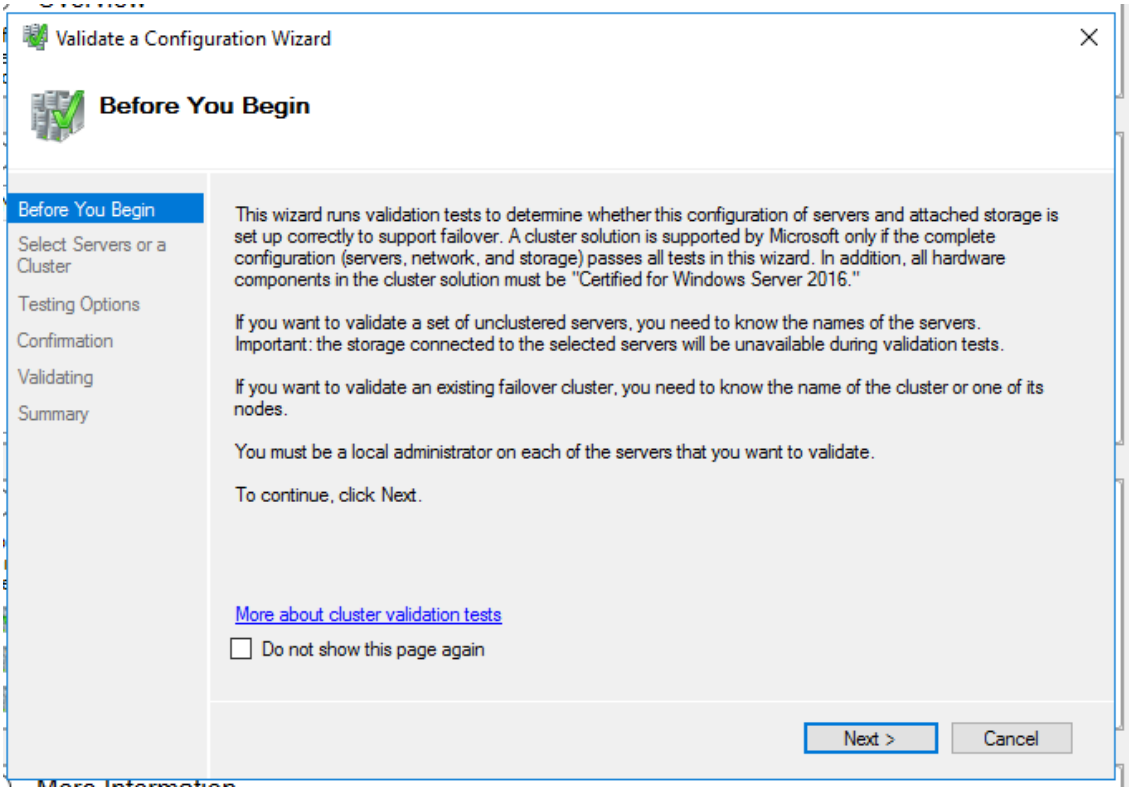
Switch to dashboard page → tools



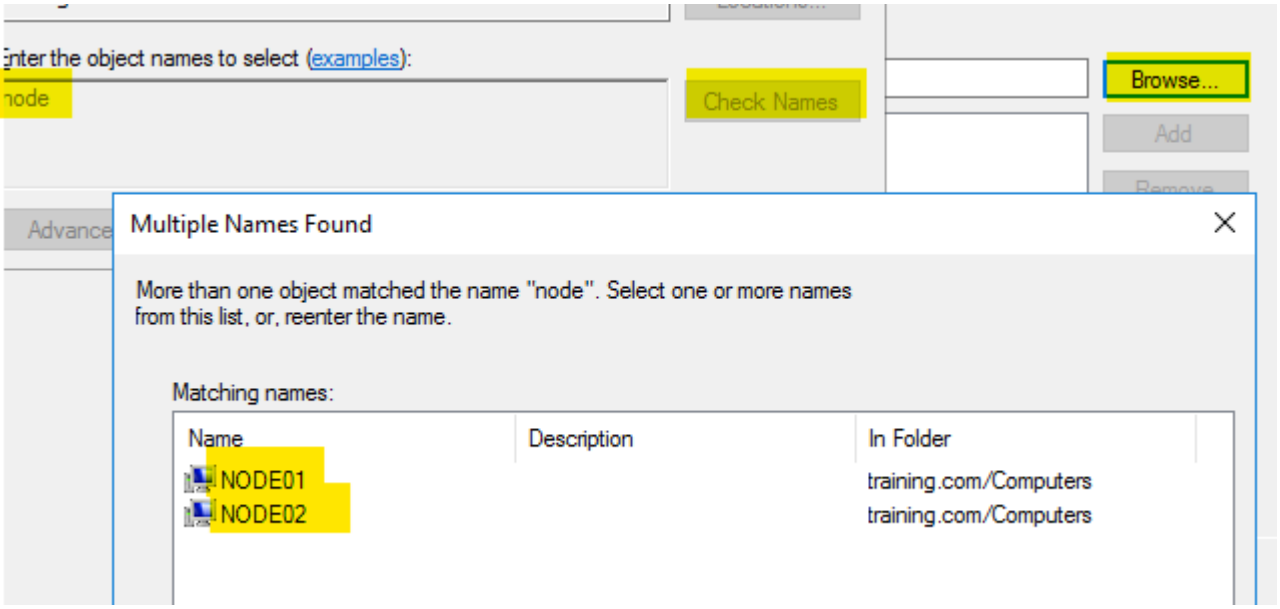
Validating configuration:

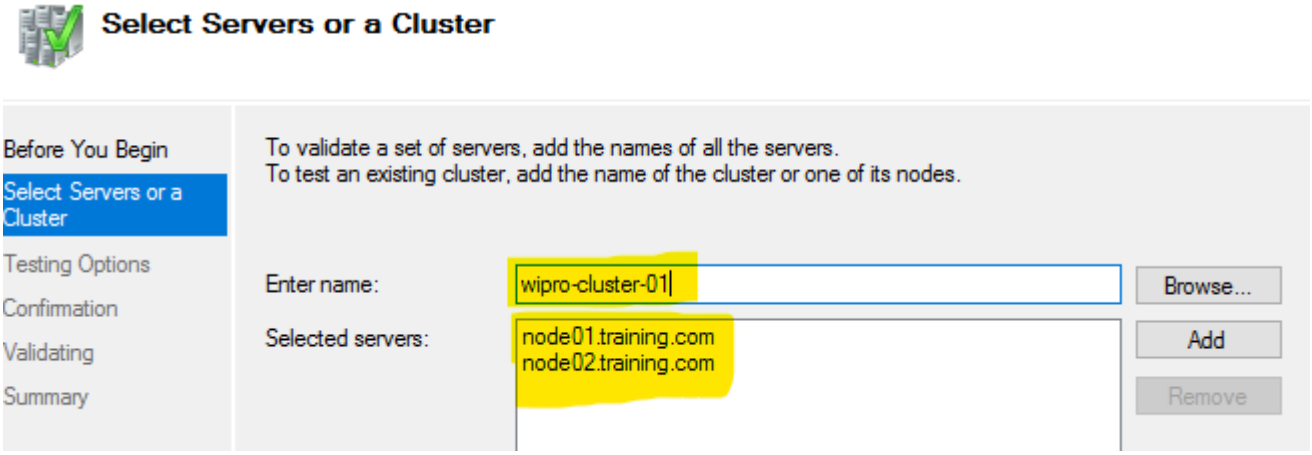


Click on Next on “before you begin”:

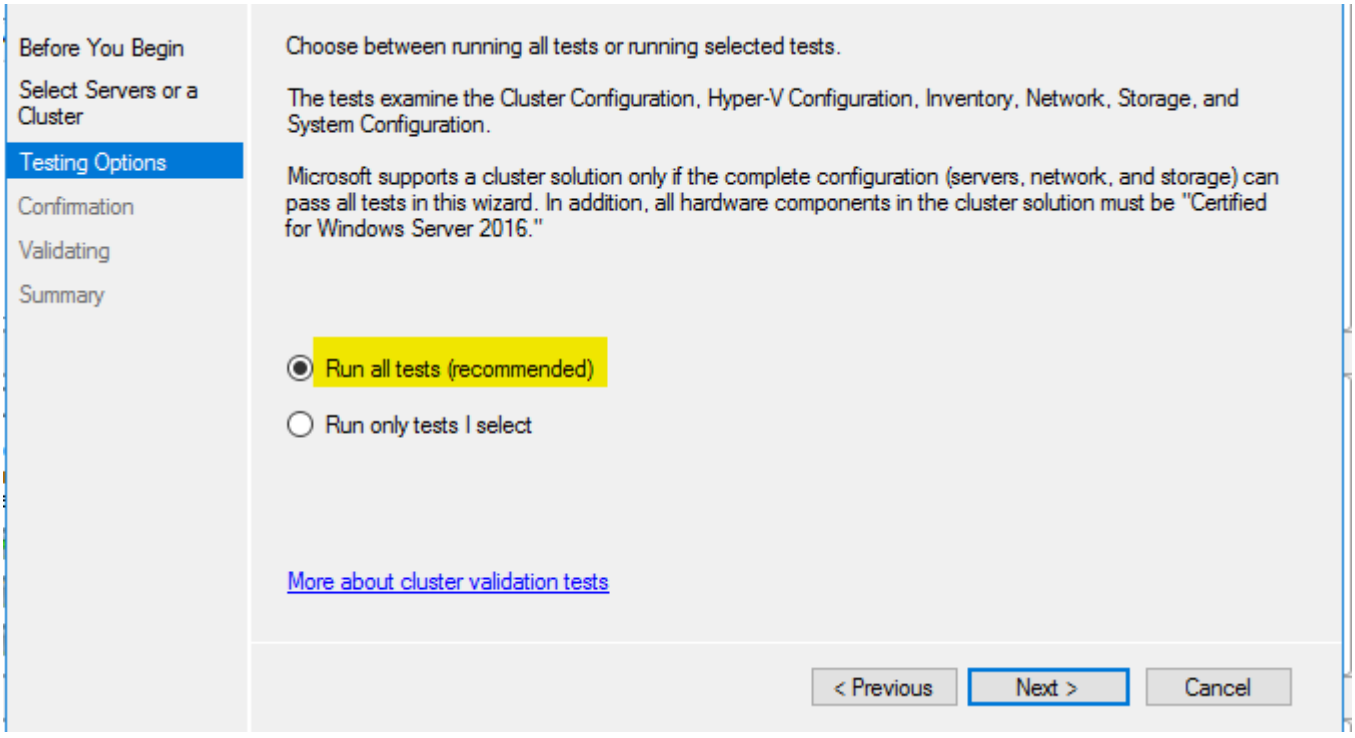


Select servers or a cluster: (browse)

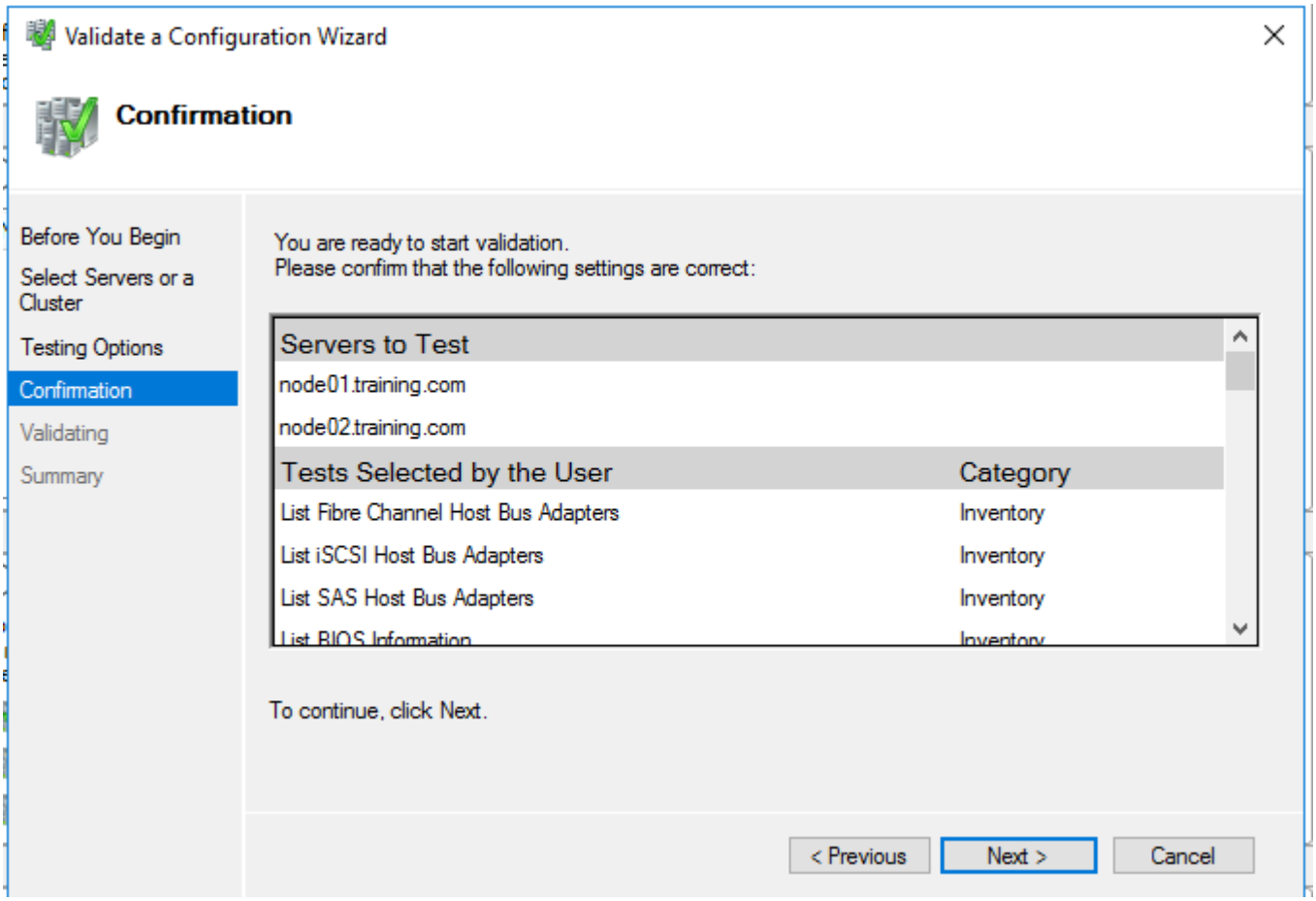




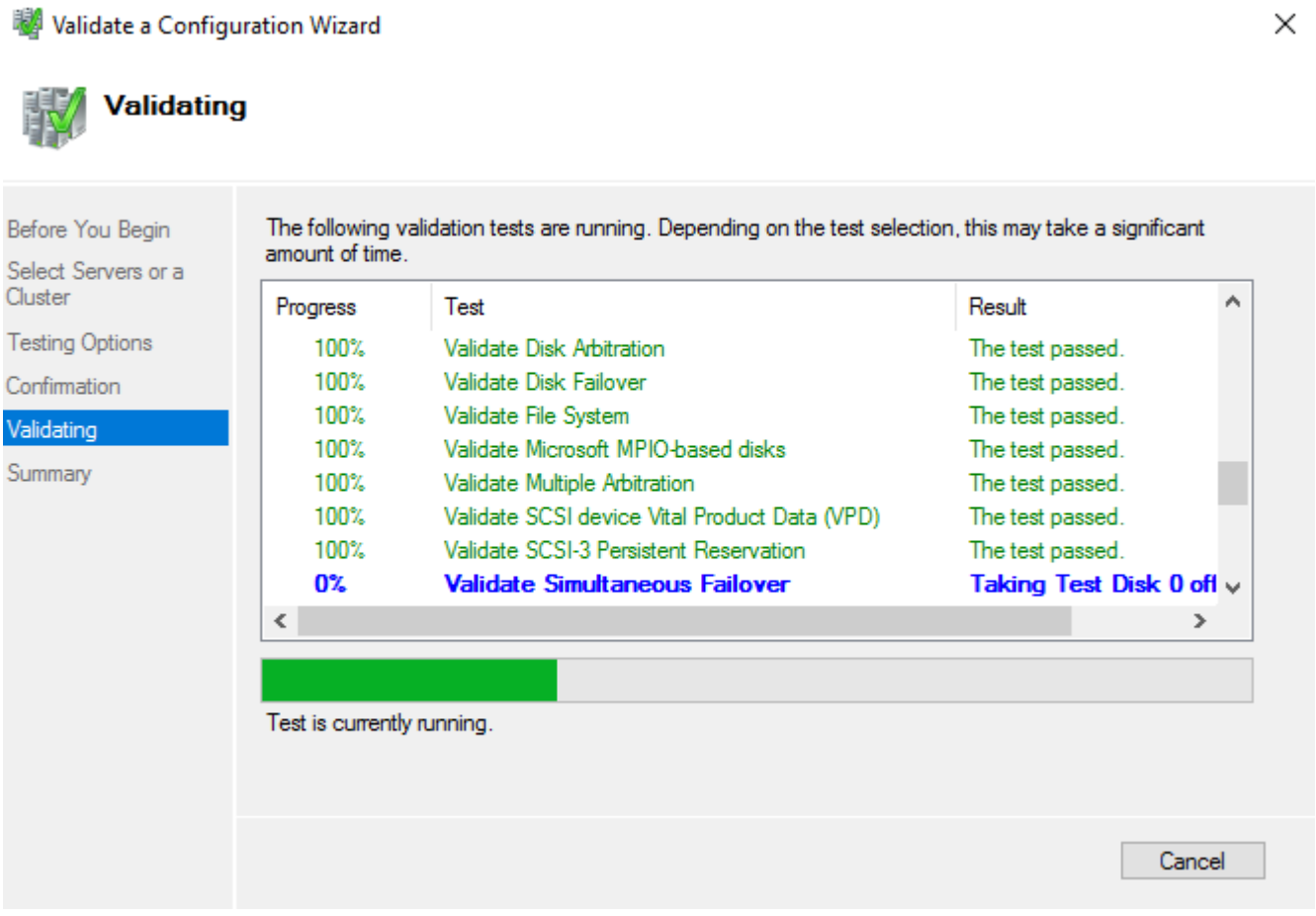
Testing option → Running all tests

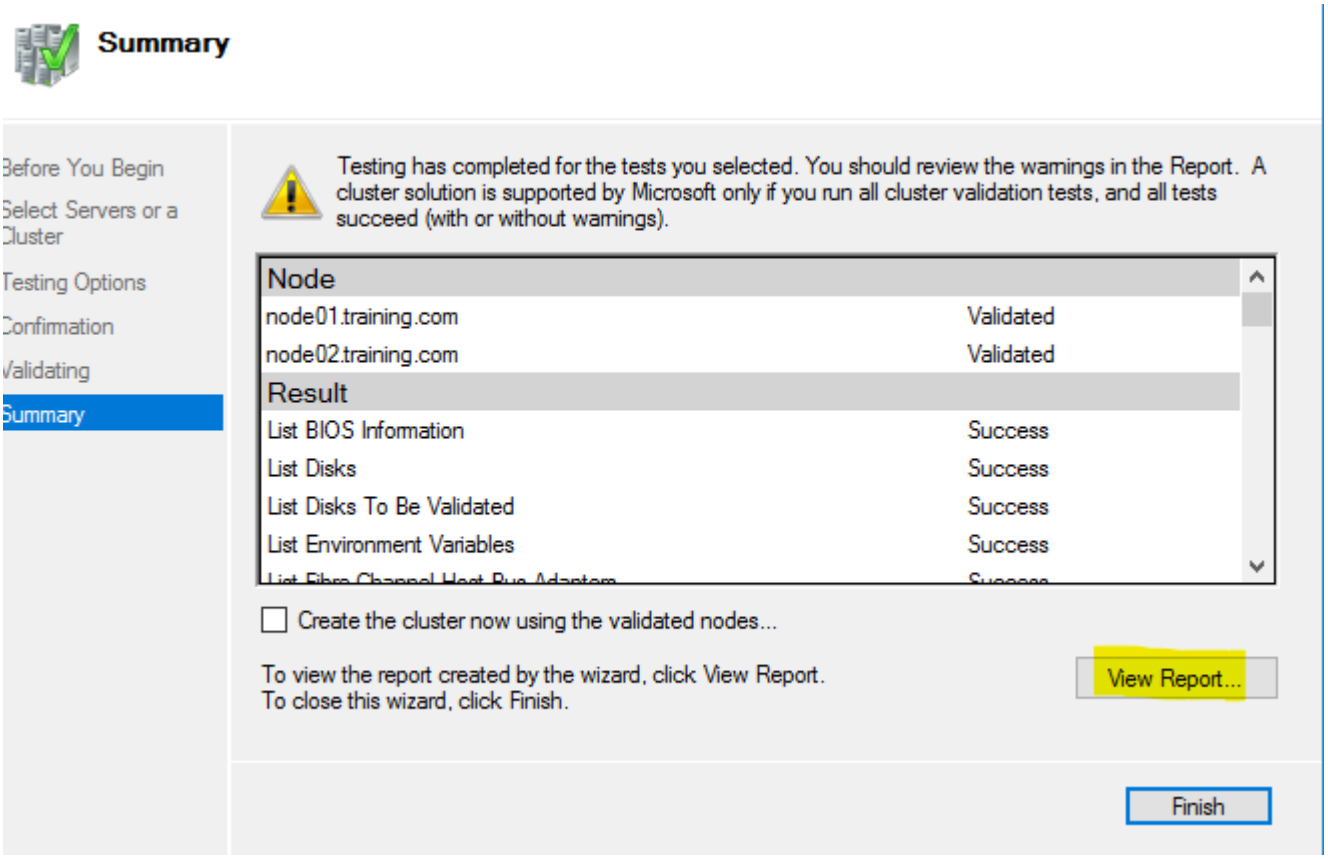


Validate:

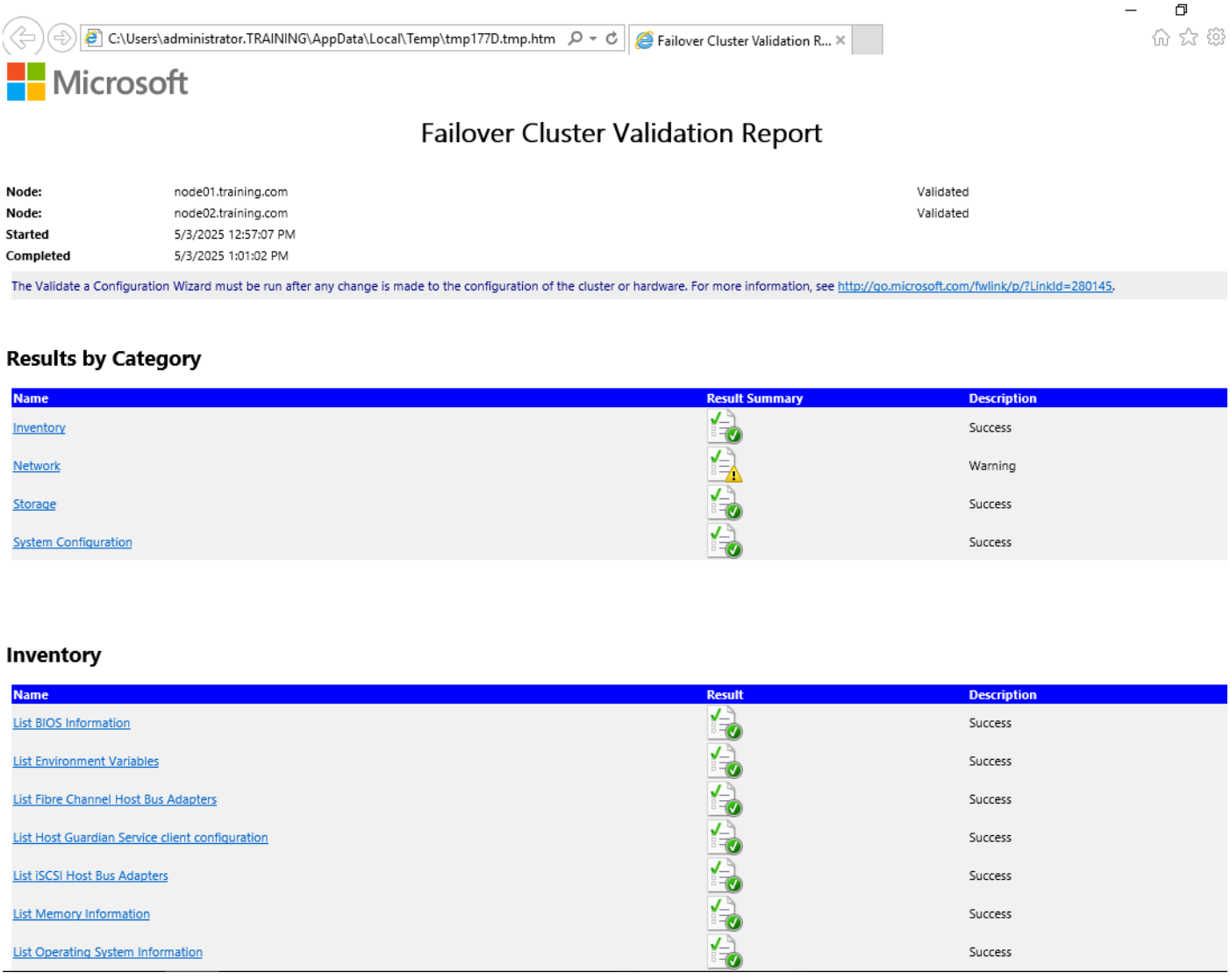


Wait…

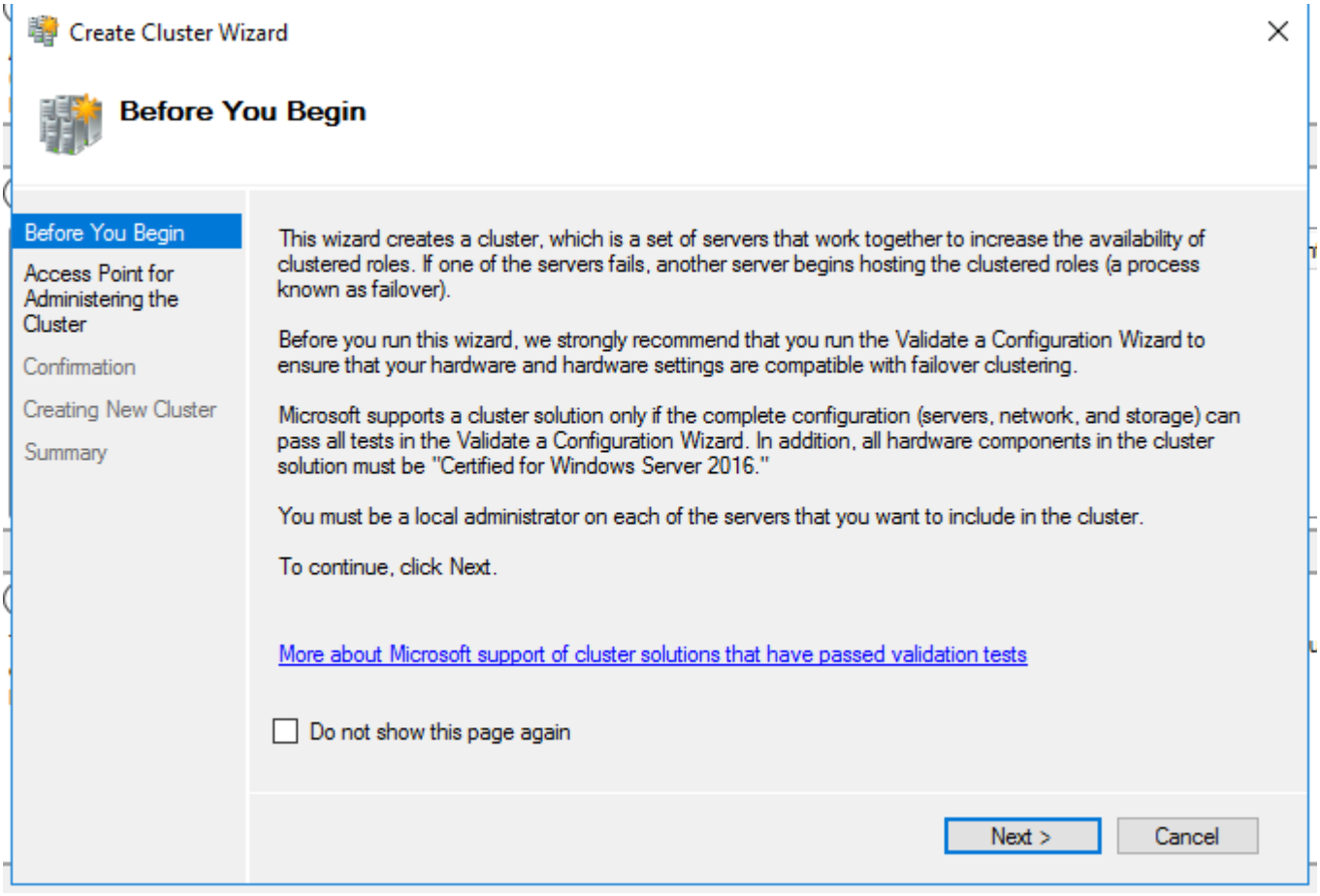



Summary
Before You Begin
Select Servers or a Cluster
Testing Options
Confirmation
Validating
Summary
Testing has completed for the tests you selected. You should review the warnings in the Report. A cluster solution is supported by Microsoft only if you run all cluster validation tests, and all tests succeed (with or without warnings).
Node
node01.training.com Validated
node02.training.com Validated
Result
List BIOS Information Success
List Disks Success
List Disks To Be Validated Success
List Environment Variables Success
Create the cluster now using the validated nodes...
To view the report created by the wizard, click View Report.
To close this wizard, click Finish.
View Report...
Finish

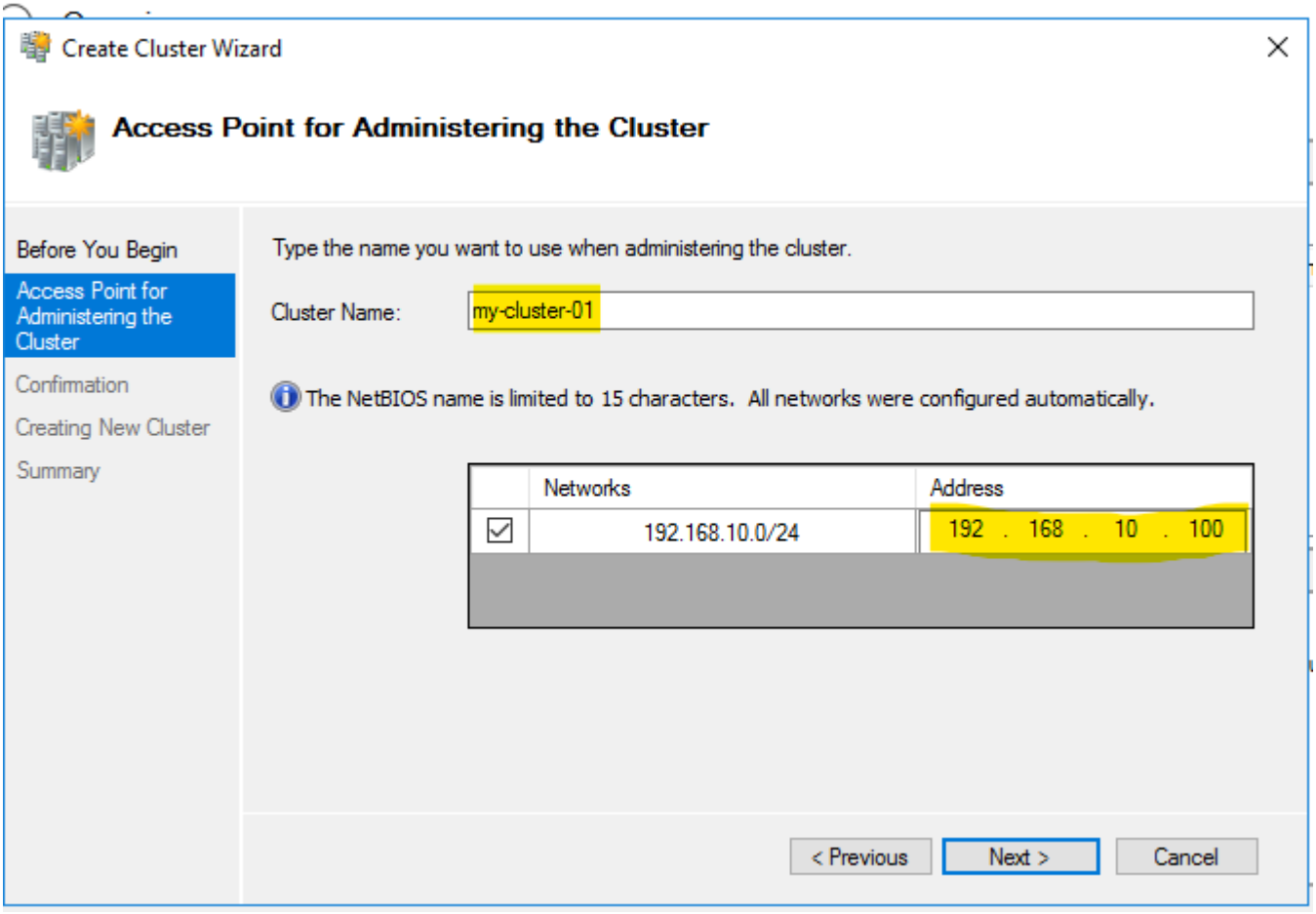
Validating:


C:\Users\administrator.TRAINING\AppData\Local\Temp\tmp177D.tmp.htm
Failover Cluster Validation R...
Microsoft
Failover Cluster Validation Report
Node: node01.training.com Validated
Node: node02.training.com Validated
Started 5/3/2025 12:57:07 PM
Completed 5/3/2025 1:01:02 PM
The Validate a Configuration Wizard must be run after any change is made to the configuration of the cluster or hardware. For more information, see http://go.microsoft.com/fwlink/p/?LinkId=280145.
Results by Category
Name Result Summary Description
Inventory Success
Network Warning
Storage Success
System Configuration Success
Inventory
Name Result Description
List BIOS Information Success
List Environment Variables Success
List Fibre Channel Host Bus Adapters Success
List Host Guardian Service client configuration Success
List iSCSI Host Bus Adapters Success
List Memory Information Success
List Operating System Information Success

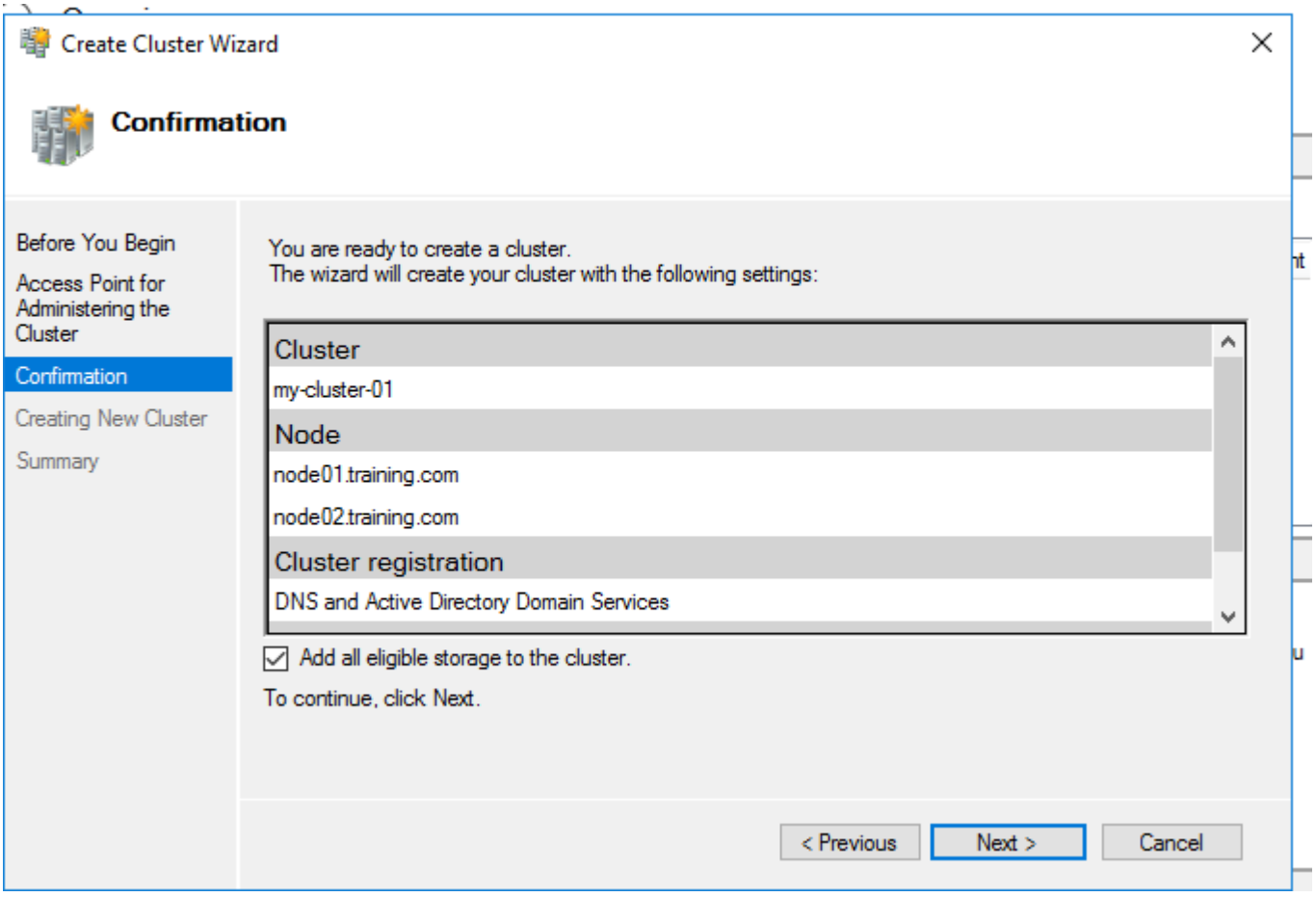
Creating cluster wizard:

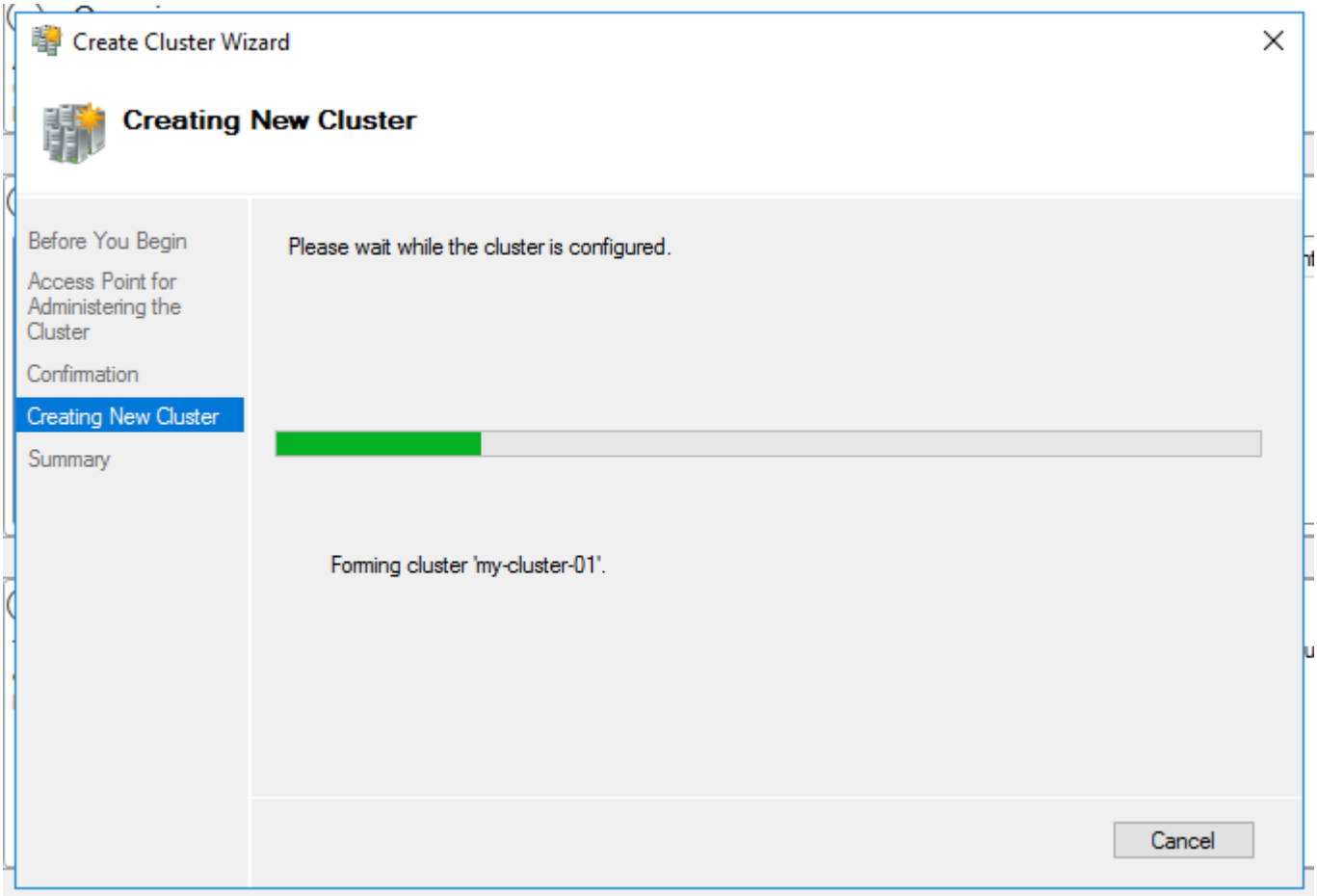


Setting cluster Name & IP address:

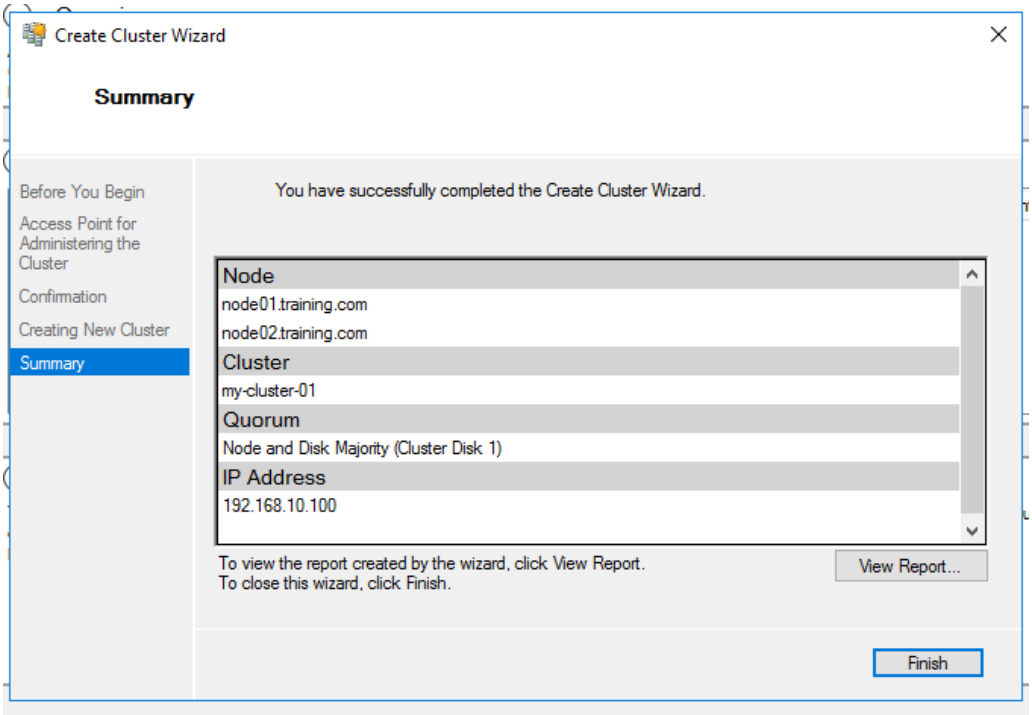


Confirmation:

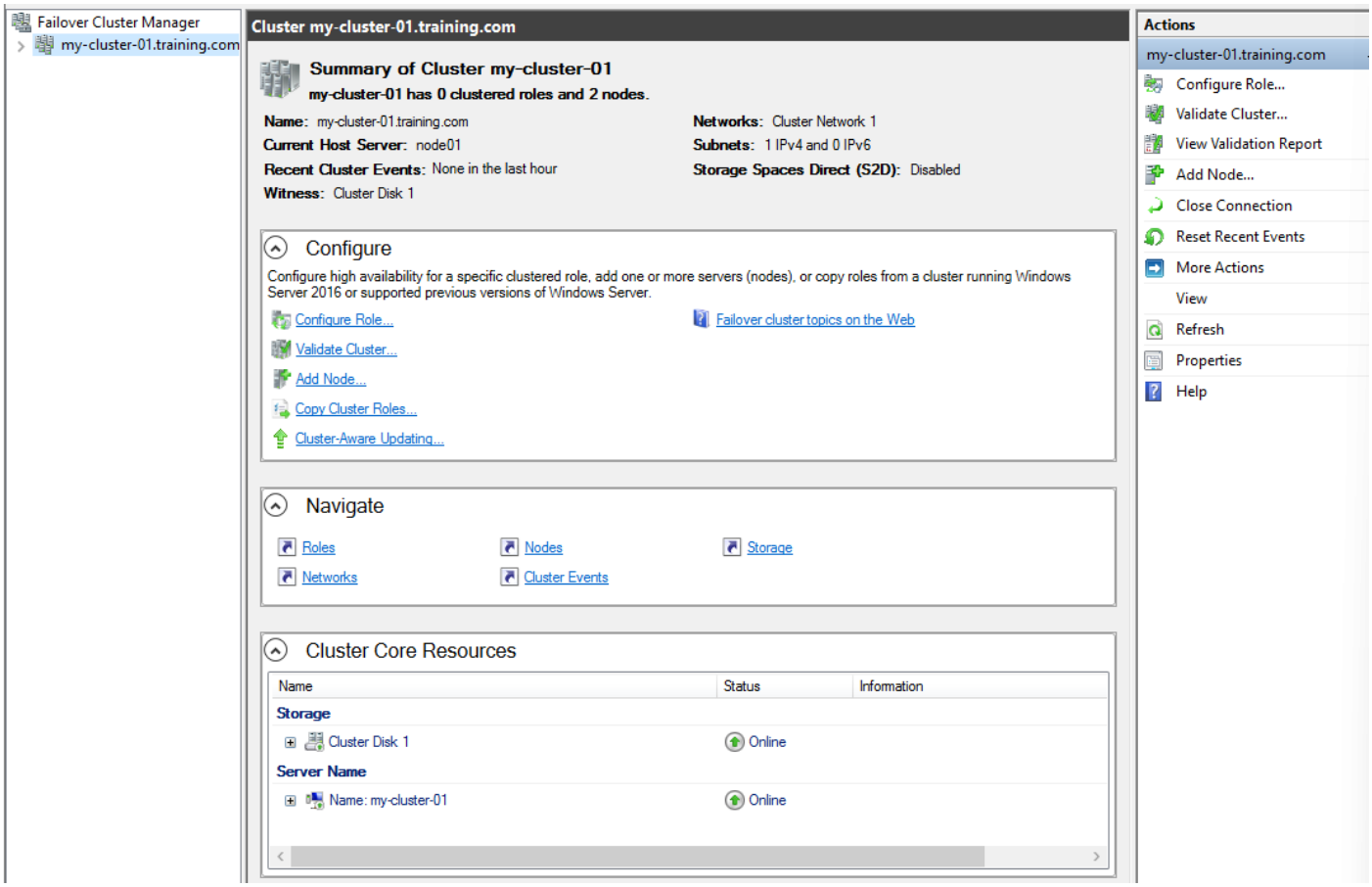




Summary:

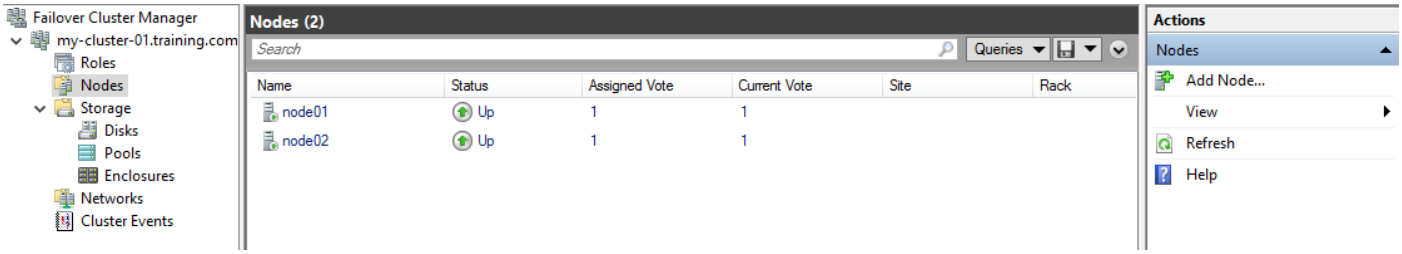


View report:



Listing disks:

Listing nodes:



################################ END of cluster ################################

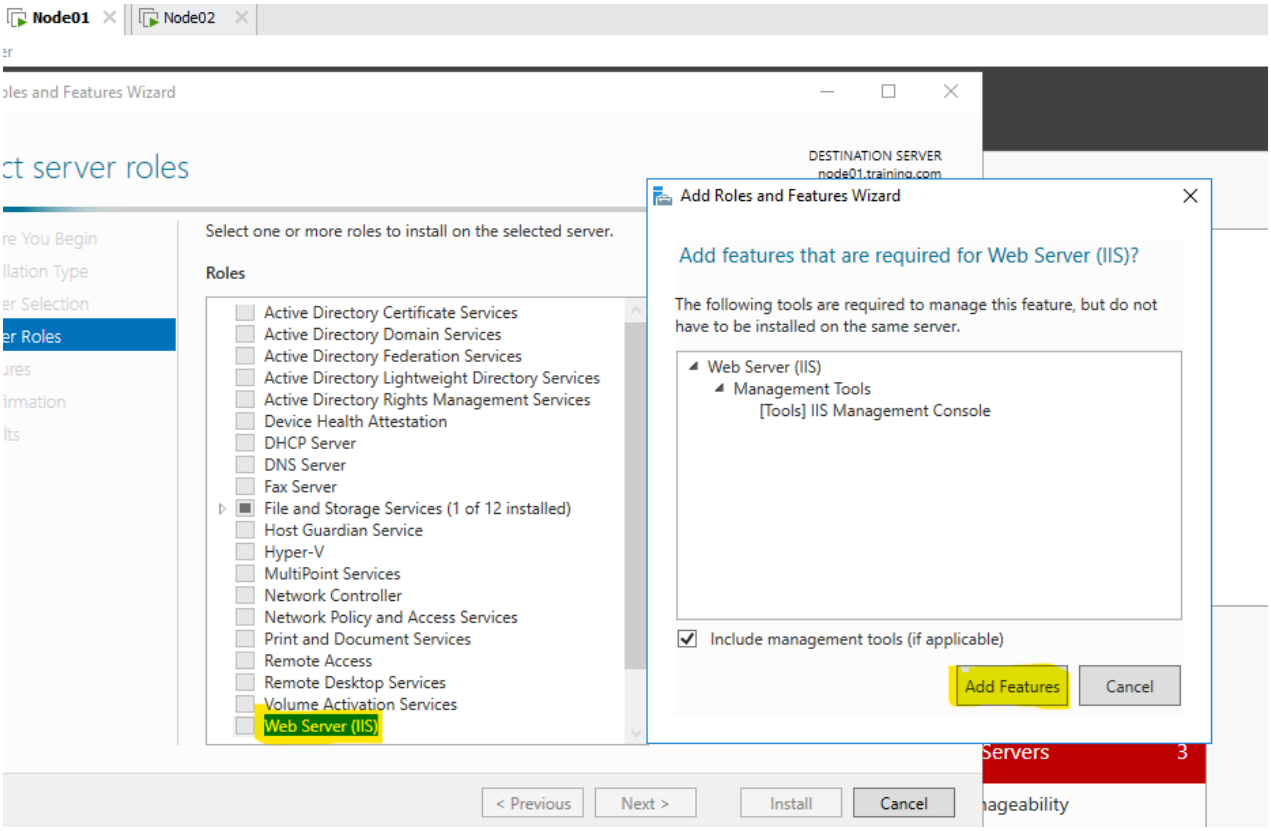
Network Load Balancing

Note: Uninstall/remove failover clustering before NLB and reboot

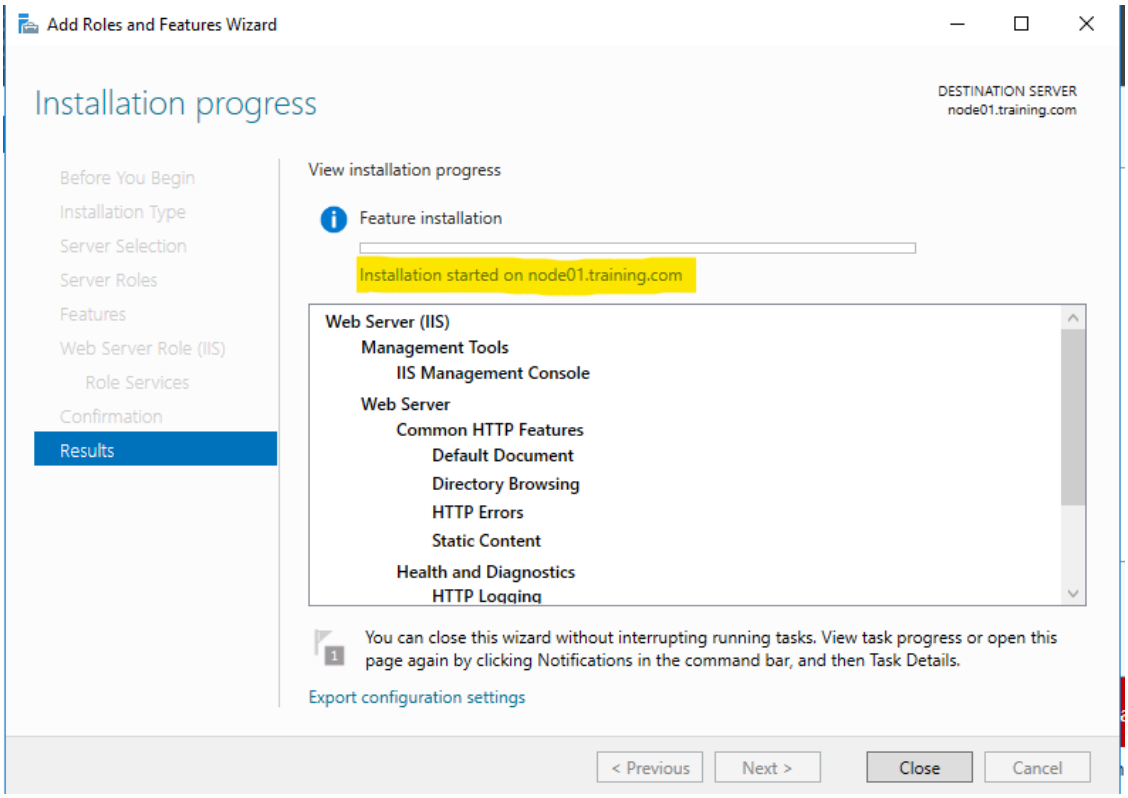
Installing IIS web server role on each Node (01 & 02):

Node 01:

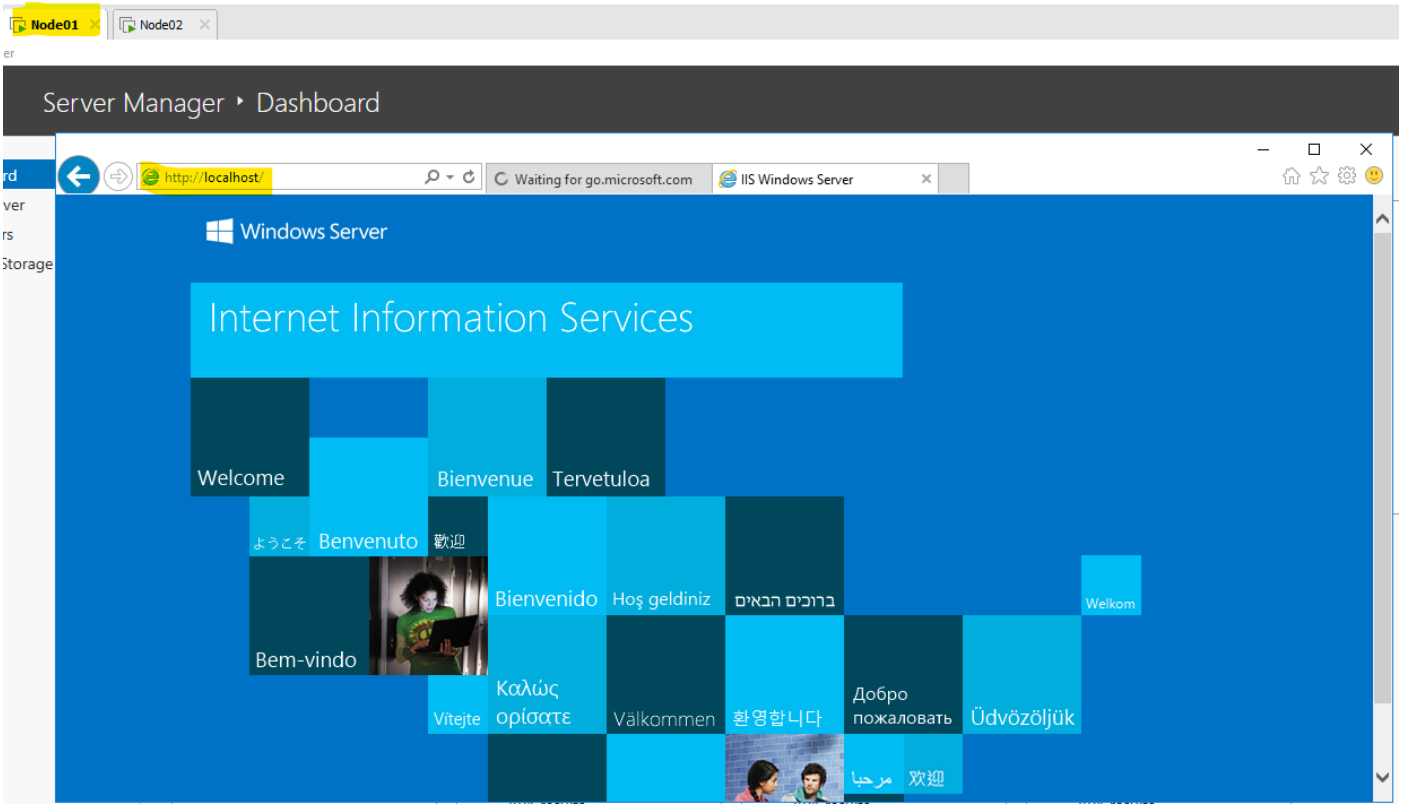
Server manager dashboard page:



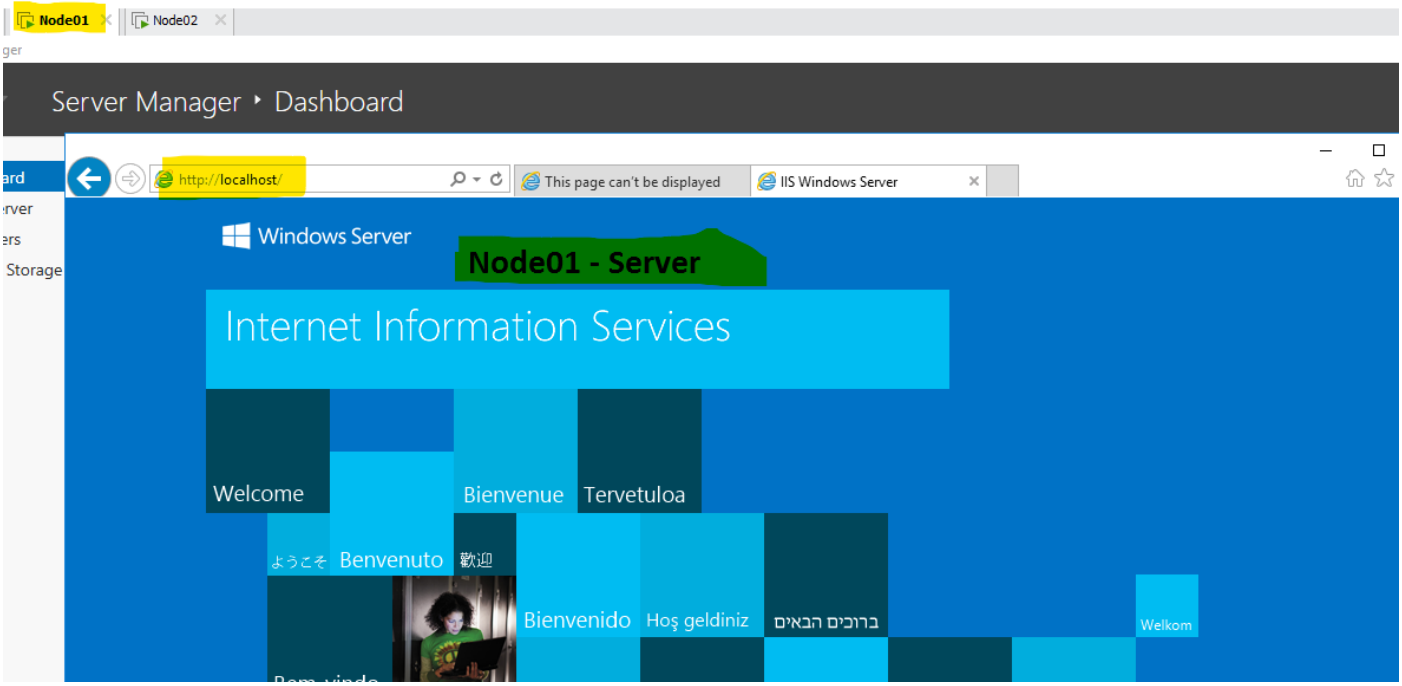
Wait…



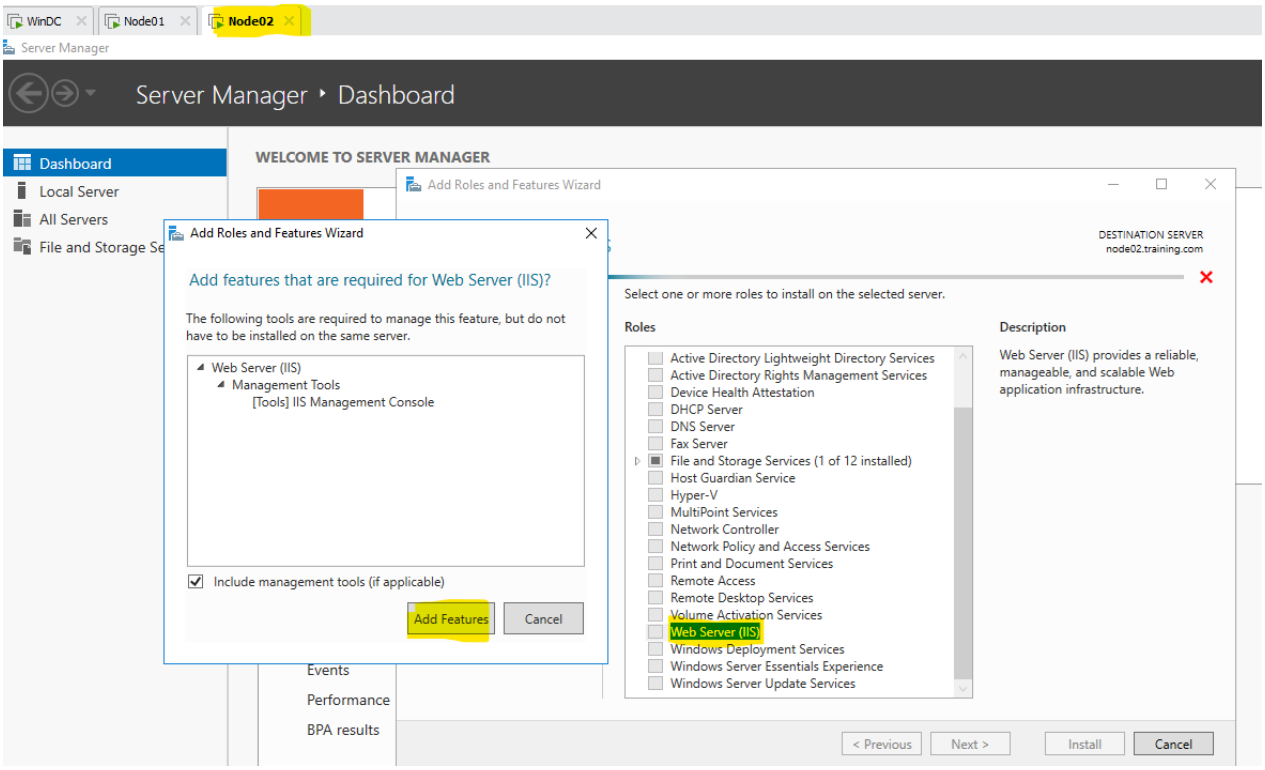
Verifying the installation using browser (http://localhost)

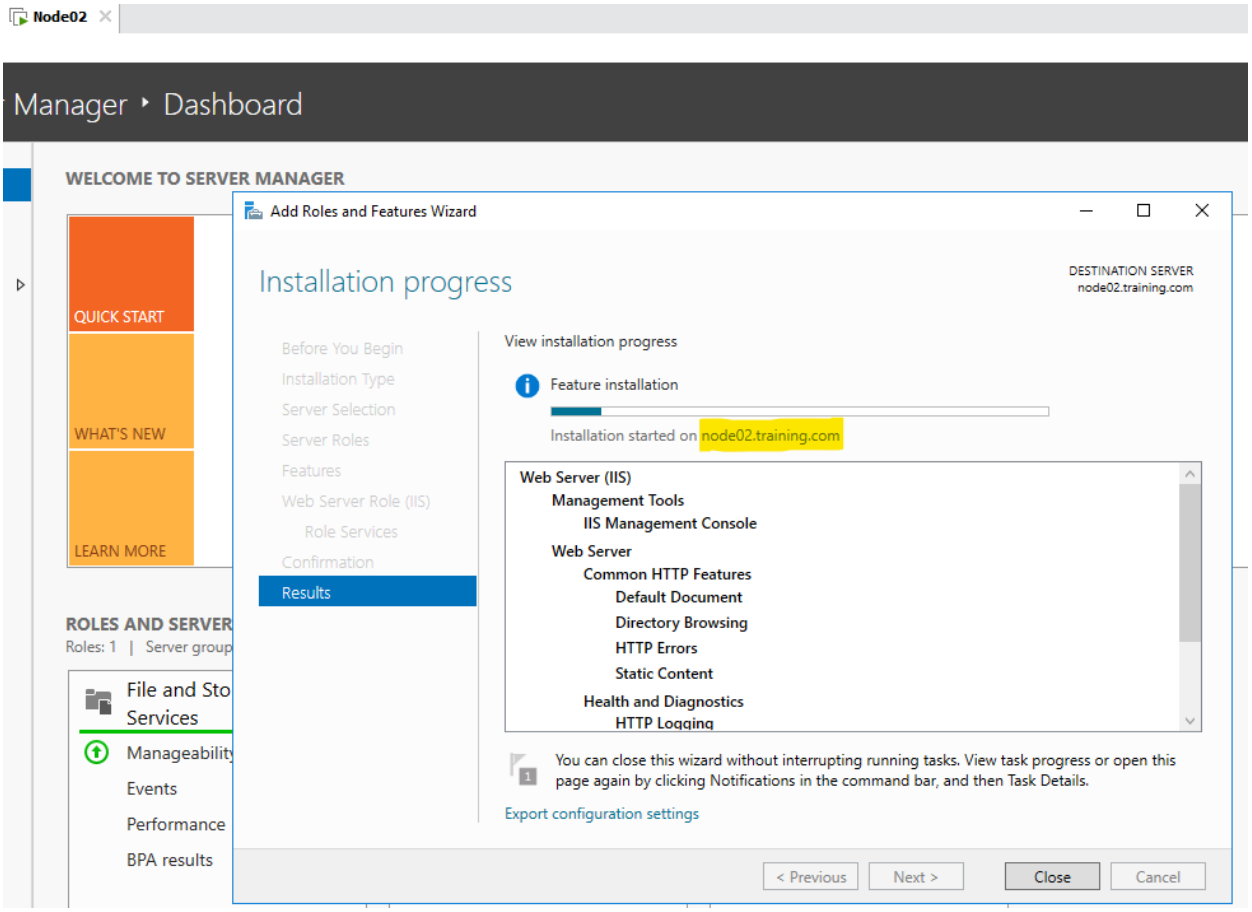


Edit the webpage or image file present on “C:\inetpub\wwwroot”:

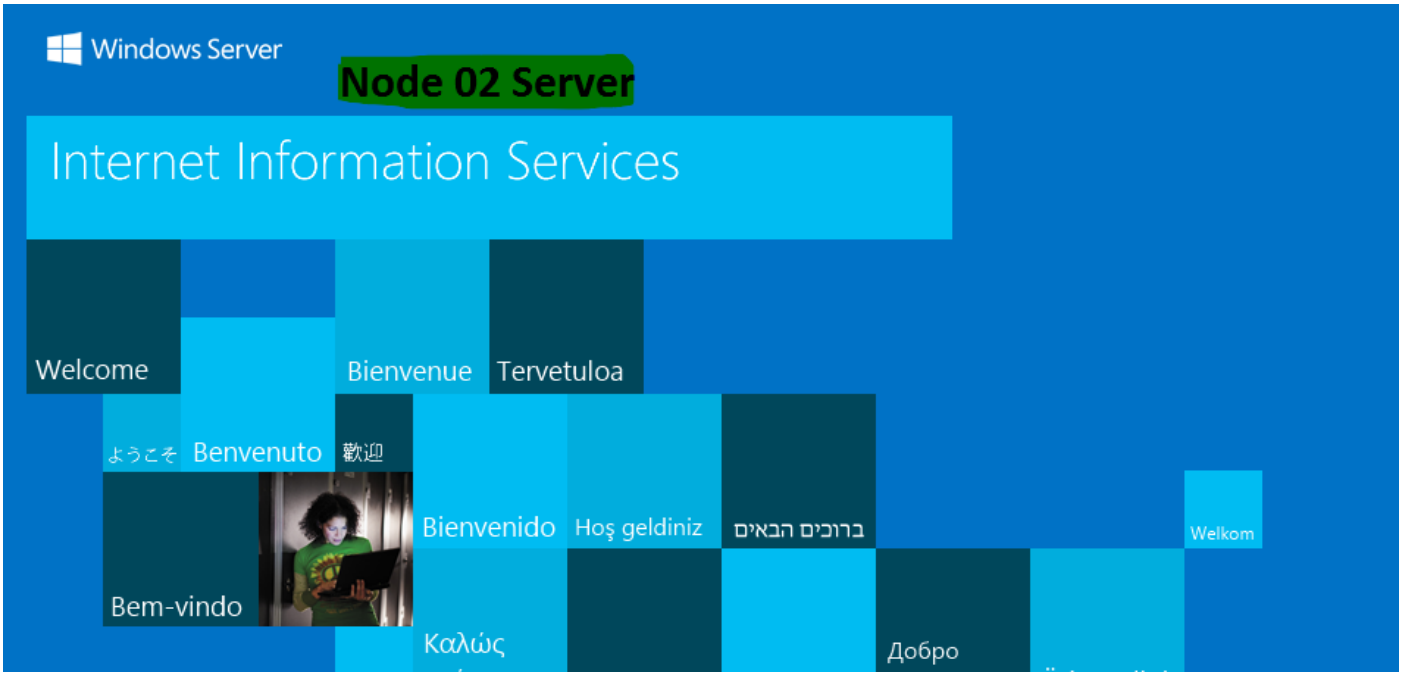


Node 02:


WinDC
Node01
Node02
Server Manager
Server Manager ‣ Dashboard
Dashboard
Local Server
All Servers
File and Storage Se
WELCOME TO SERVER MANAGER
Add Roles and Features Wizard
Add features that are required for Web Server (IIS)?
The following tools are required to manage this feature, but do not have to be installed on the same server.
Web Server (IIS)
Management Tools
[Tools] IIS Management Console
Include management tools (if applicable)
Add Features
Cancel
Add Roles and Features Wizard
DESTINATION SERVER
node02.training.com
Select one or more roles to install on the selected server.
Roles
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Device Health Attestation
DHCP Server
DNS Server
Fax Server
File and Storage Services (1 of 12 installed)
Host Guardian Service
Hyper-V
MultiPoint Services
Network Controller
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Volume Activation Services
Web Server (IIS)
Windows Deployment Services
Windows Server Essentials Experience
Windows Server Update Services
Description
Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.
Events
Performance
BPA results
< Previous
Next >
Install
Cancel

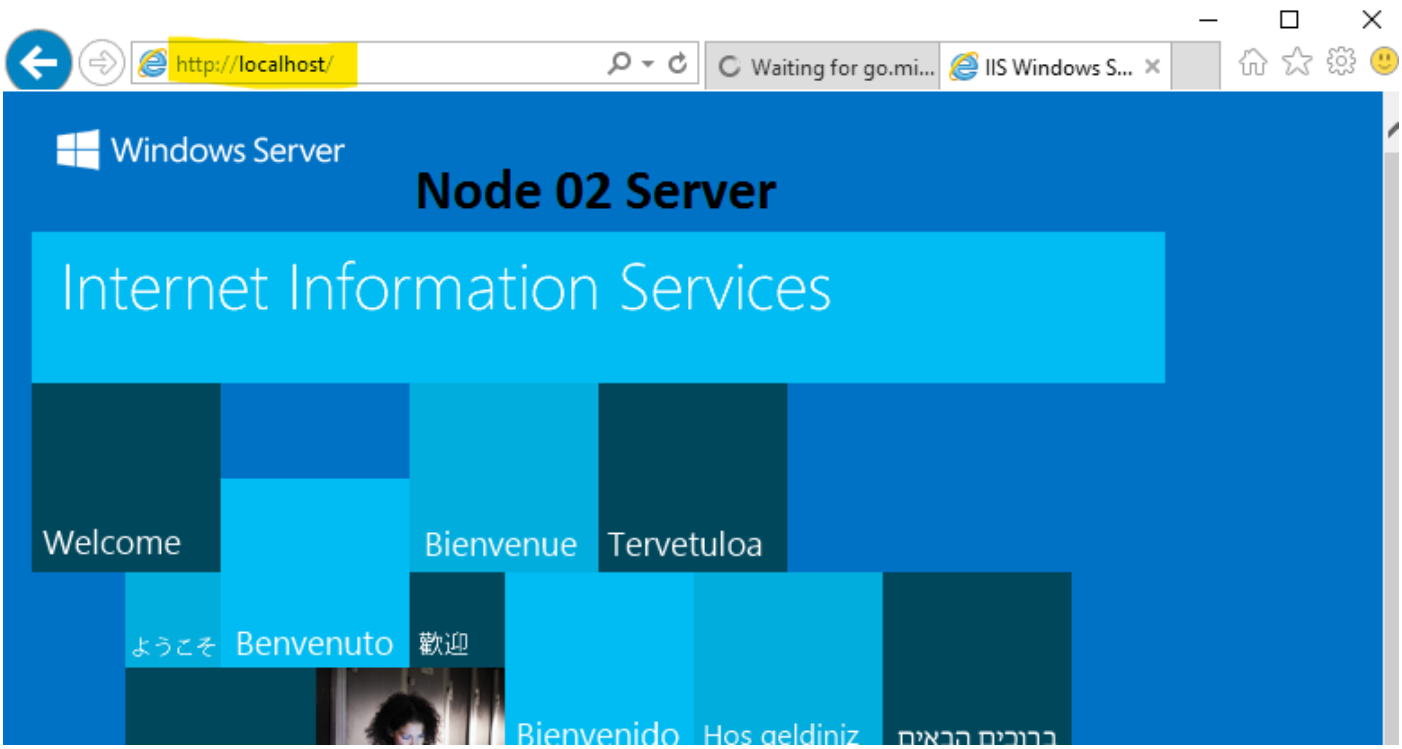

Node02
Manager ‣ Dashboard
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
ROLES AND SERVER
Roles: 1 | Server group
File and Sto
Services
Manageability
Events
Performance
BPA results
Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
node02.training.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results
View installation progress
Feature installation
Installation started on node02.training.com
Web Server (IIS)
Management Tools
IIS Management Console
Web Server
Common HTTP Features
Default Document
Directory Browsing
HTTP Errors
Static Content
Health and Diagnostics
HTTP Logging
You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.
Export configuration settings
< Previous
Next >
Close
Cancel

Edit the page at default HTML page or Image file on “C:\inetpub\wwwroot\”



Verify on localhost:

Open web browser and type “http://localhost/”



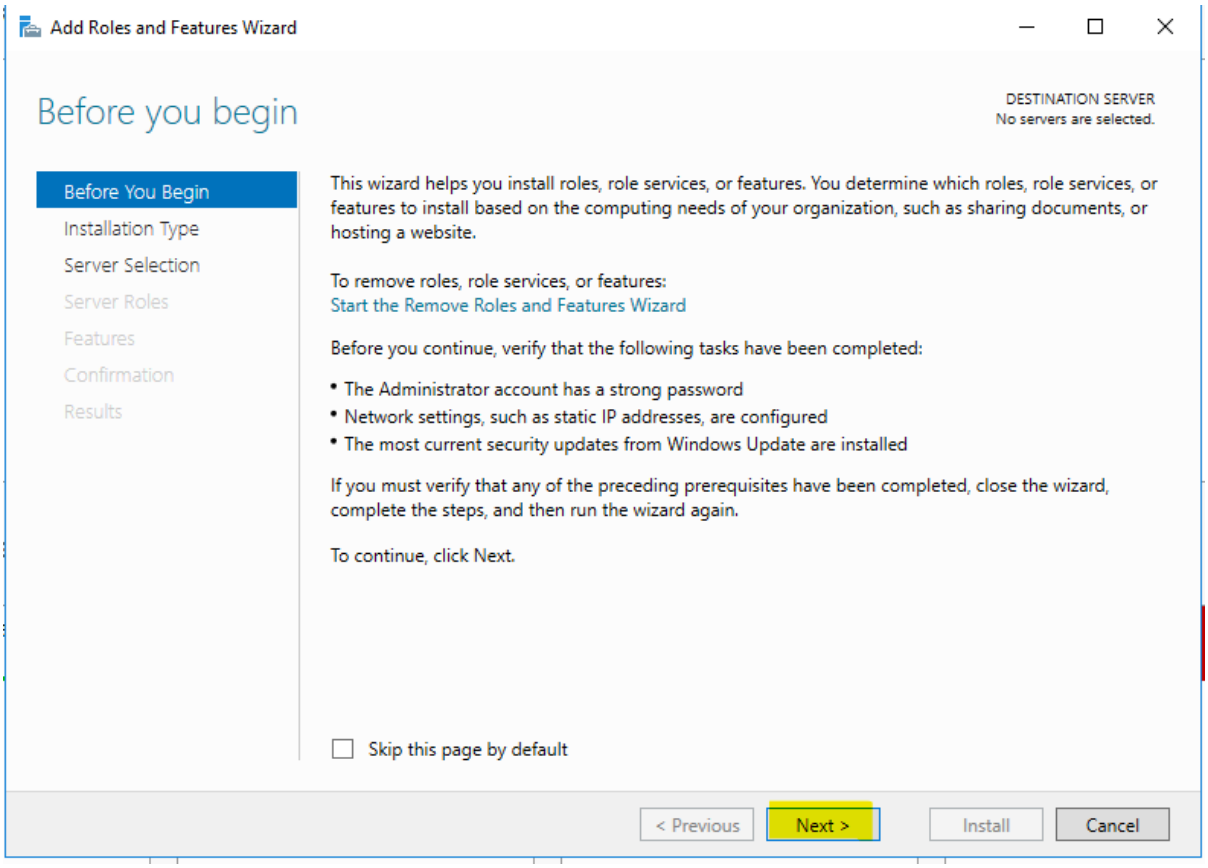
Now installing Network Load Balancer (NLB) on both Nodes 01 & 02:

Note: Uninstall/remove failover clustering before NLB

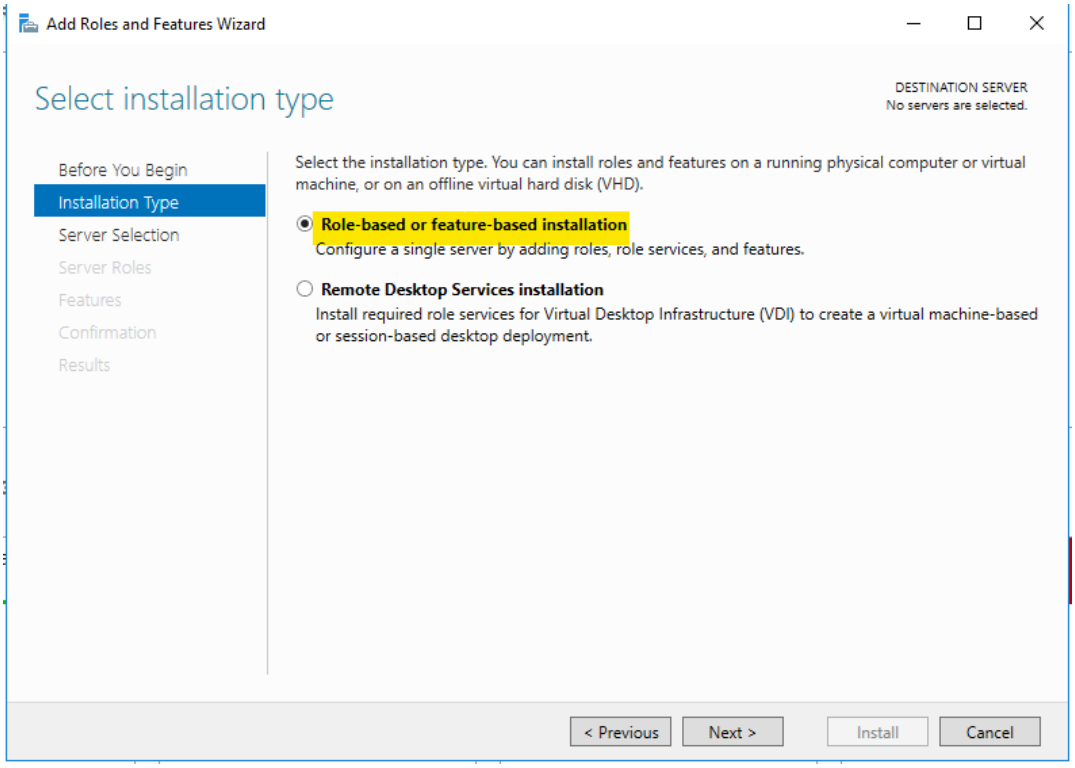
Node01:

Server Manager Dashboard → NLB role

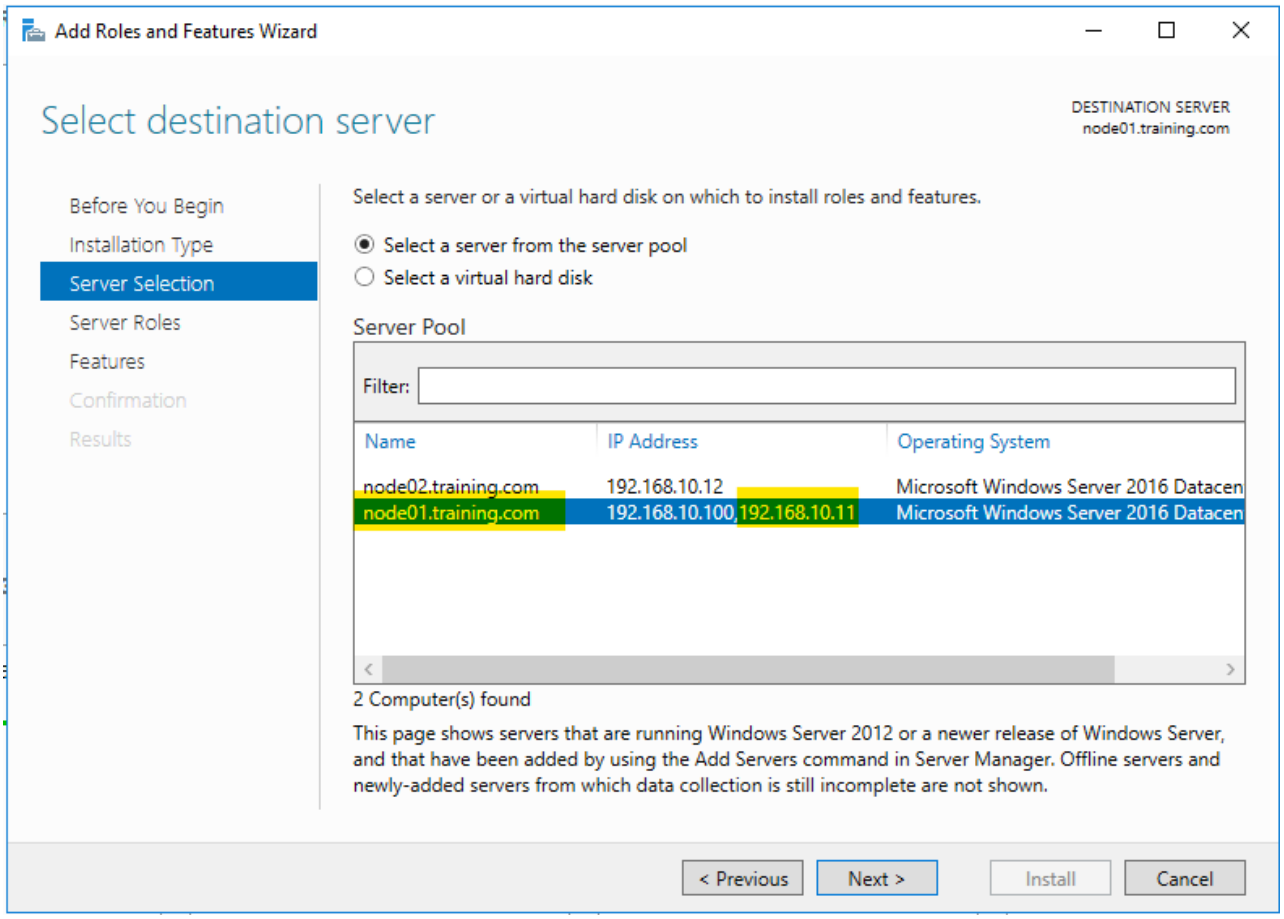
Skip 1st page:



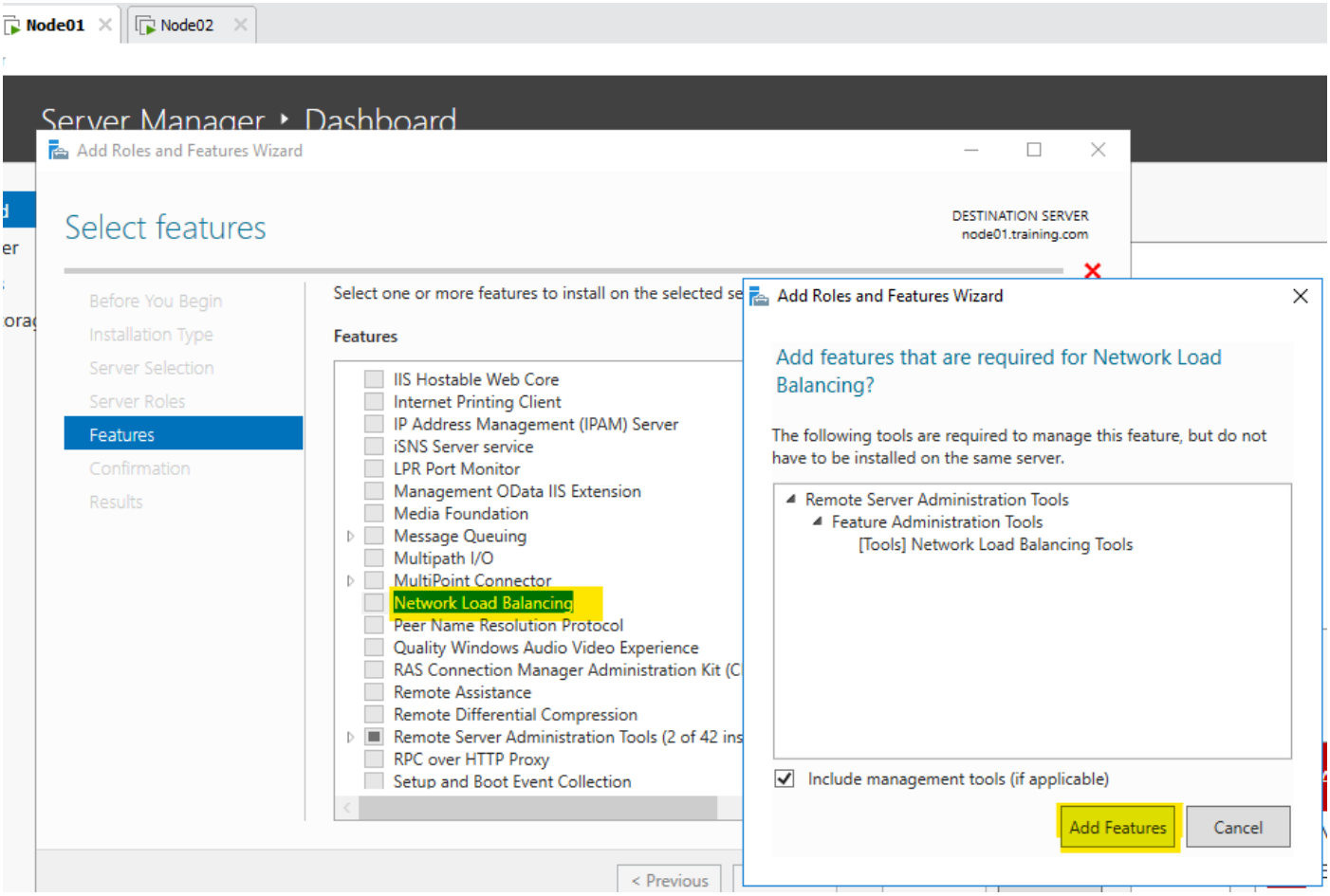
Select “Role-base or feature-based installation”:



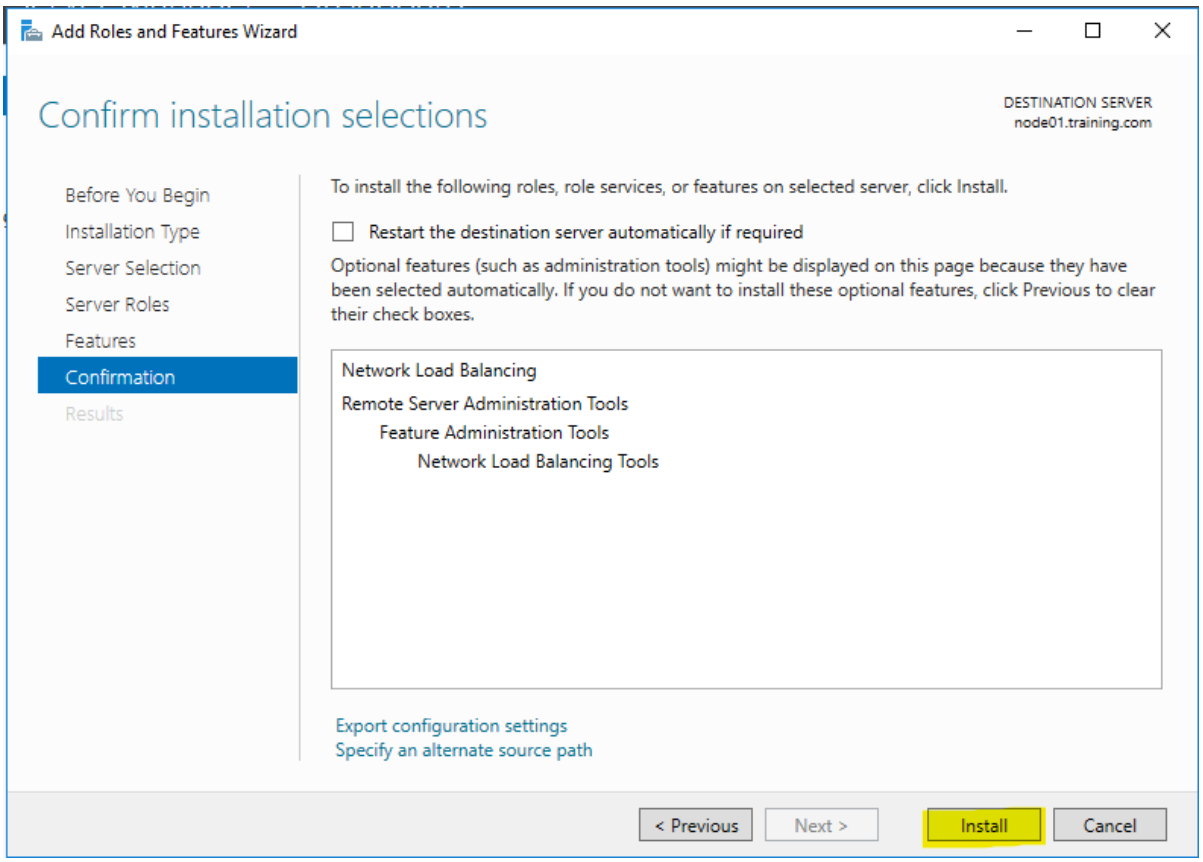
Select proper destination server:

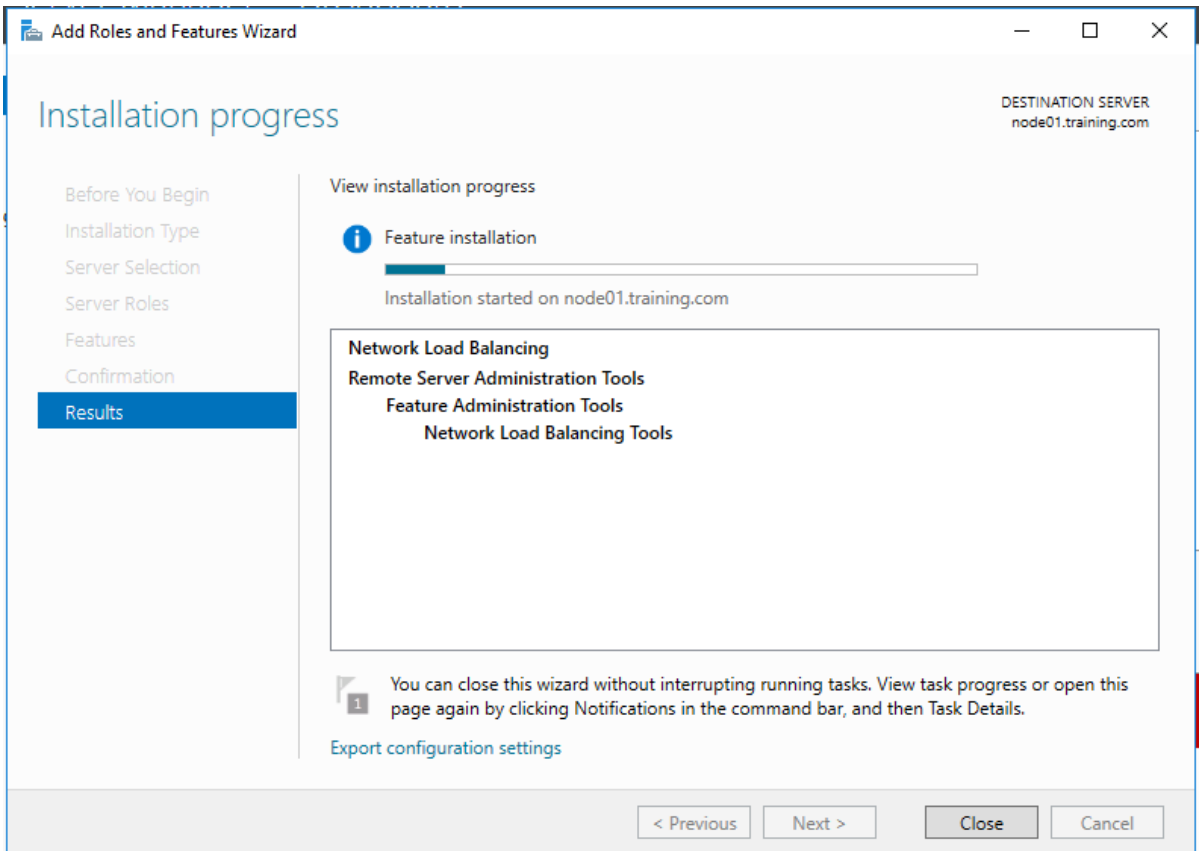


Installing Network Load Balancing (feature) on both Nodes01 & 02:



Click “install”:

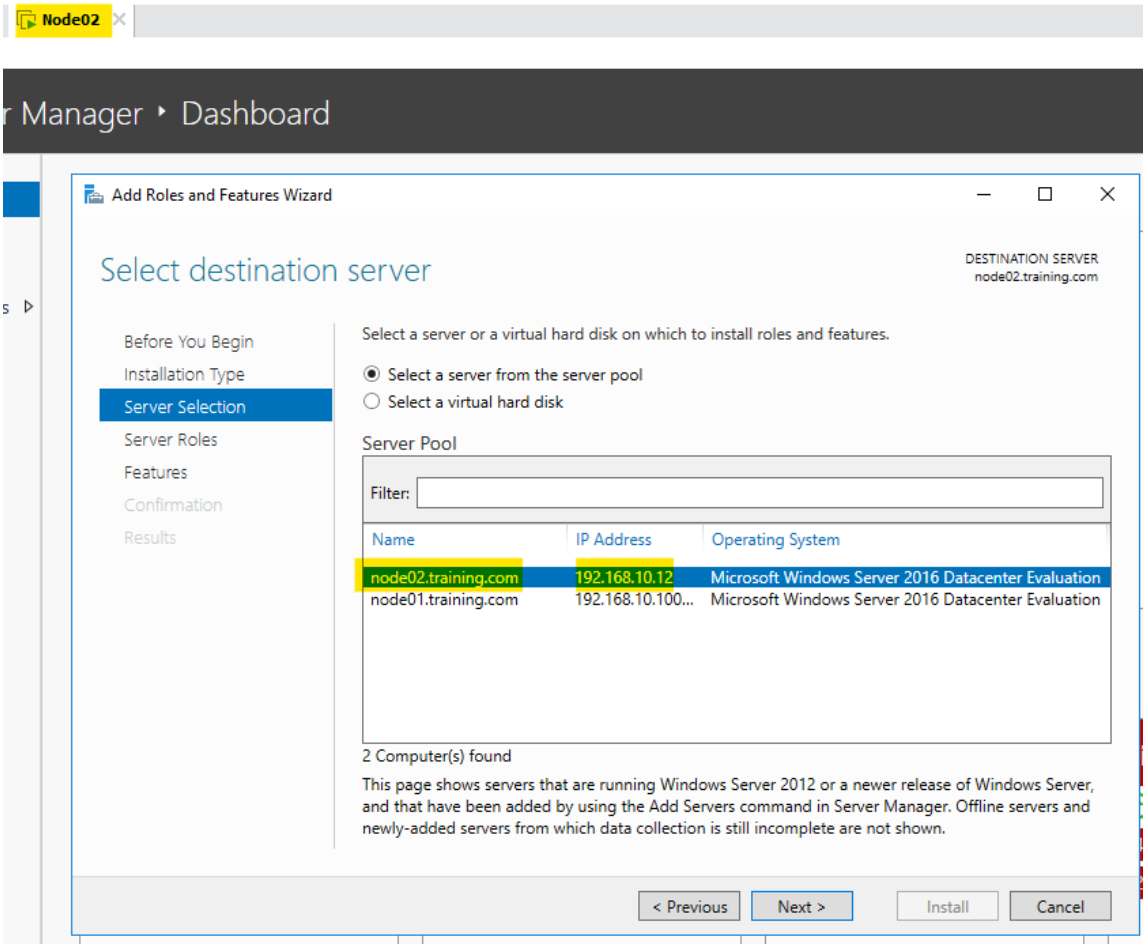




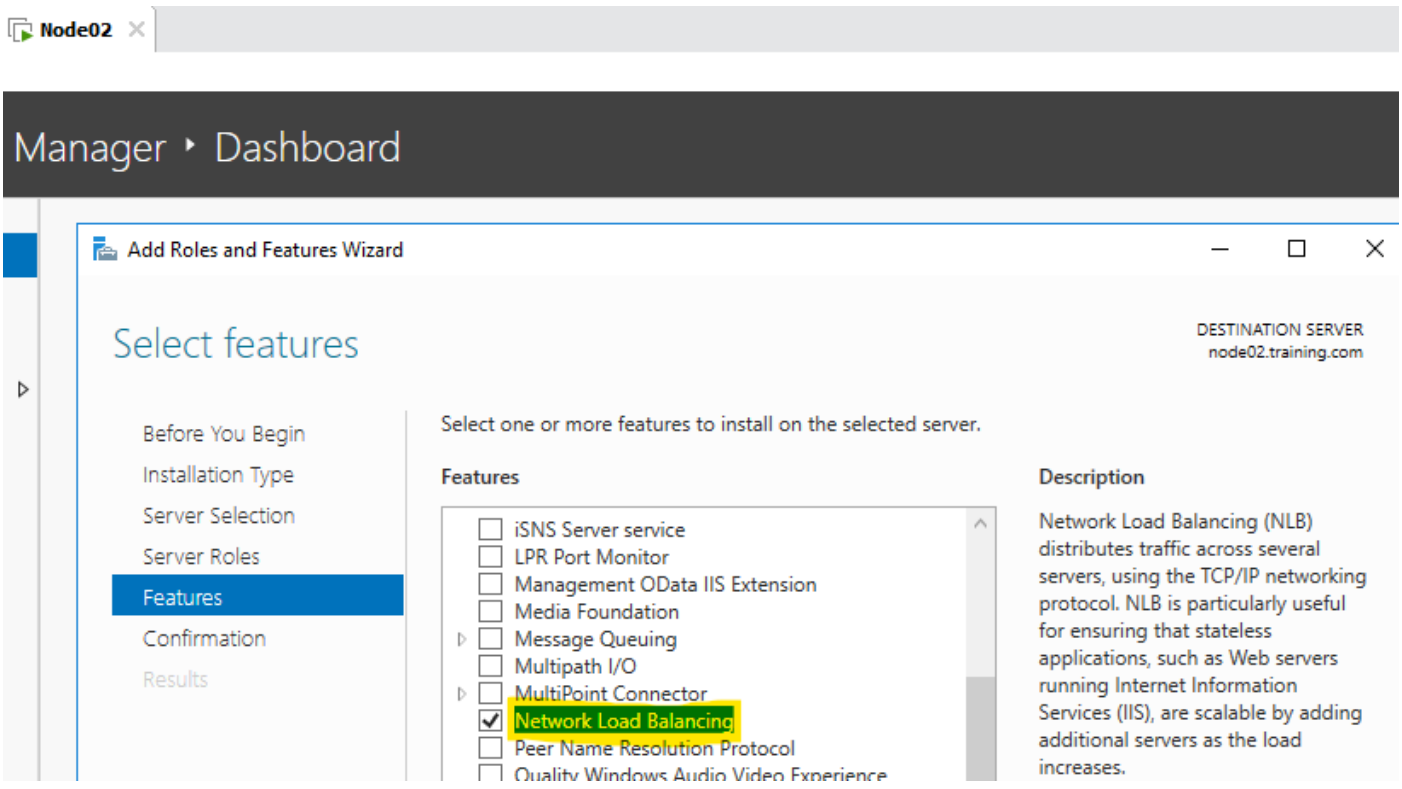
Node02:

Server Manager Dashboard → NLB role

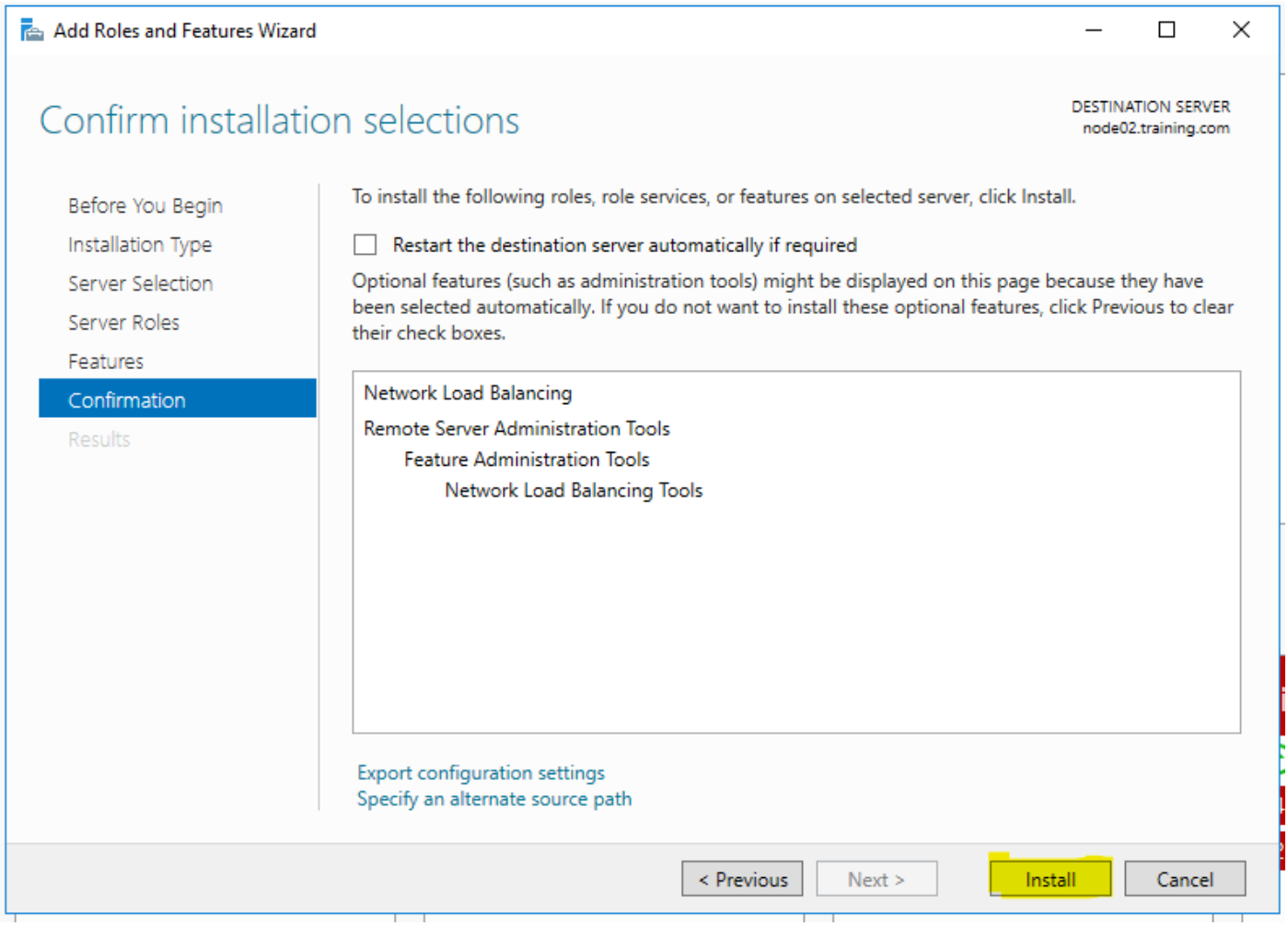
Skip 1st page:

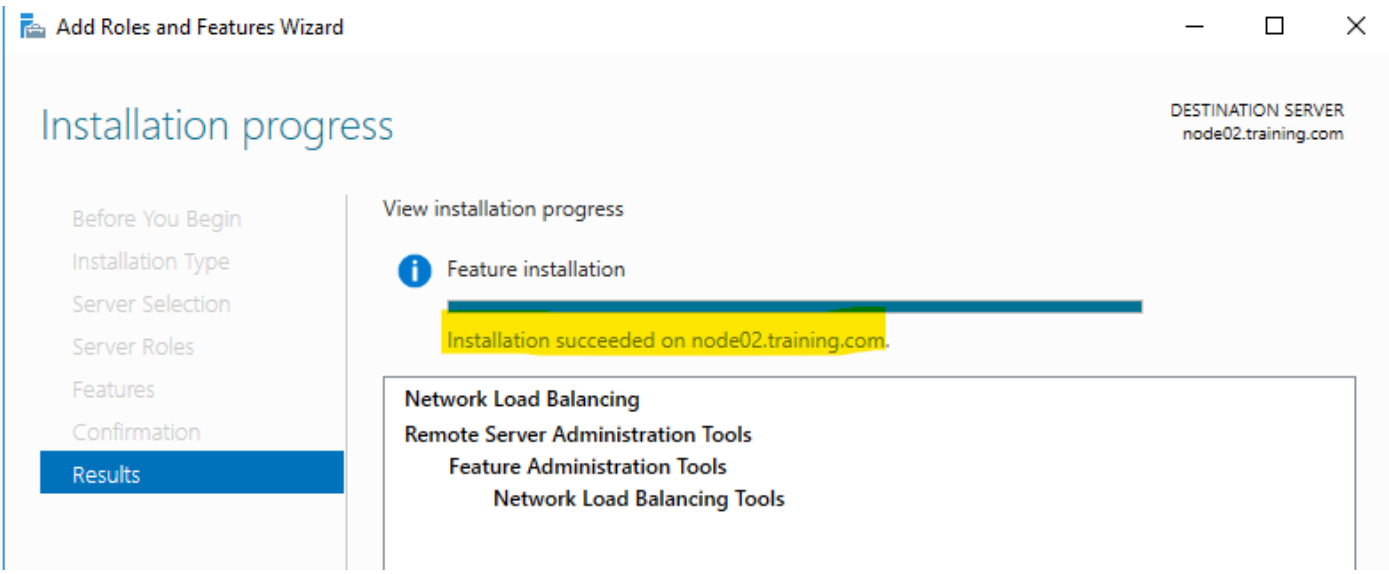


Selecting Network Load Balancing (NLB):



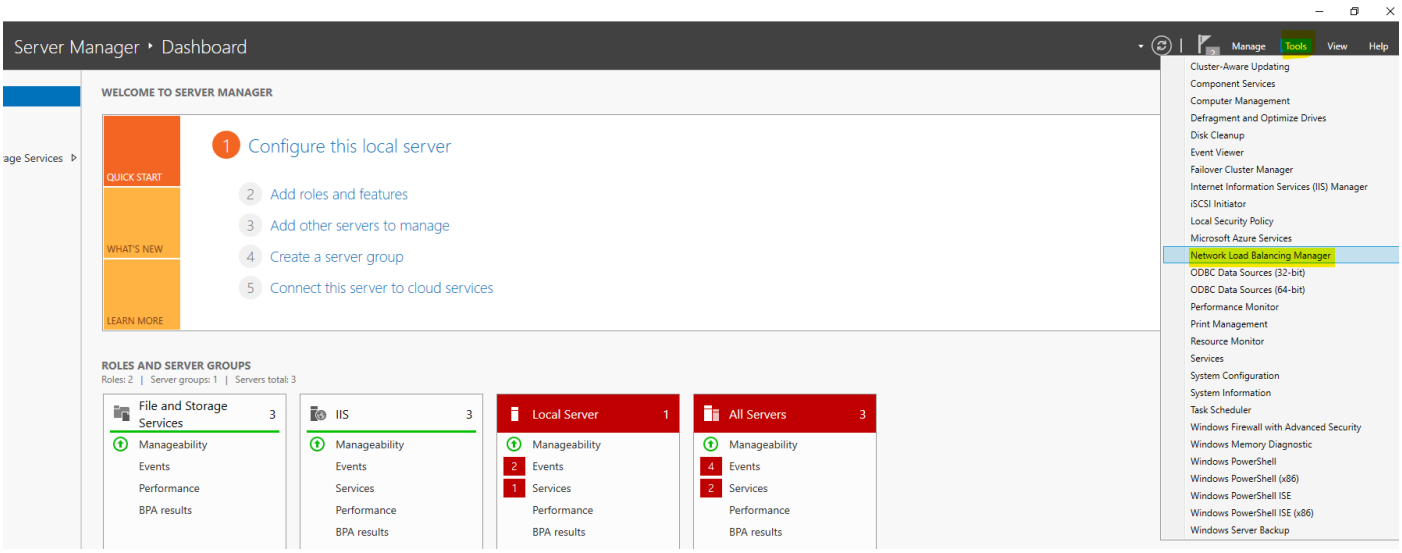
Install:


Add Roles and Features Wizard
Confirm installation selections
DESTINATION SERVER
node02.training.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
To install the following roles, role services, or features on selected server, click Install.
Restart the destination server automatically if required
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.
Network Load Balancing
Remote Server Administration Tools
Feature Administration Tools
Network Load Balancing Tools
Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel

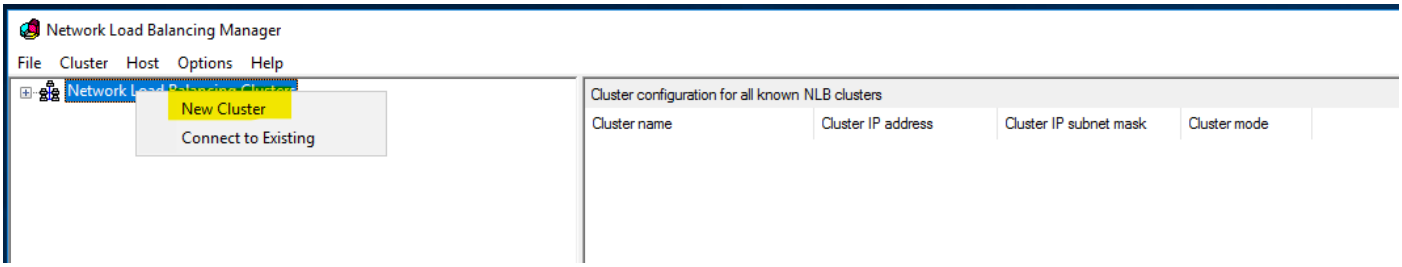

Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
node02.training.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
View installation progress
Feature installation
Installation succeeded on node02.training.com.
Network Load Balancing
Remote Server Administration Tools
Feature Administration Tools
Network Load Balancing Tools

Configuring NLB on Node01:

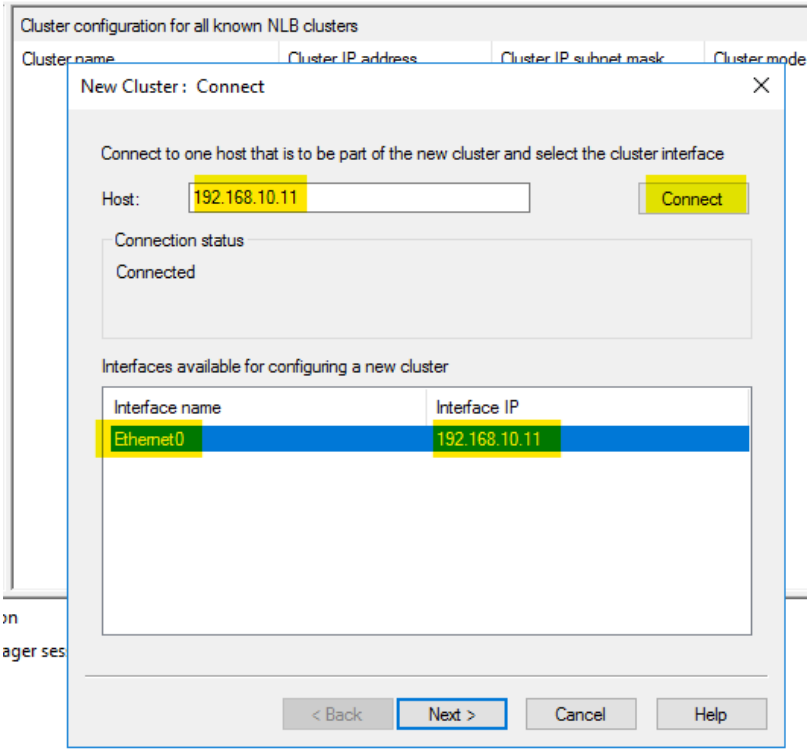
Server Manager Dashboard → Tools → Network Load balancing:



Right-click on the NLB clustering:

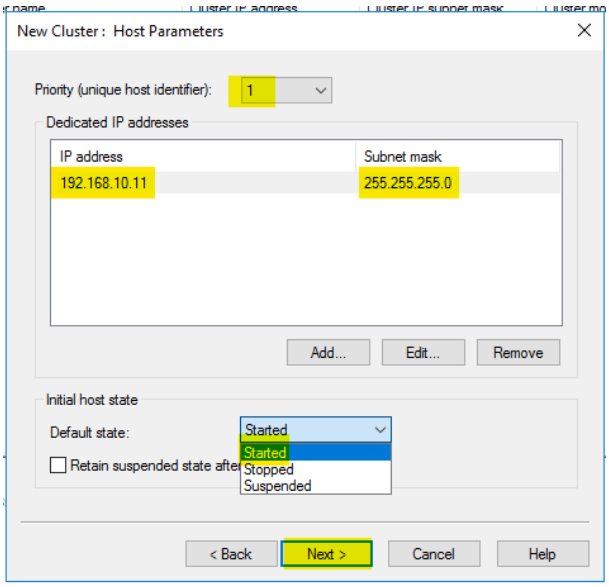


Enter Node01 (IP Address: 192.168.10.11) & click on “Connect”

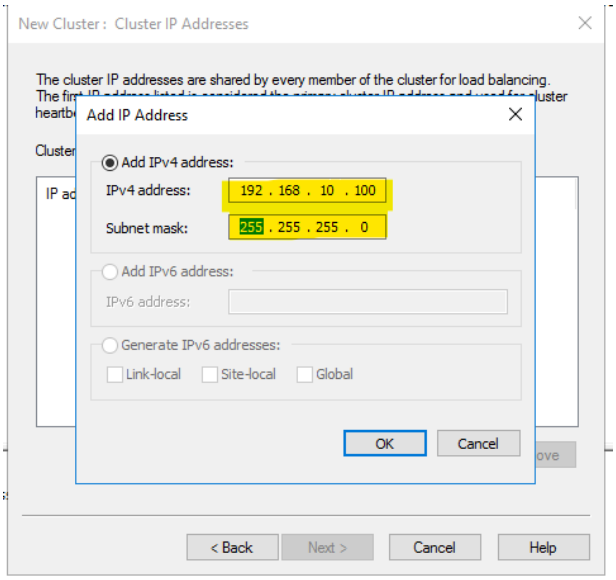


And click “Next”

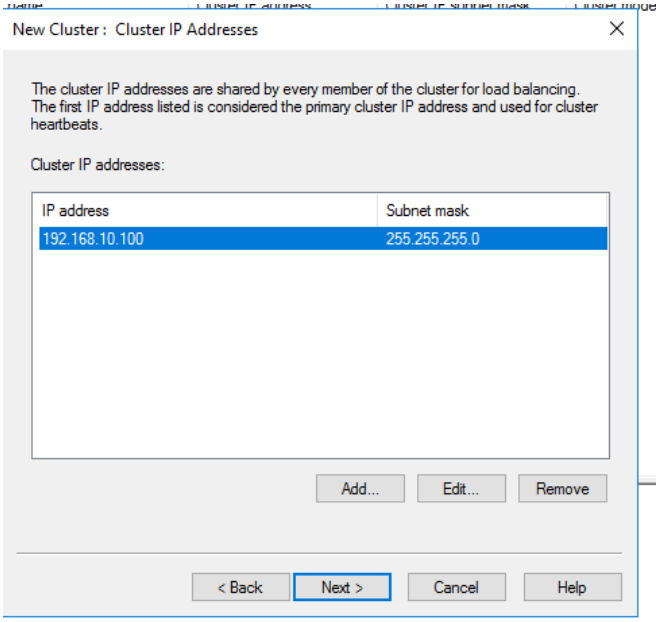
Verify “New Cluster: Host Parameters”:



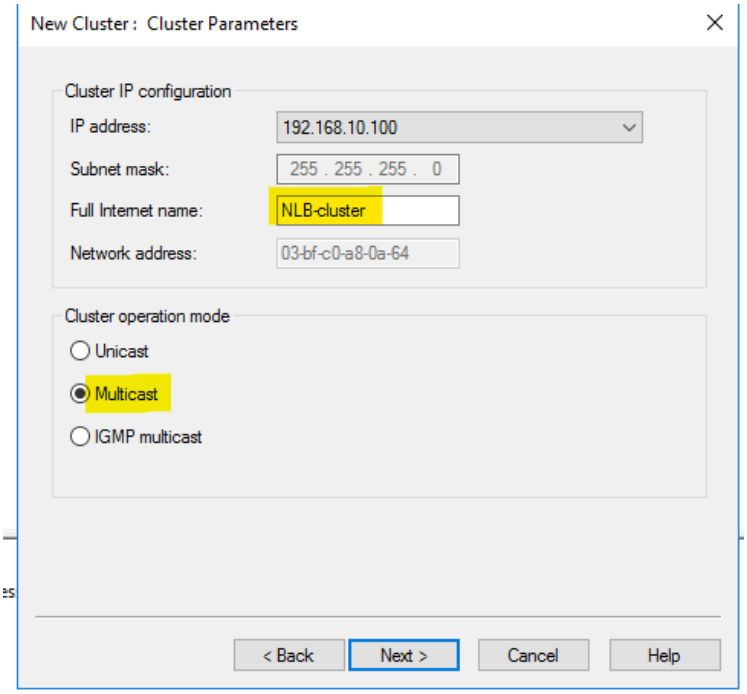
Add a new IP address (192.168.10.100) with subnet mask:



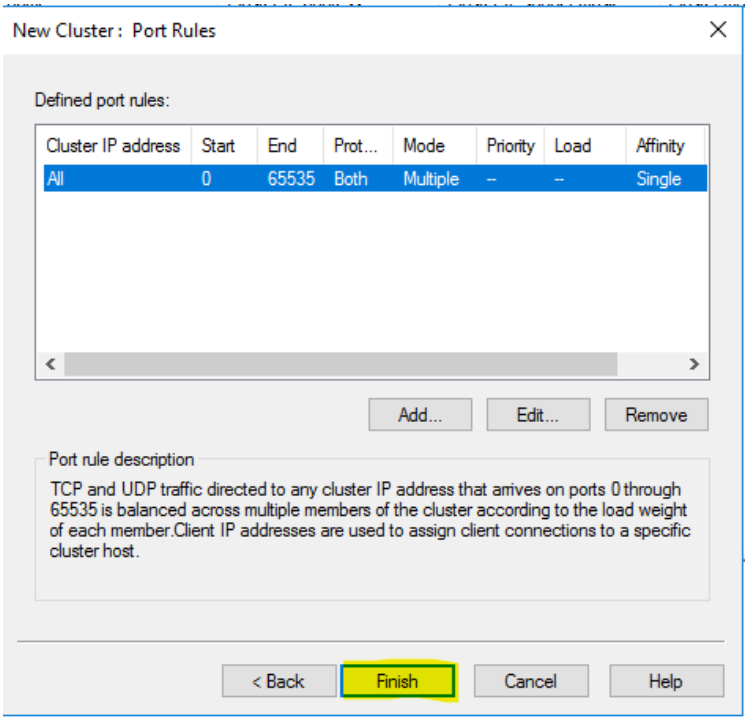
Next:

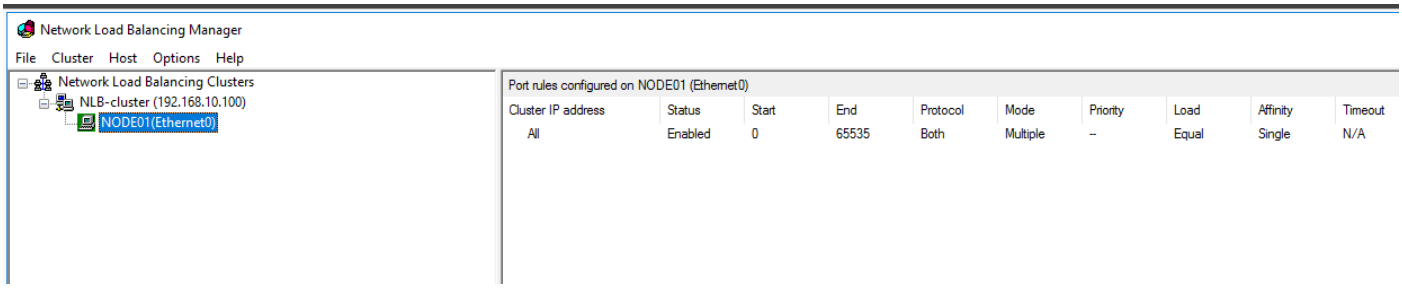


In Cluster Parameters: - Enter “Full Internet name: NLB-cluster”:



Click “Finish”:

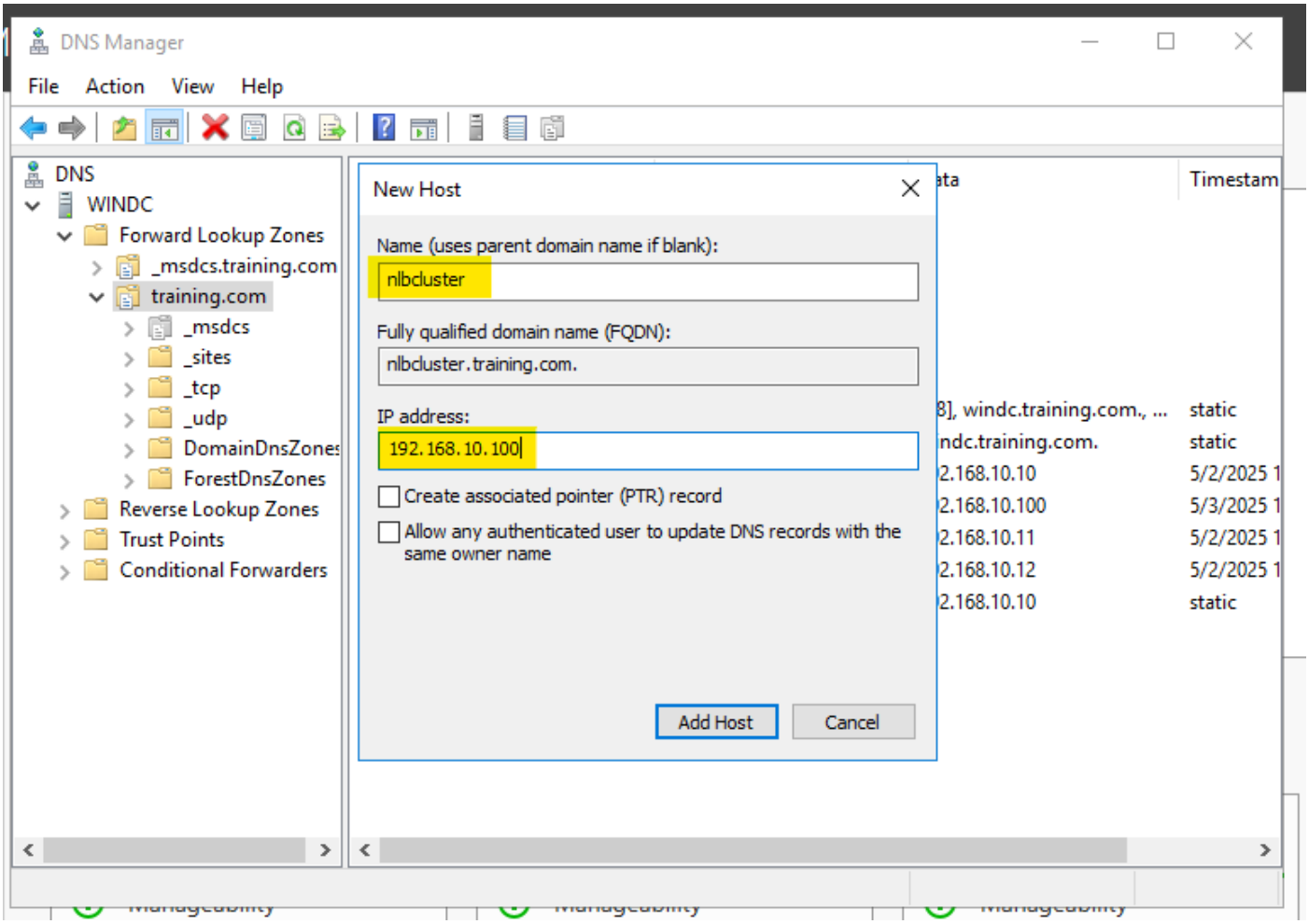




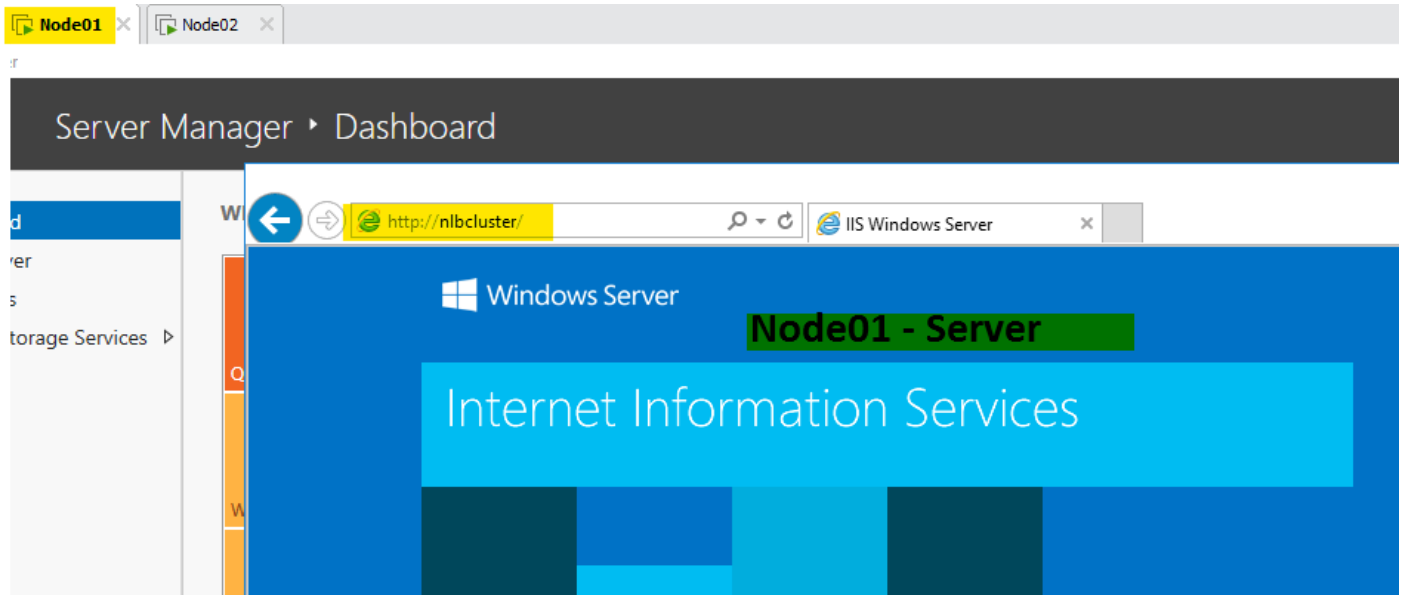
Now, create an A record in DNS server

Create DNS – A record name: nlb-cluster, IP: 192.168.10.100

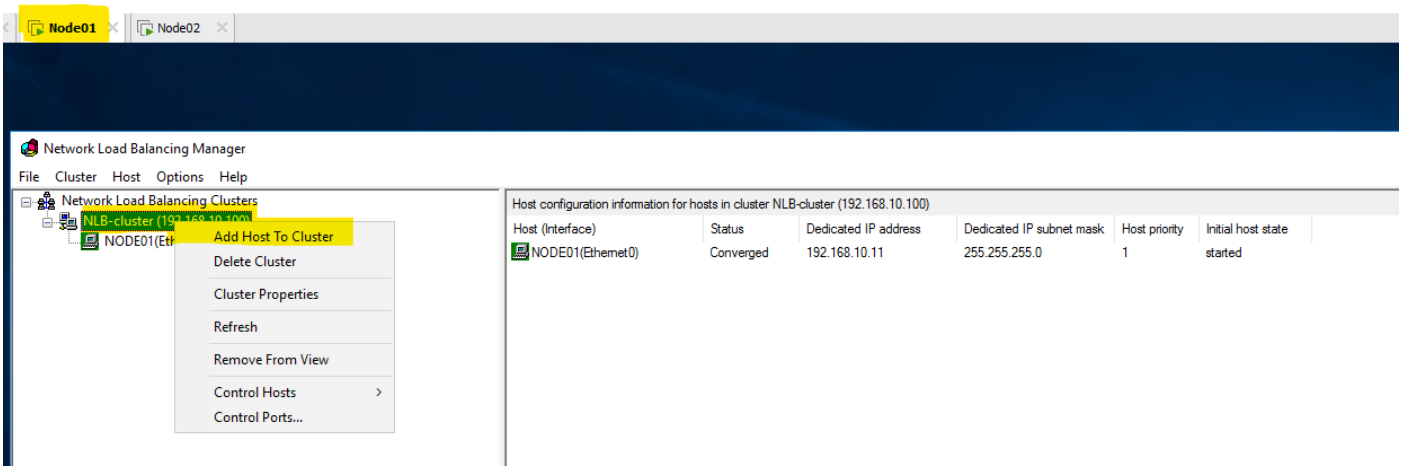
DNS:



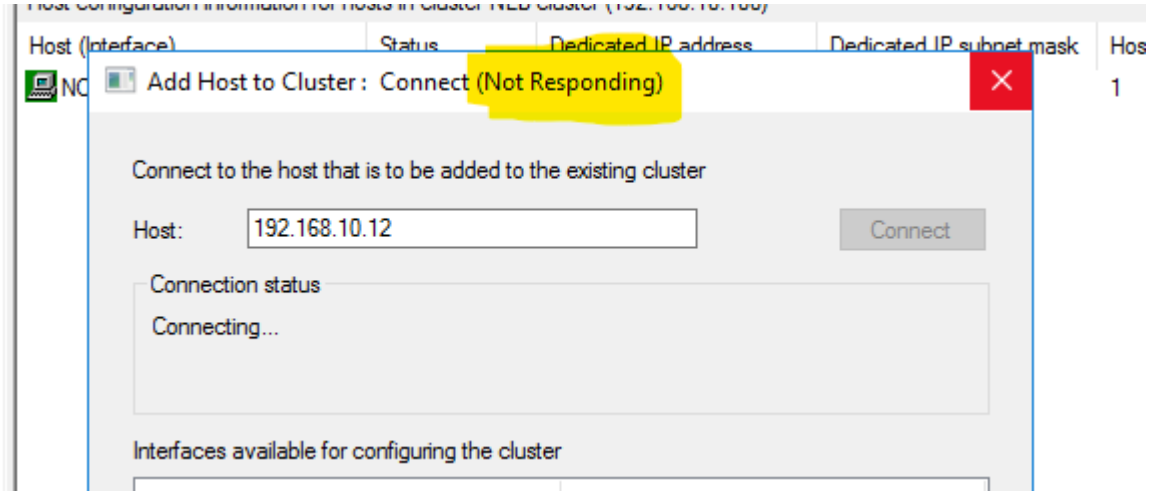
Verify on Node01's web browser:



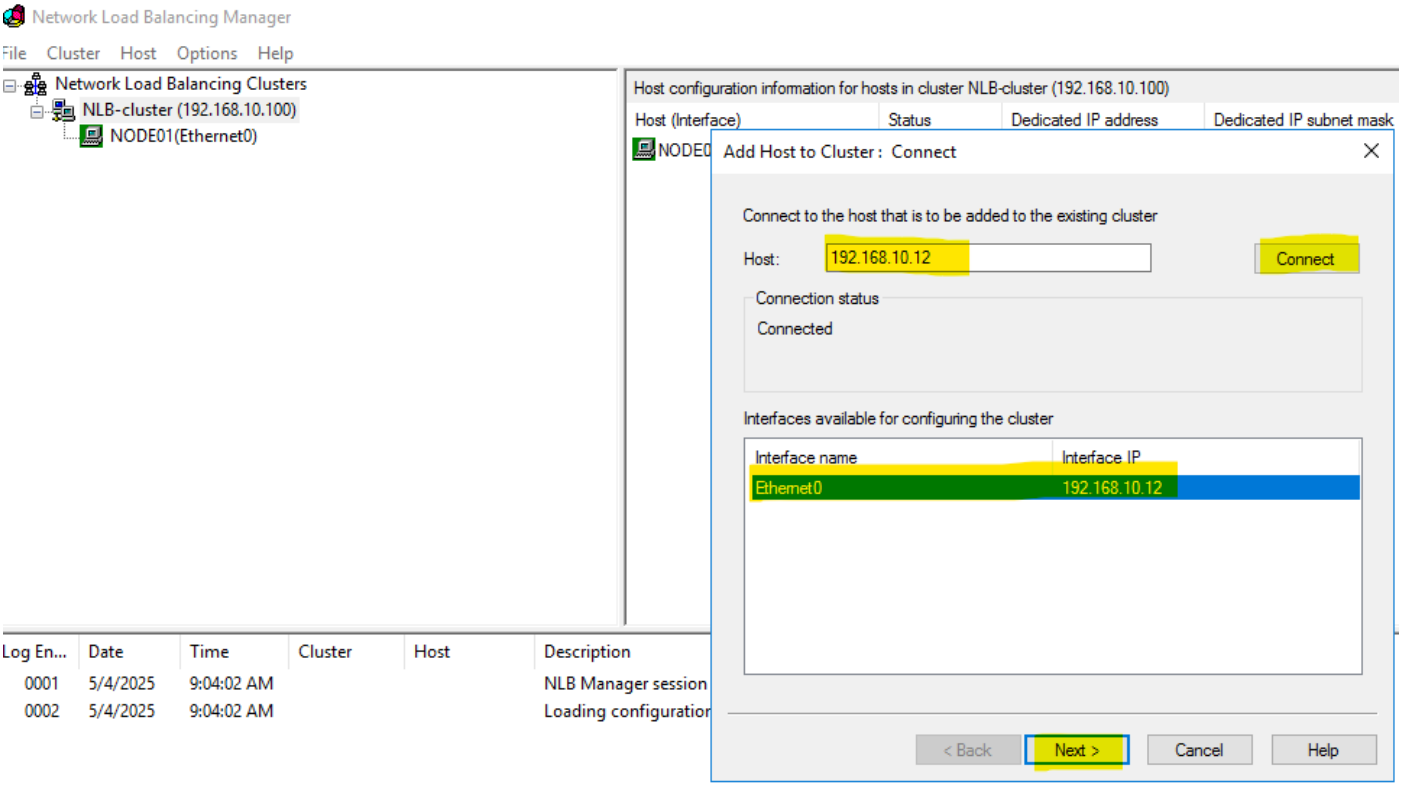
Now adding Node02 on Node01's Network Load Balancing Manager:



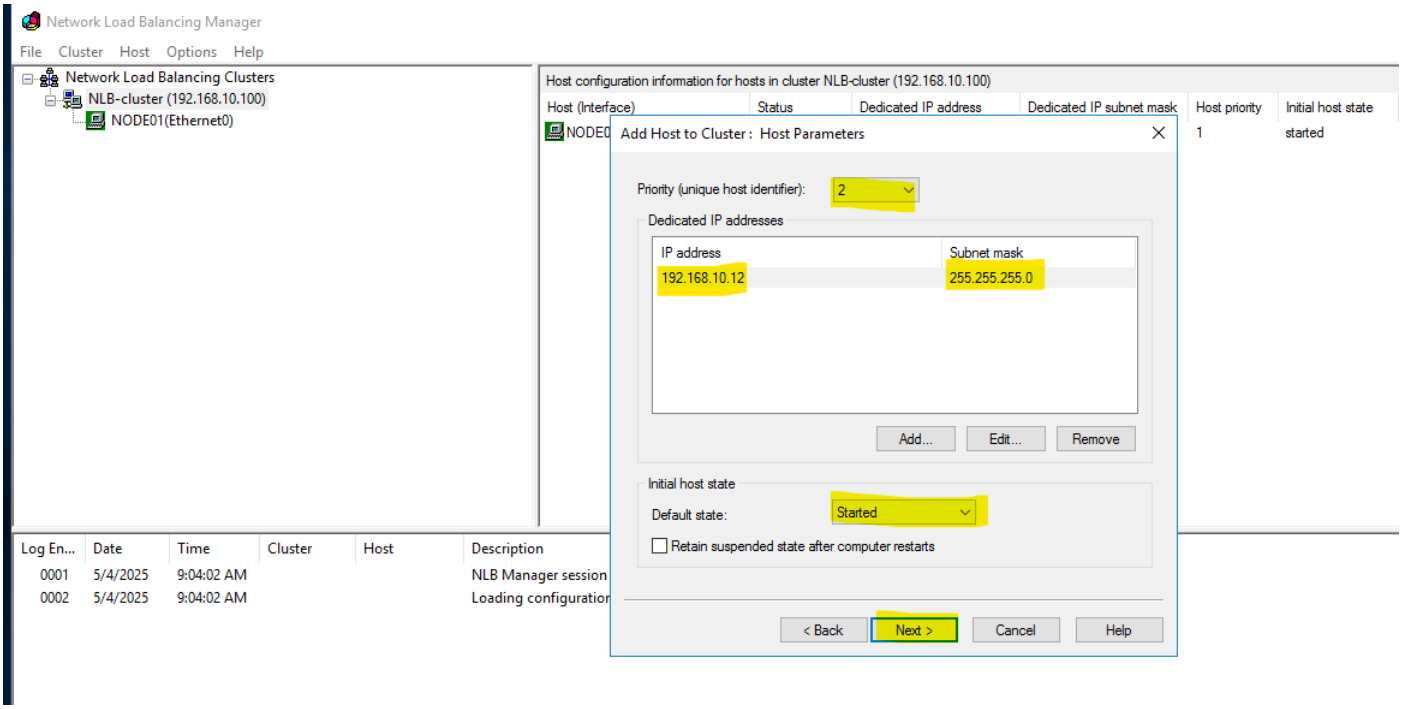
Which adding Node02(192.168.10.12), it is expected to see "Not Responding":



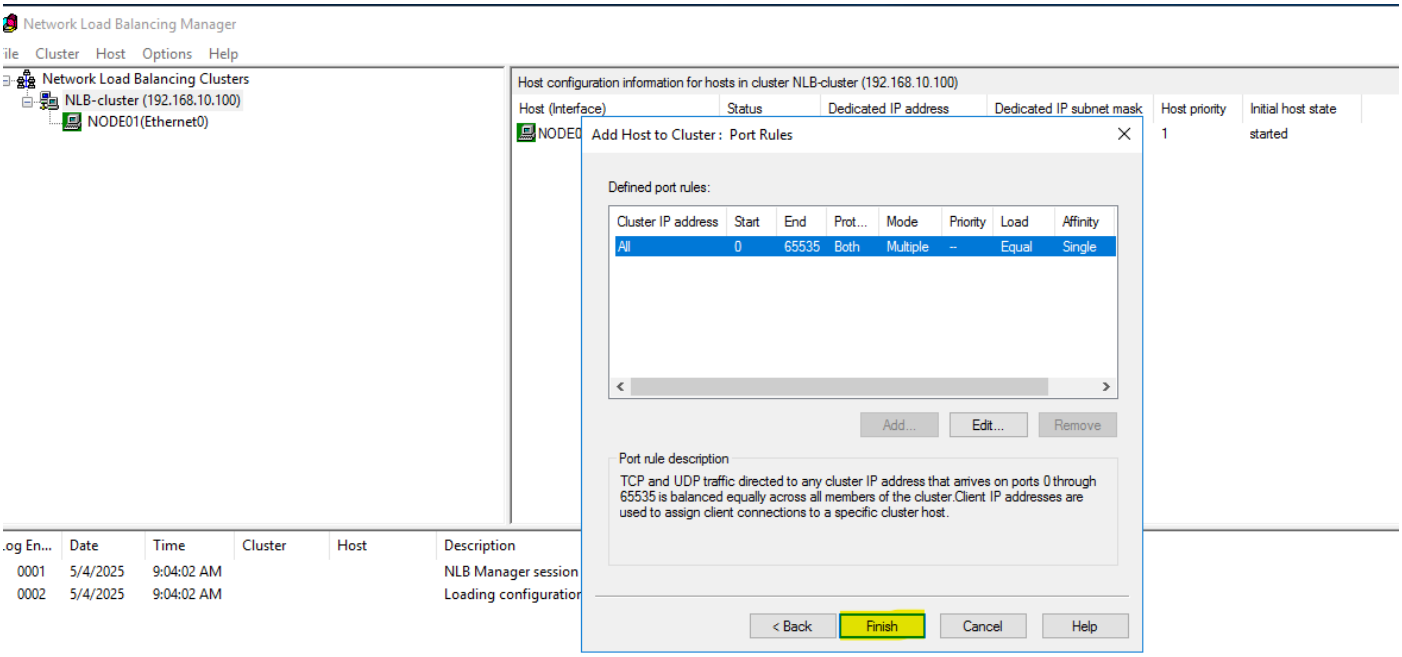
Click Next:



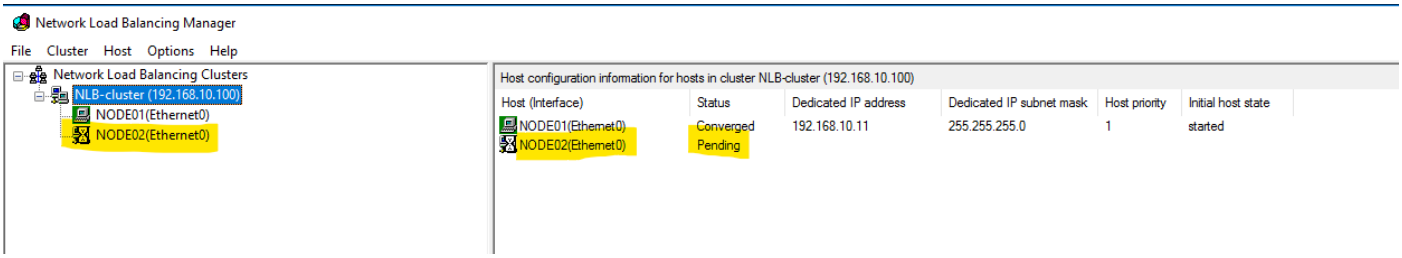
Verify the priority (as 2) & click Next:



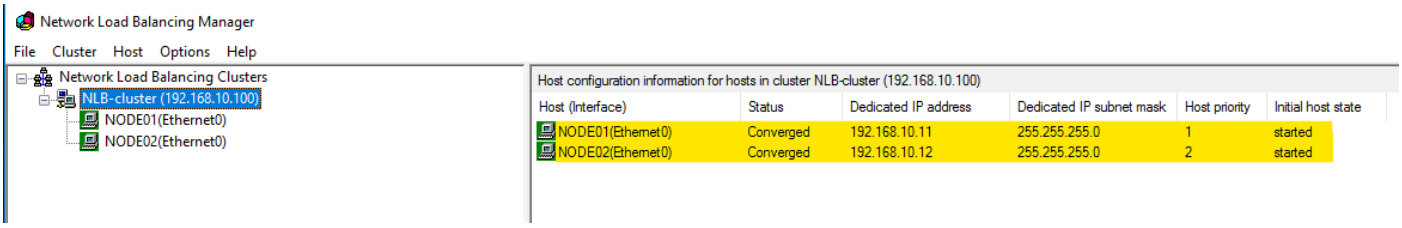
Click finish:



Wait until status changes:

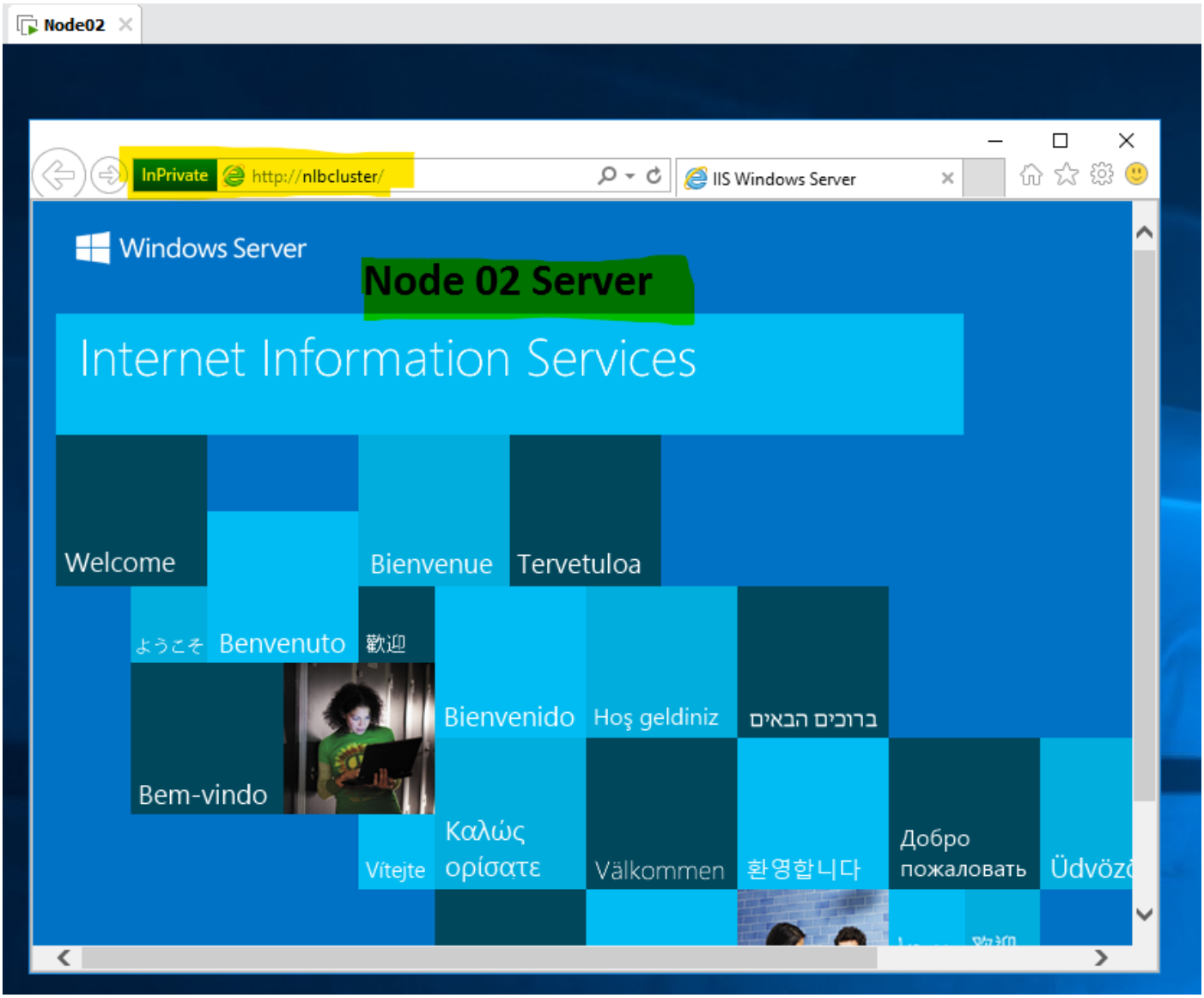


Else refresh the NLB cluster & verify:



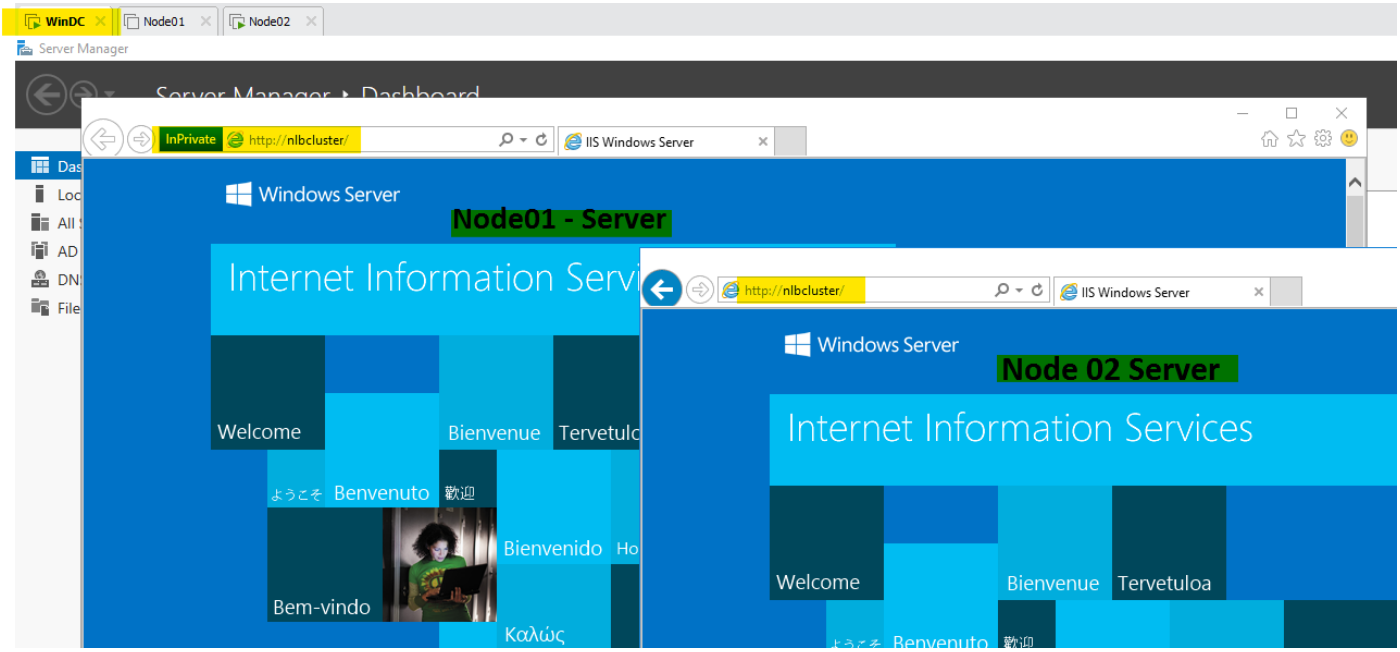
Now switch back to Internet explorer & copy the same UTL (http://nlbcluster) and paste it into incognito mode:

Or switch to Node02 and access the same URL (http://nlbcluster/)



To check if NLB is working or not, switch to DC machine and access the same URL in regular browser and in incognito mode:

Note – if it doesn't work, then turn of one node (say Node01) and then try:



Microsoft Deployment Toolkit (MDT):

- Microsoft Deployment Toolkit (MDT) is a free, powerful tool from Microsoft that helps automate the deployment of Windows operating systems and applications across computers in an organization.
- It supports both Lite Touch Installation (LTI) and integrates with System Center Configuration Manager (SCCM) for Zero Touch Installation (ZTI).

Key Features of MDT

- Automates deployment of:
  - Windows operating systems (Windows 10, 11, Server 2016–2022)
  - Drivers and applications
  - Updates and patches
- Supports:
  - Image creation and deployment
  - User State Migration (USMT)
  - Disk partitioning and formatting
  - Uses task sequences to define step-by-step deployment logic.
  - Generates bootable media (USB, ISO, or PXE boot with WDS).

Deployment Scenarios

Scenario	Description
Lite Touch Installation (LTI)	Requires minimal user interaction (used with bootable USB or PXE boot).
Zero Touch Installation (ZTI)	Fully automated (requires SCCM).
User-Driven Installation (UDI)	Users choose options via a GUI (with SCCM and MDT integration).

Components of MDT

- Deployment Workbench: GUI console to manage deployments.
- Deployment Share: Central repository for OS images, drivers, apps, and scripts.
- Task Sequences: Scripted workflows for installation.
- Bootstrap.ini & CustomSettings.ini: Configuration files that control deployment behavior.

What You Can Do with MDT

- Create and deploy custom Windows images (WIM).
- Add device drivers and OS patches during deployment.
- Automate domain join, user profile migration, and app installs.
- Integrate with Windows Deployment Services (WDS) for PXE boot support.

Advantages of Using MDT

- Free to use.
- Reduces manual effort and errors.
- Highly customizable and scriptable.
- Works well in both small and enterprise environments.
- Can be used standalone or integrated with SCCM.

Installing and configuring WSUS

What is WSUS?

WSUS allows administrators to:

- Download and store Microsoft updates locally.
- Approve or decline updates before deployment.
- Target specific computers or groups for different update policies.
- Save internet bandwidth by centralizing updates.

Prerequisites

- Windows Server 2016 installed and updated.
- At least 10 GB free disk space (40+ GB recommended).
- A working Active Directory environment (for GPO-based client control).
- Internet access or proxy configured (if required).

WSUS without a Domain (Workgroup Environment)

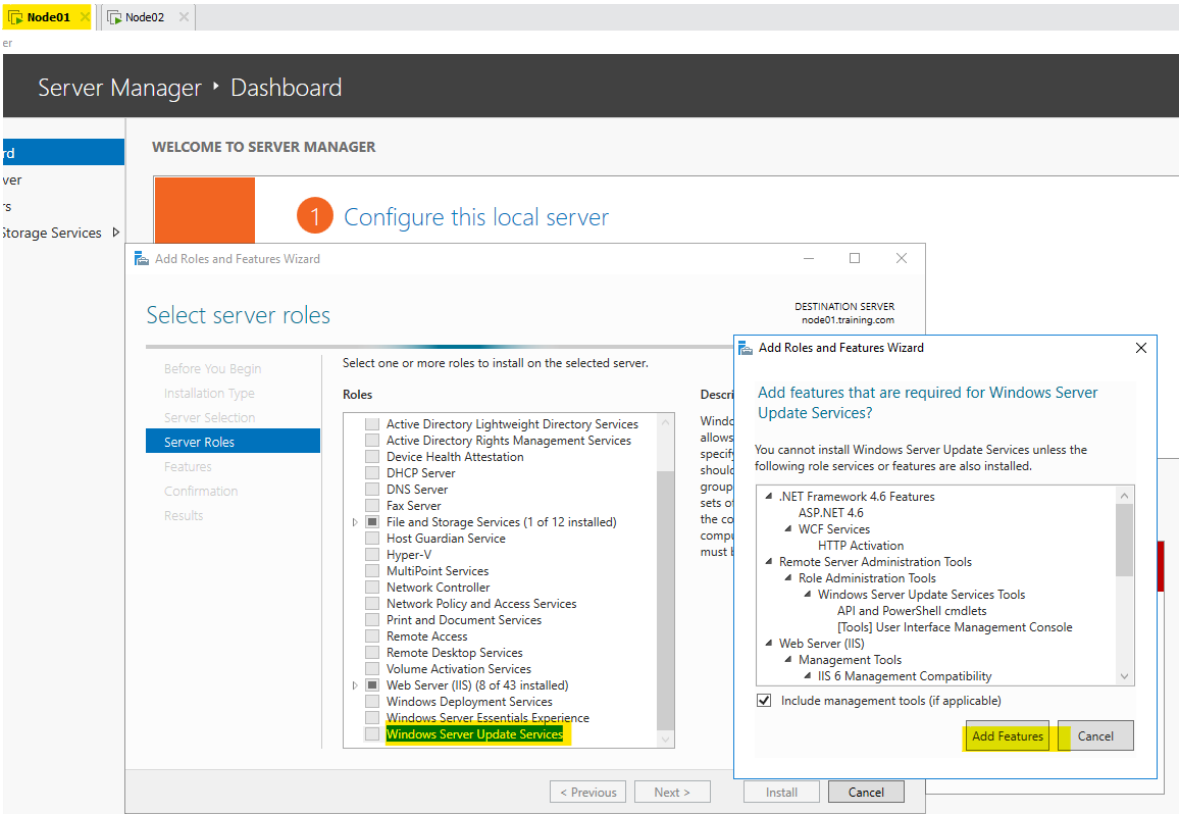
- WSUS can operate independently of a domain.
- Clients must be configured manually or via local group policy:
- Use gpedit.msc on each machine.
- Configure update server location (http://WSUS_Server:8530).
- No centralized client control via Group Policy Objects (GPO).
- Manual client grouping or use of client-side targeting in WSUS.

WSUS with a Domain (Recommended for Larger Environments)

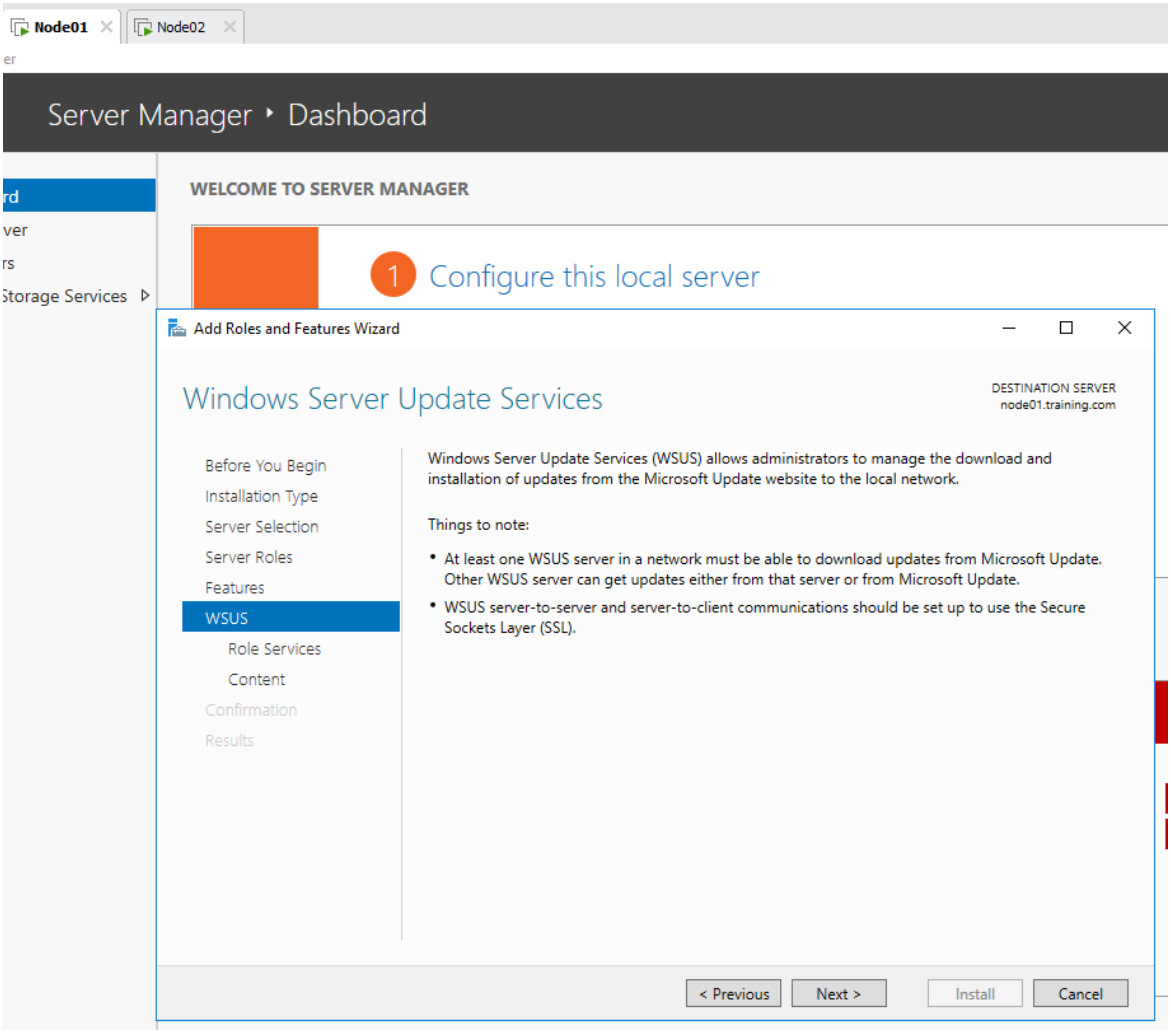
- Centralized management using Group Policy.
- Easier to:
    - Configure many clients at once.
    - Automate client grouping.
    - Enforce update compliance.
    - Ideal for enterprise or large network environments.

Steps to install WSUS on Node01:

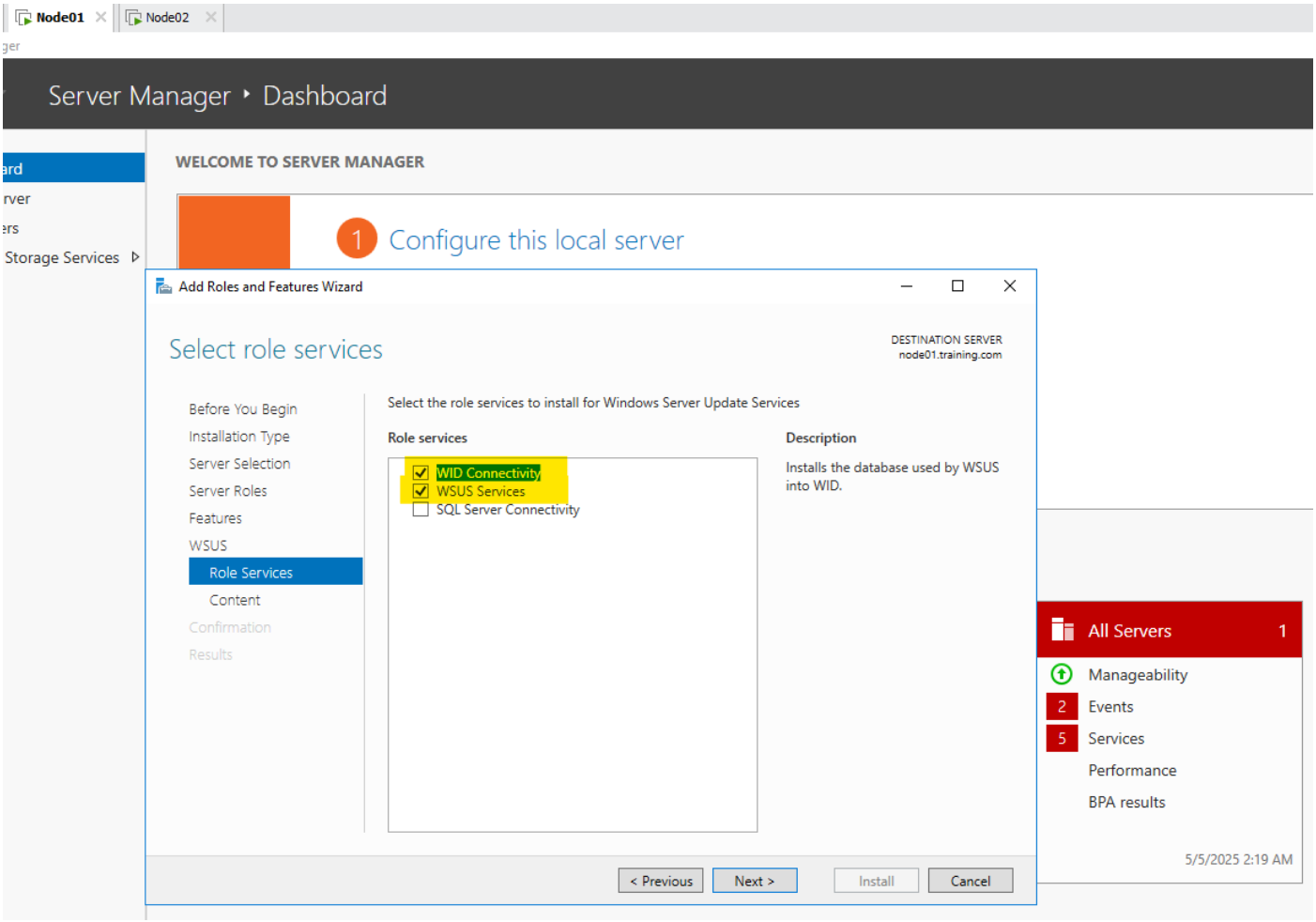
Server Manager → Manage → Add roles and features → Role (Windows Server Update Service)



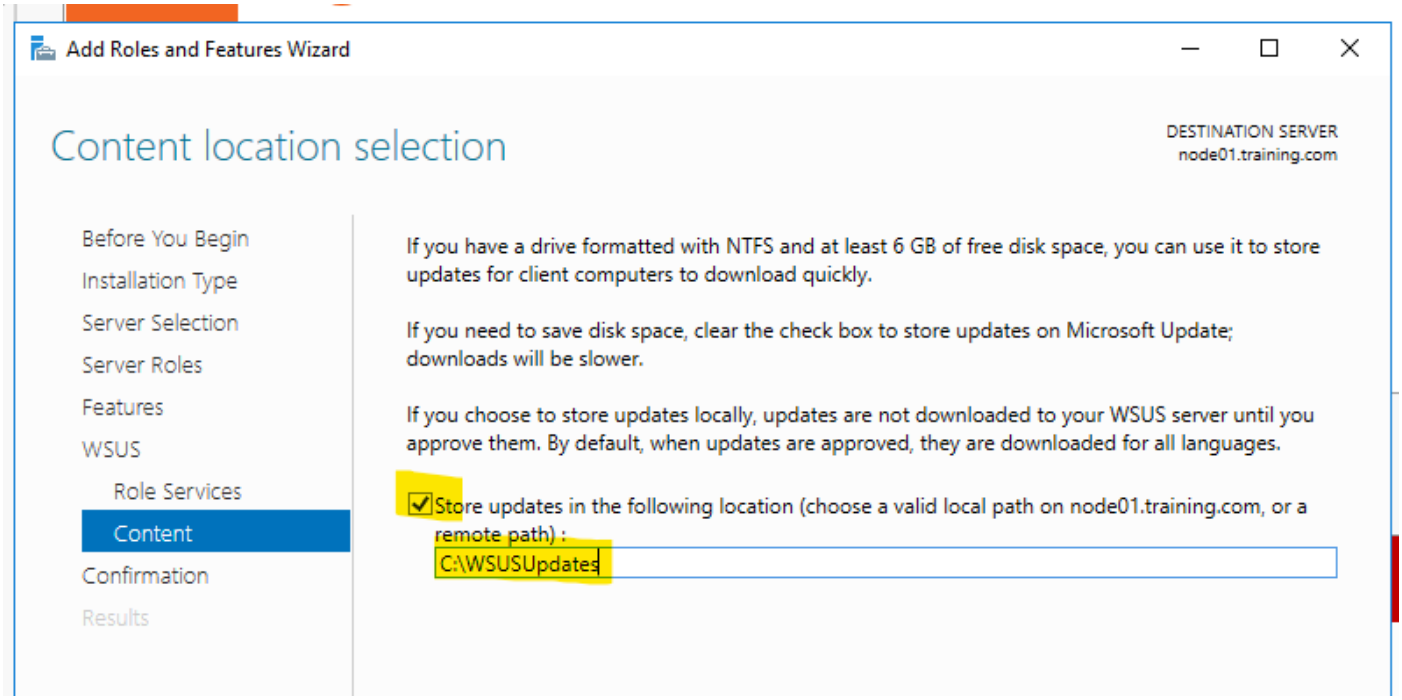
No features to be added:



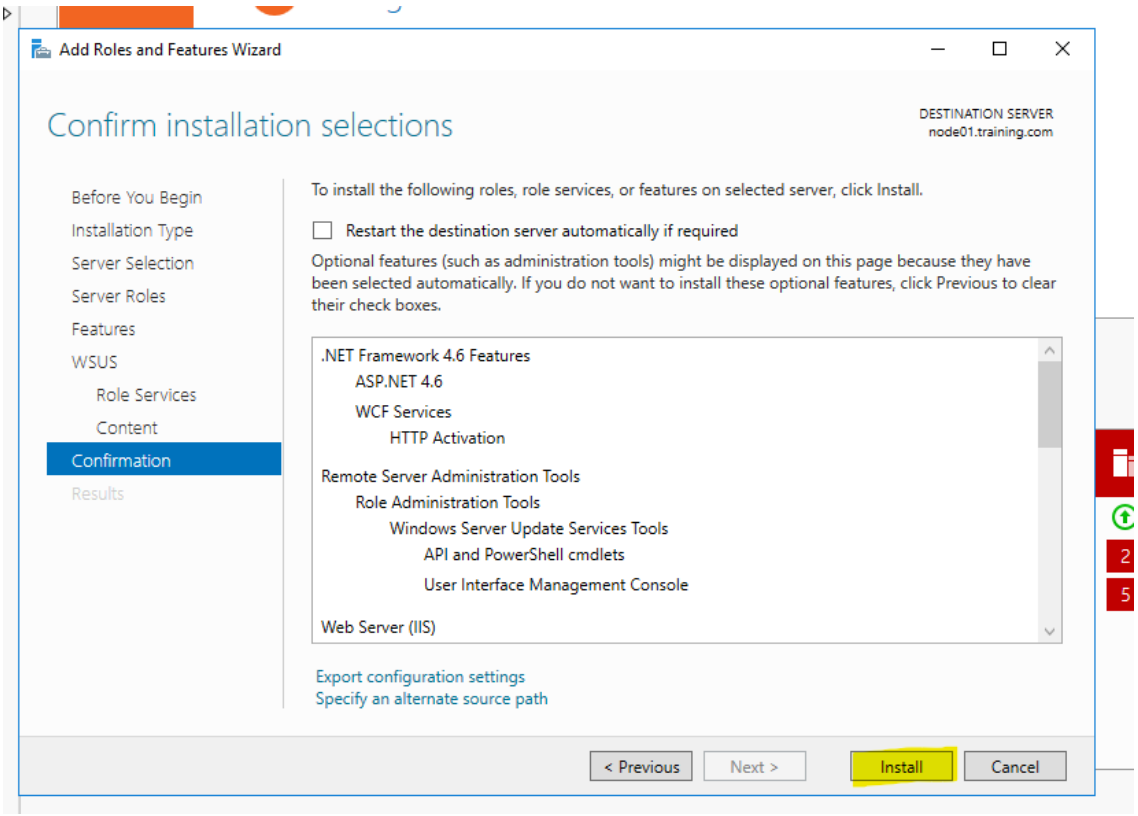
Select required role services:



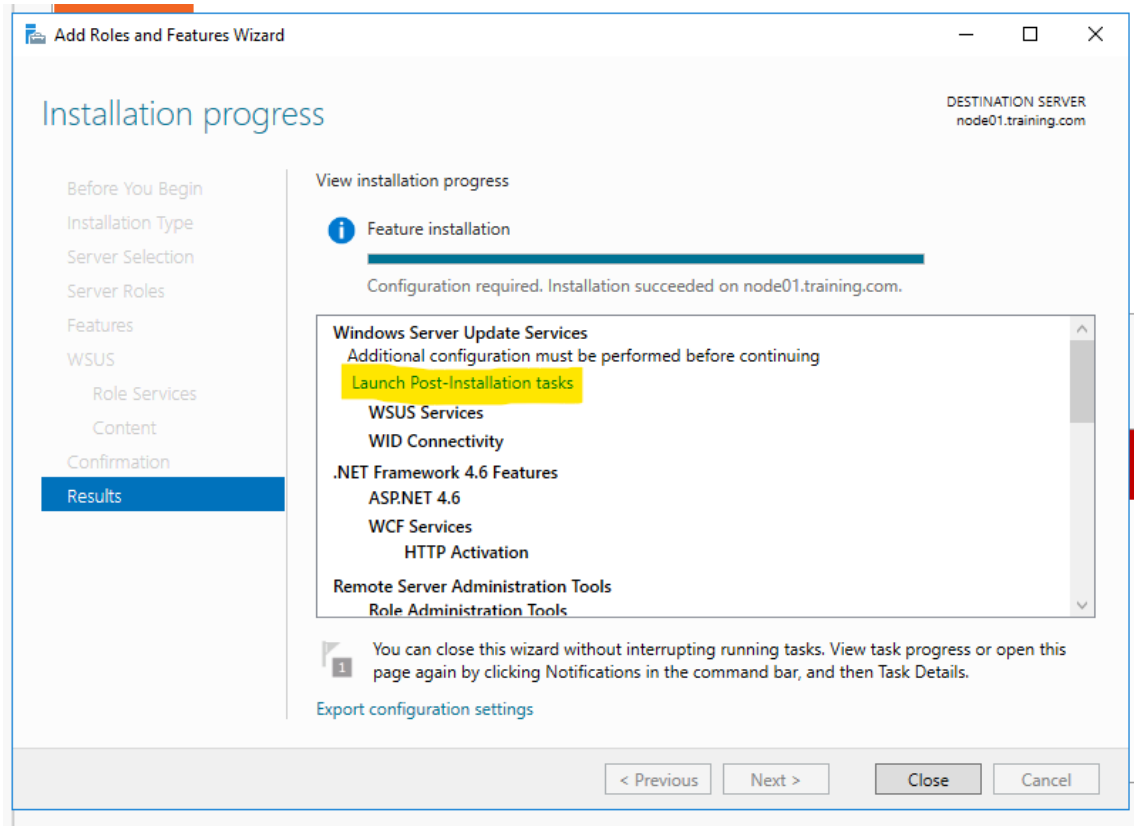
Adding path for storing updates (create new folder):



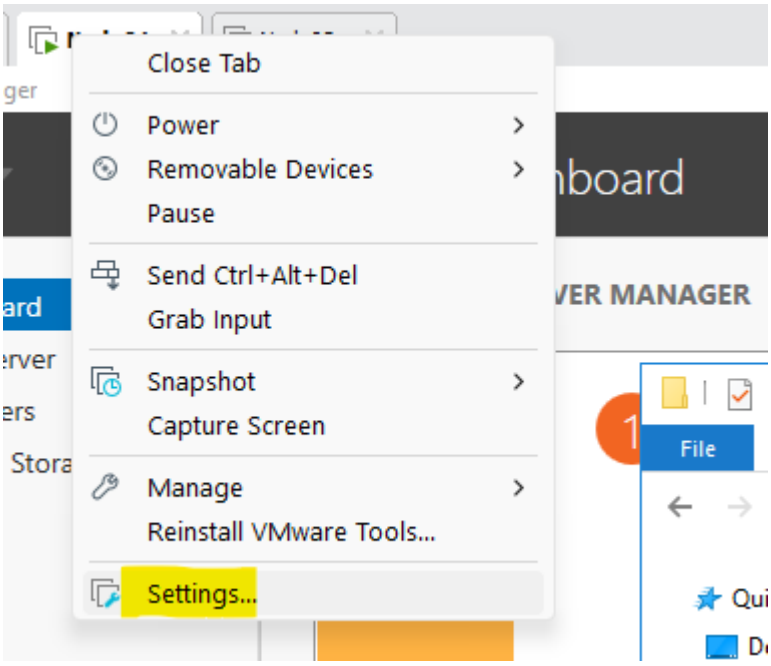
Install:



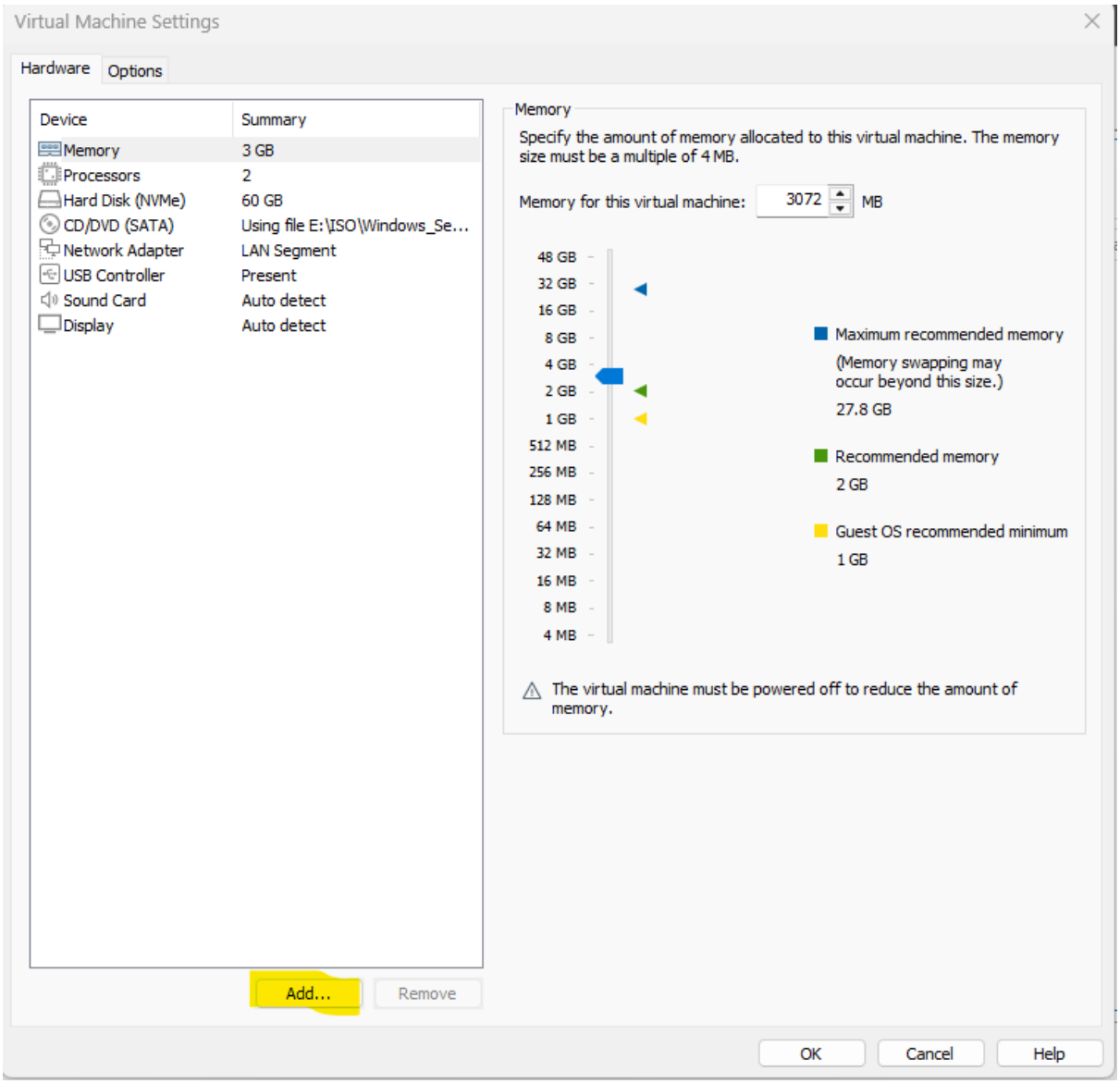
Click on “Launch Post-Installation tasks”



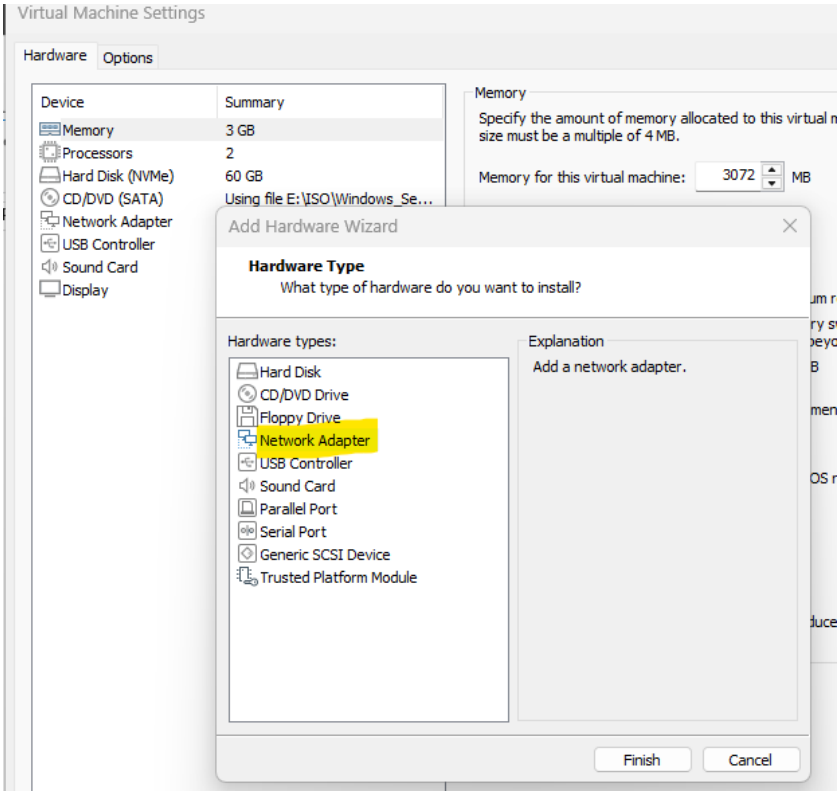
Add a new NIC card to node VM (Node01):



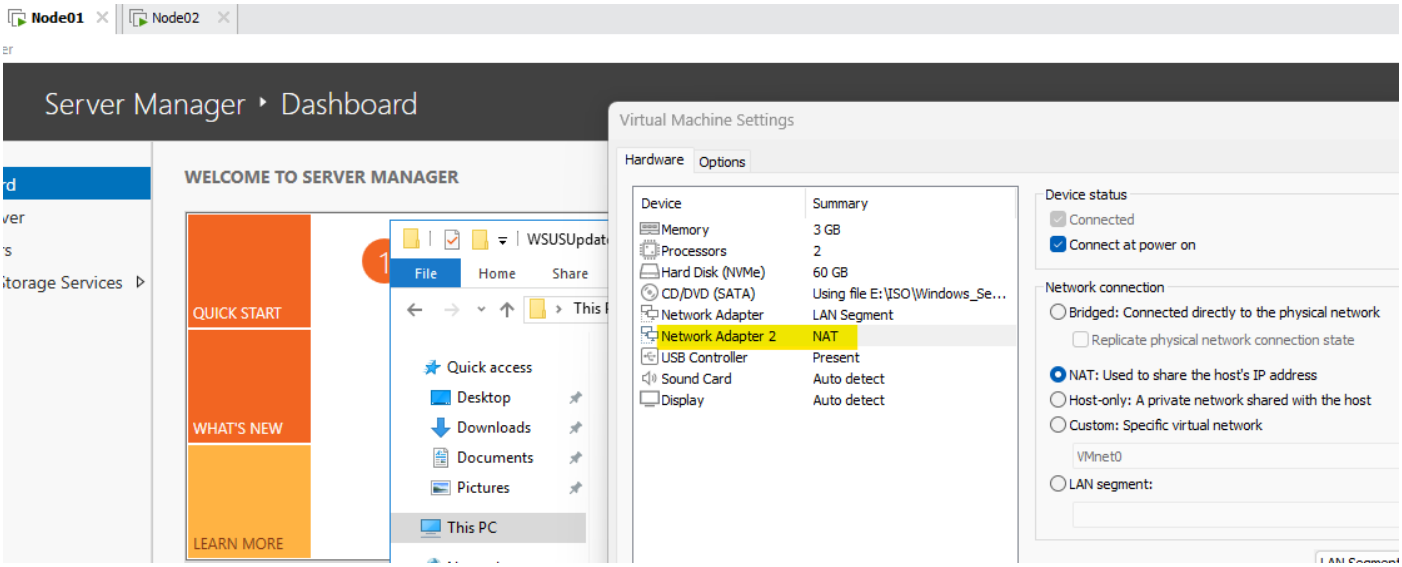
Click on “ADD”:



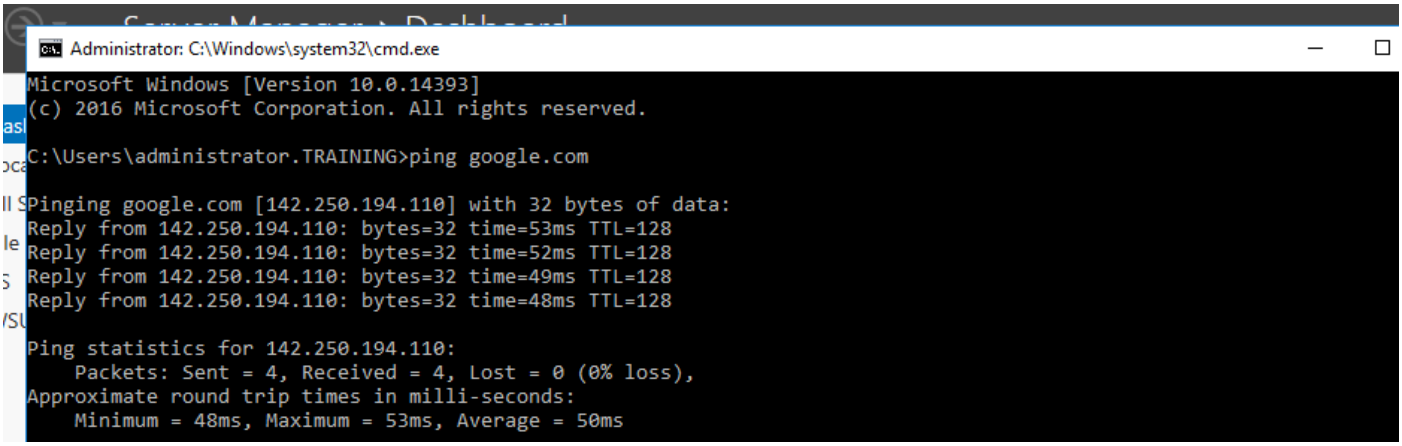
Select “Network Adapter”:



Ensure that new network adapter is on NAT:

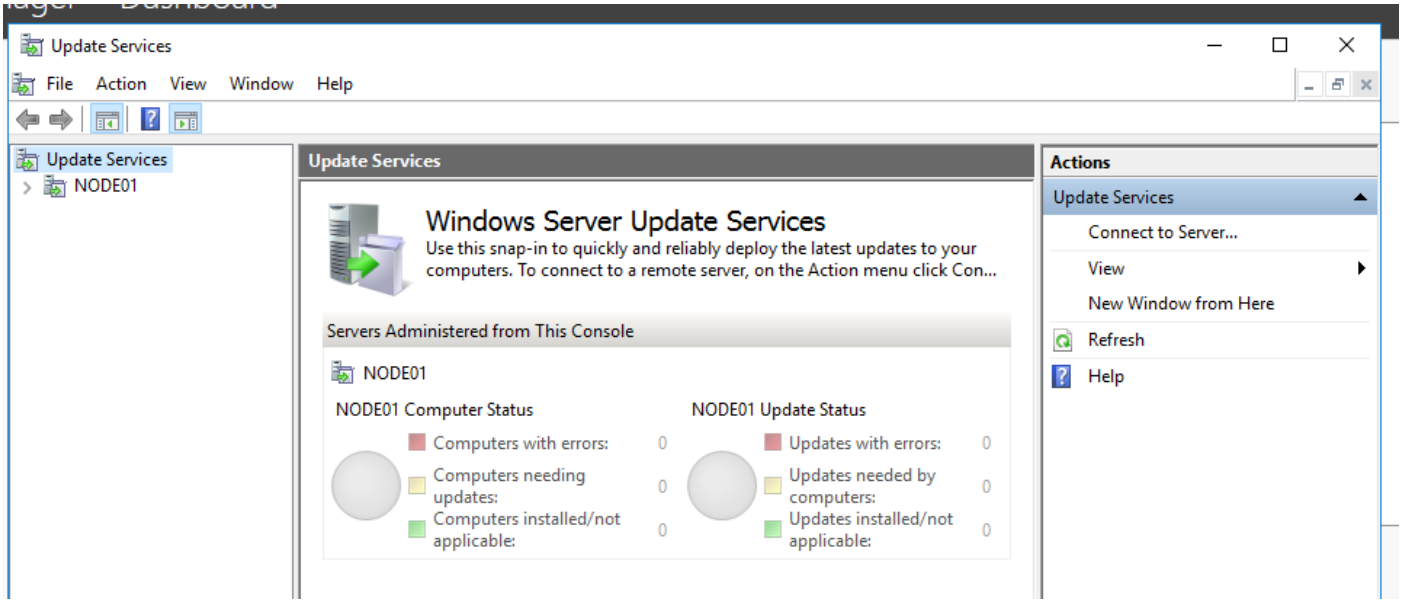


Now ping Google.com to test if internet is working:

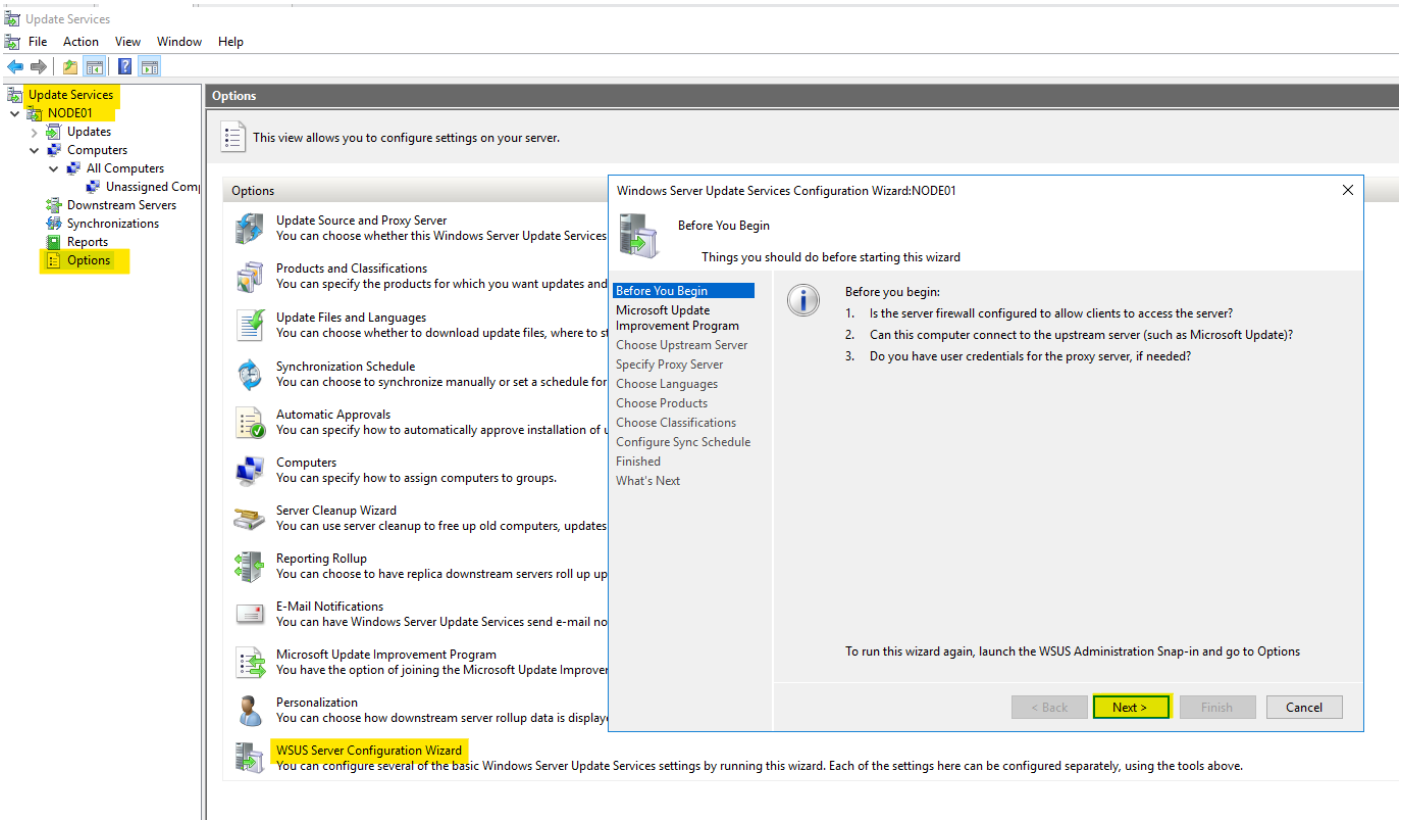


Configuring WSUS on Node01:

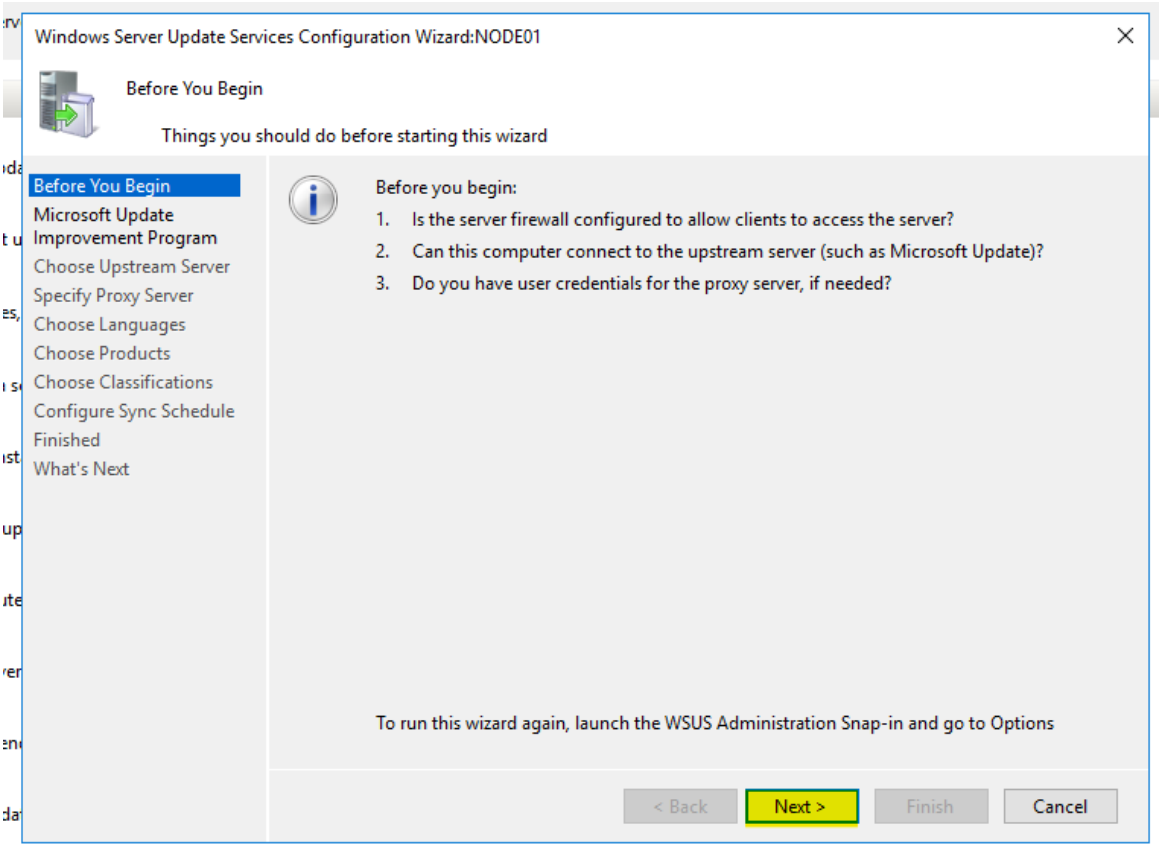
Server Manager Dashboard Page → Tools → Windows Server Update Service



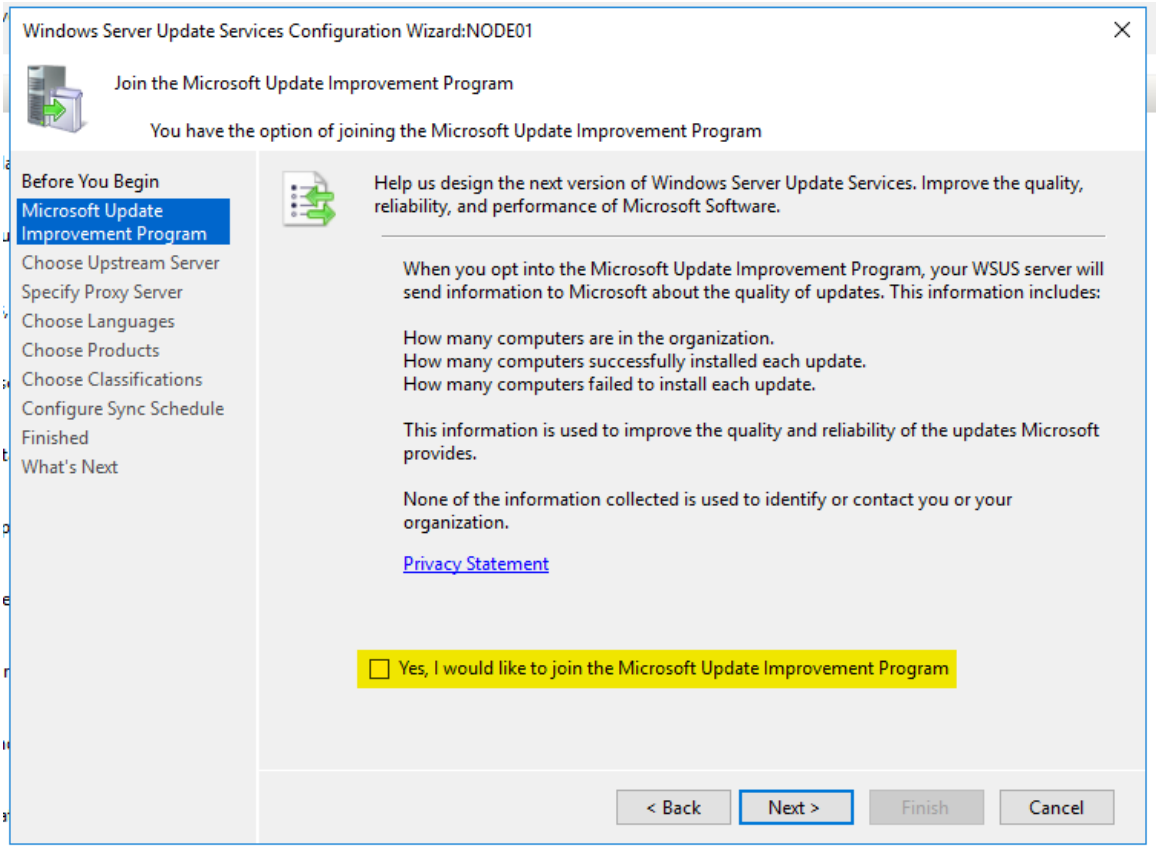
To configure WSUS configuration, Tools → Windows Server Update Service Console (select Options on left side):



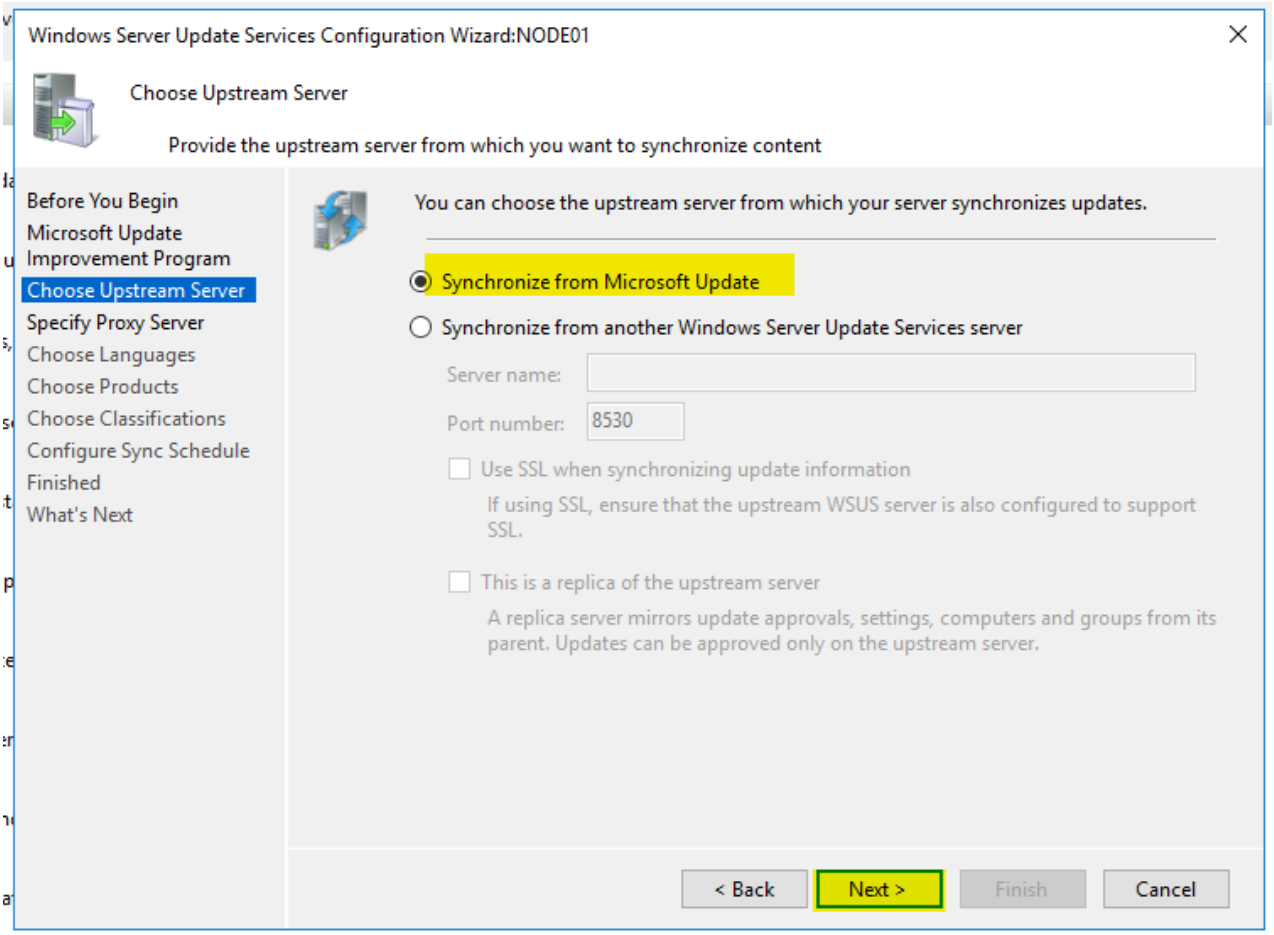
Click Next on “Before You Begin”:



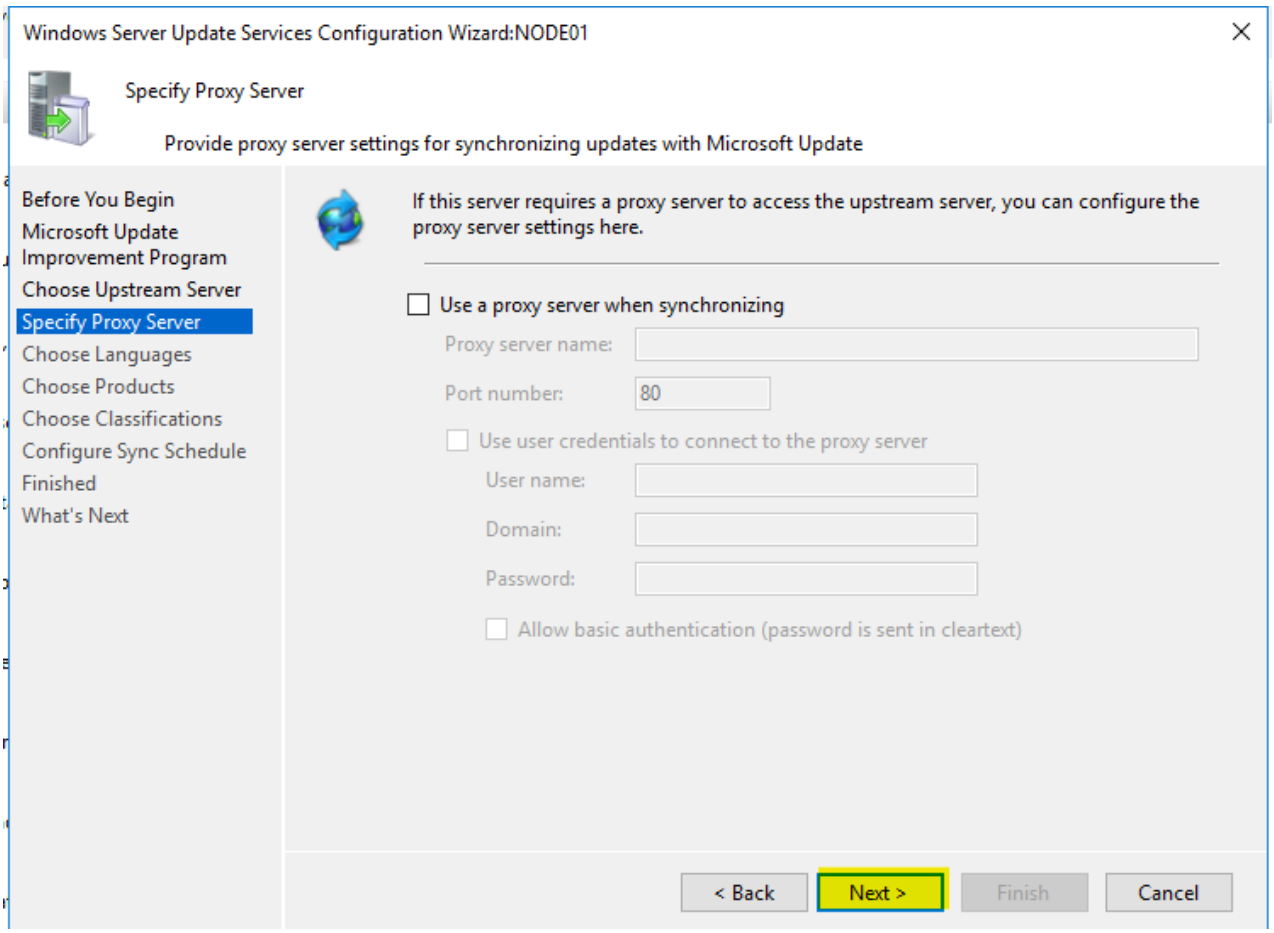
Untick “Yes, I would like to join Microsoft Update improvement program”



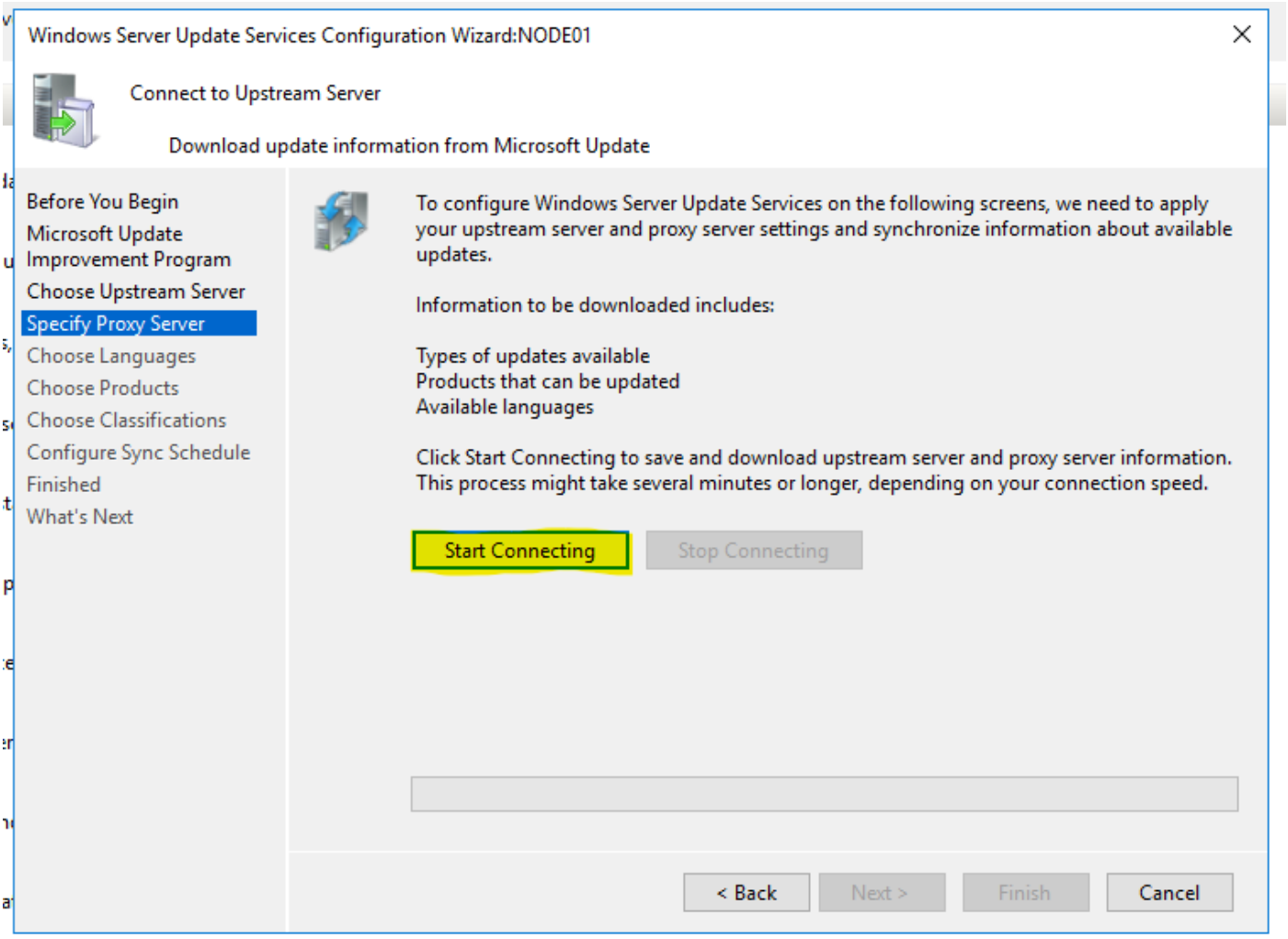
Select “Synchronize from Microsoft Update”, as we are connected to internet:

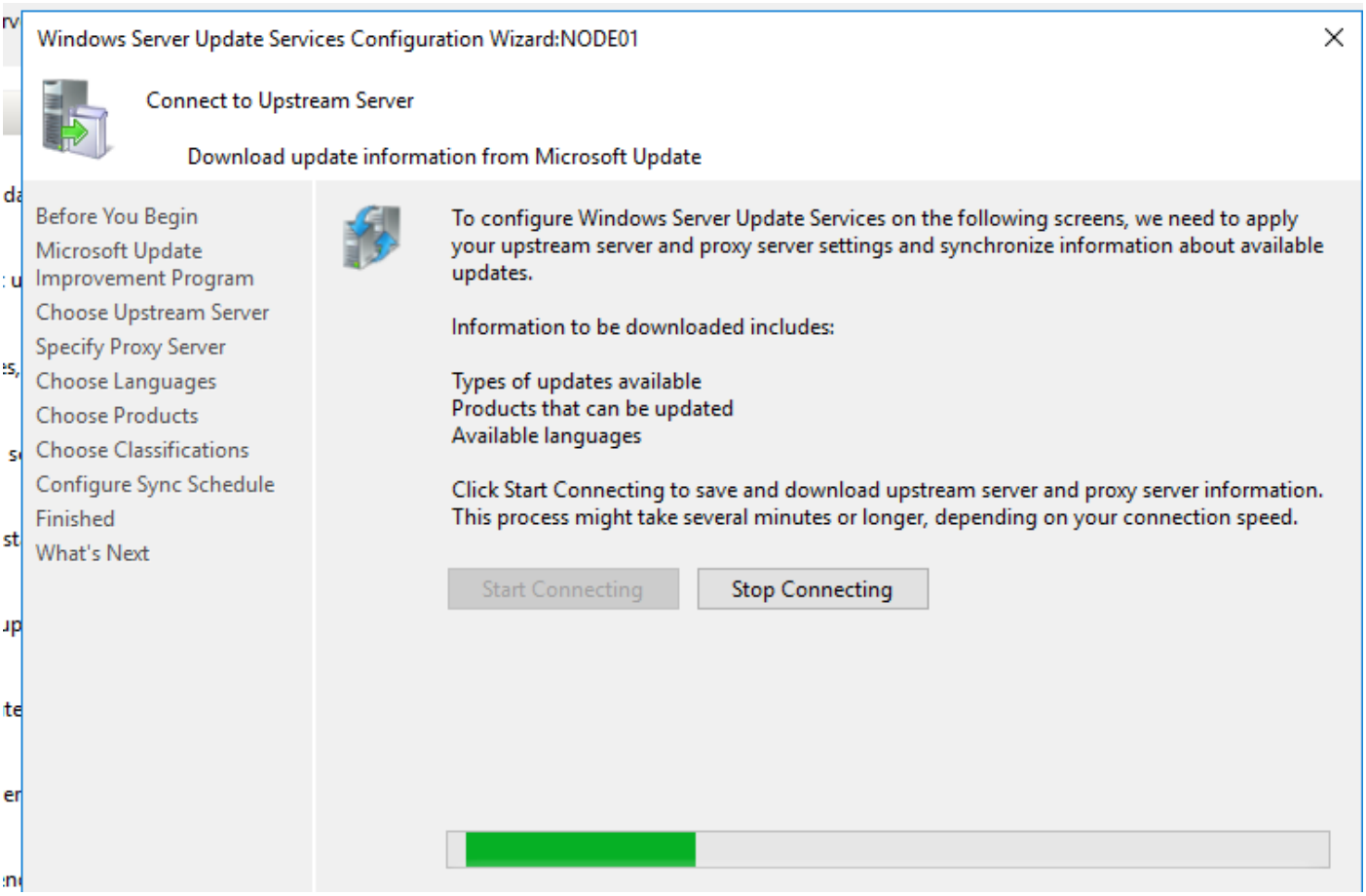


Leave the proxy server page and click Next:

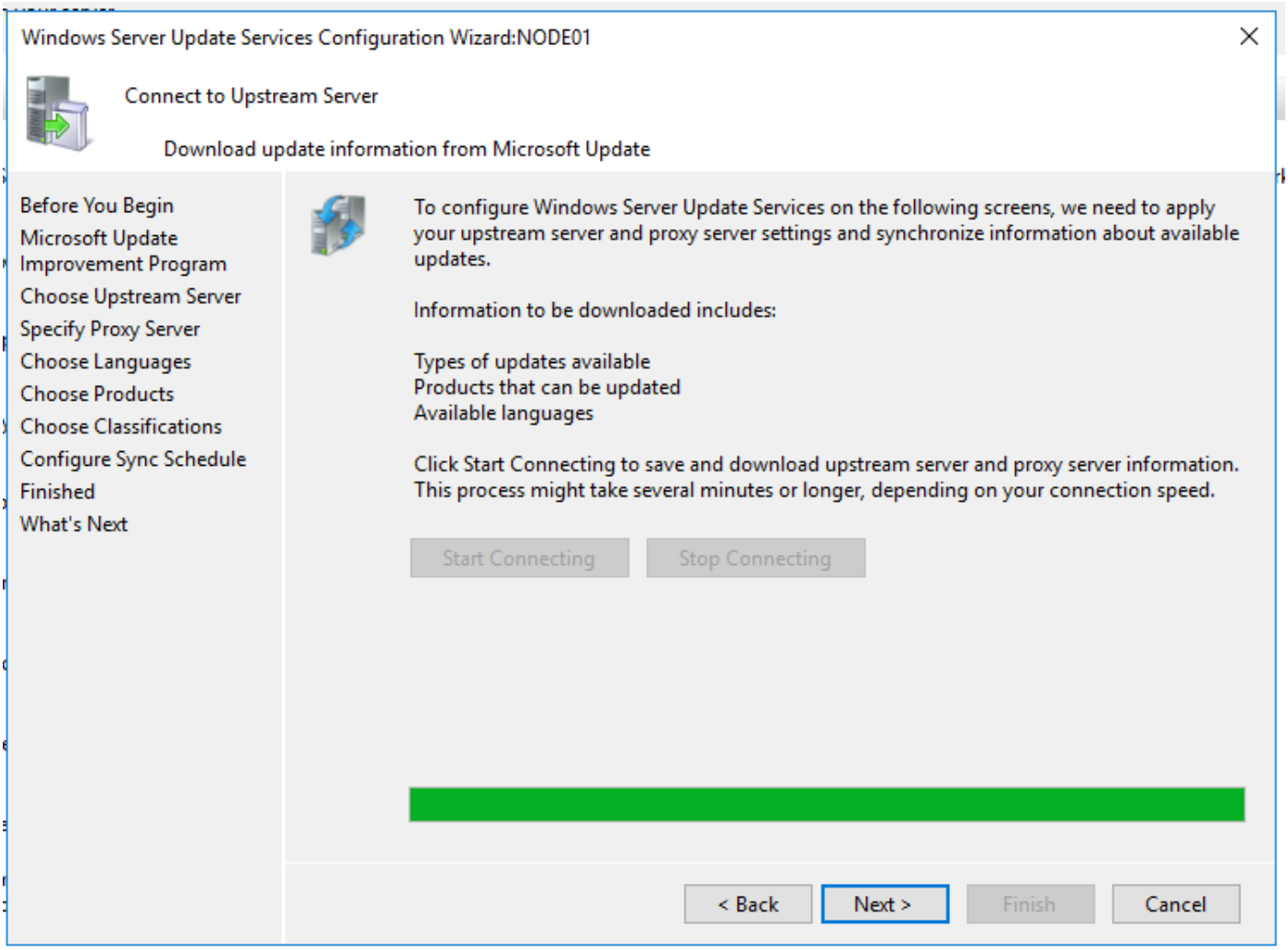


Click on “Start Connecting”:

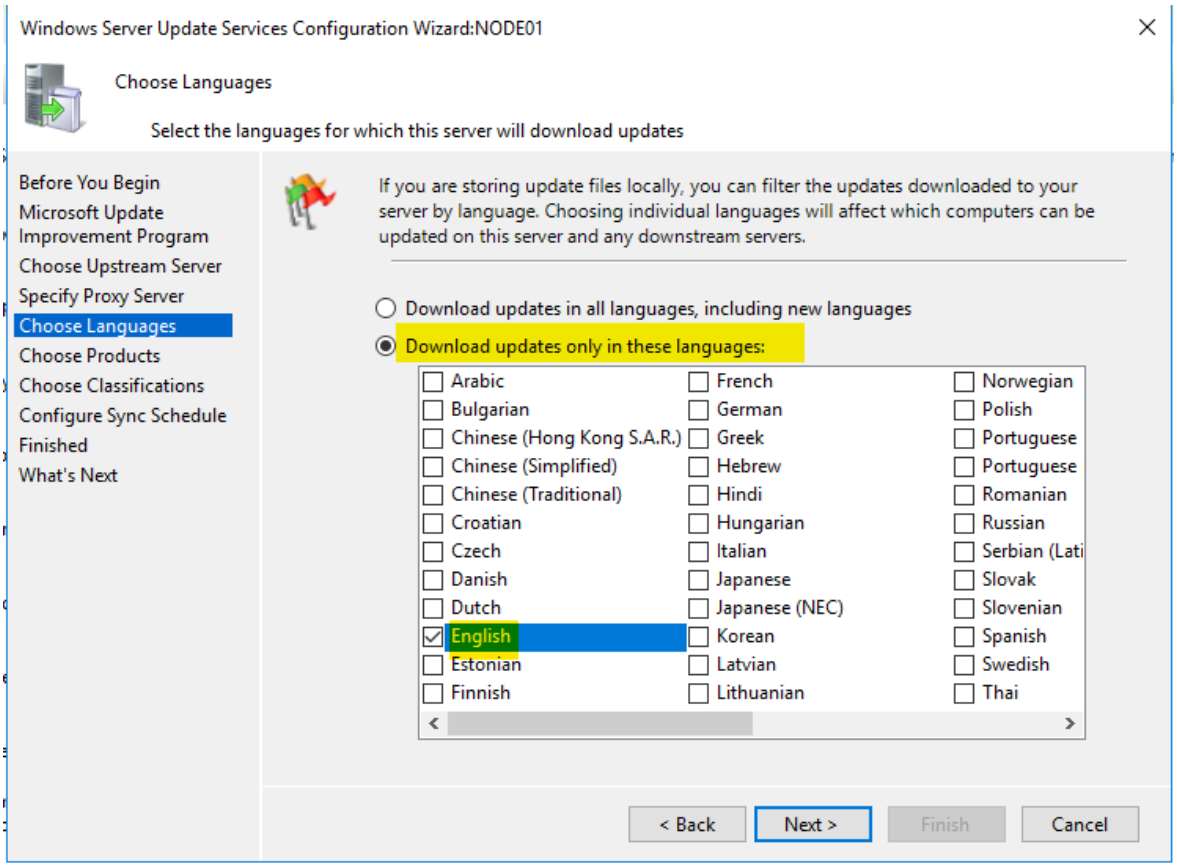




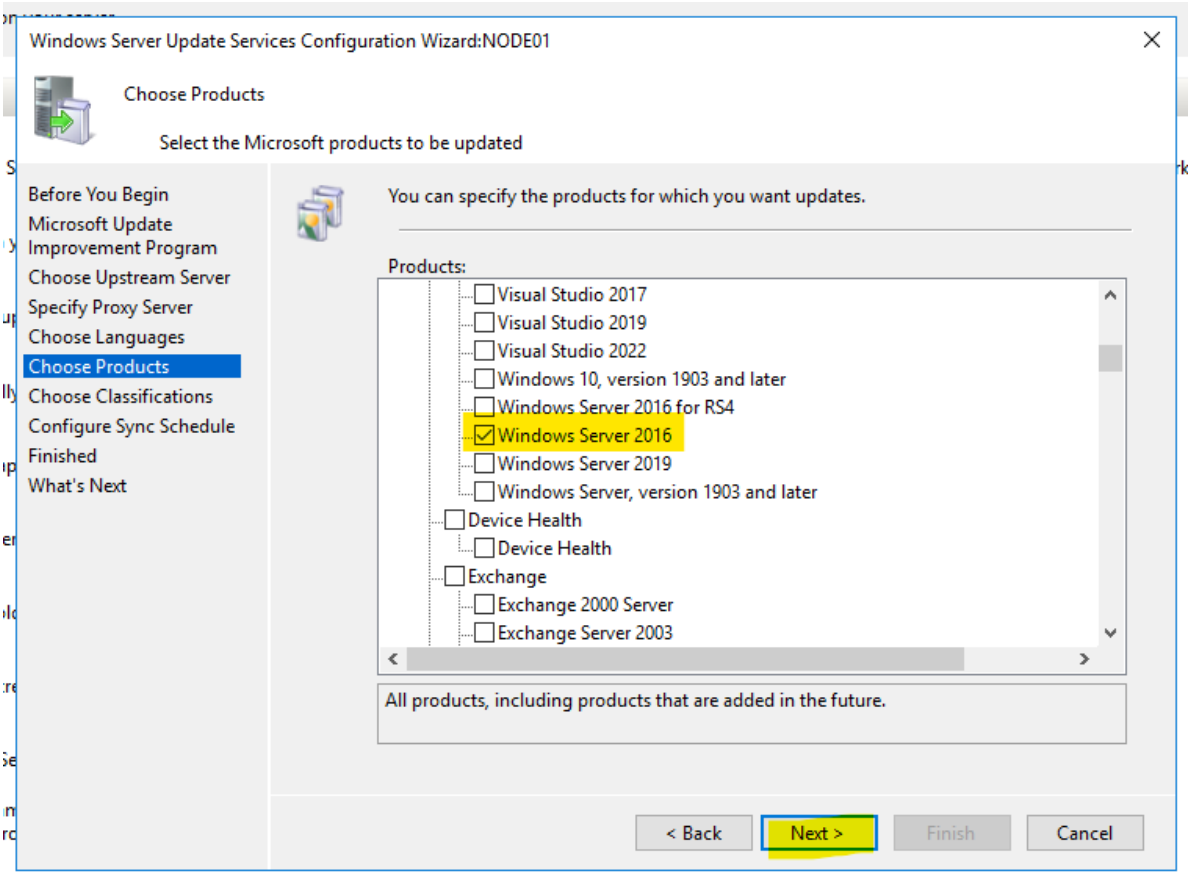
Approx. after 30mins the update was complete. Now click on Next:



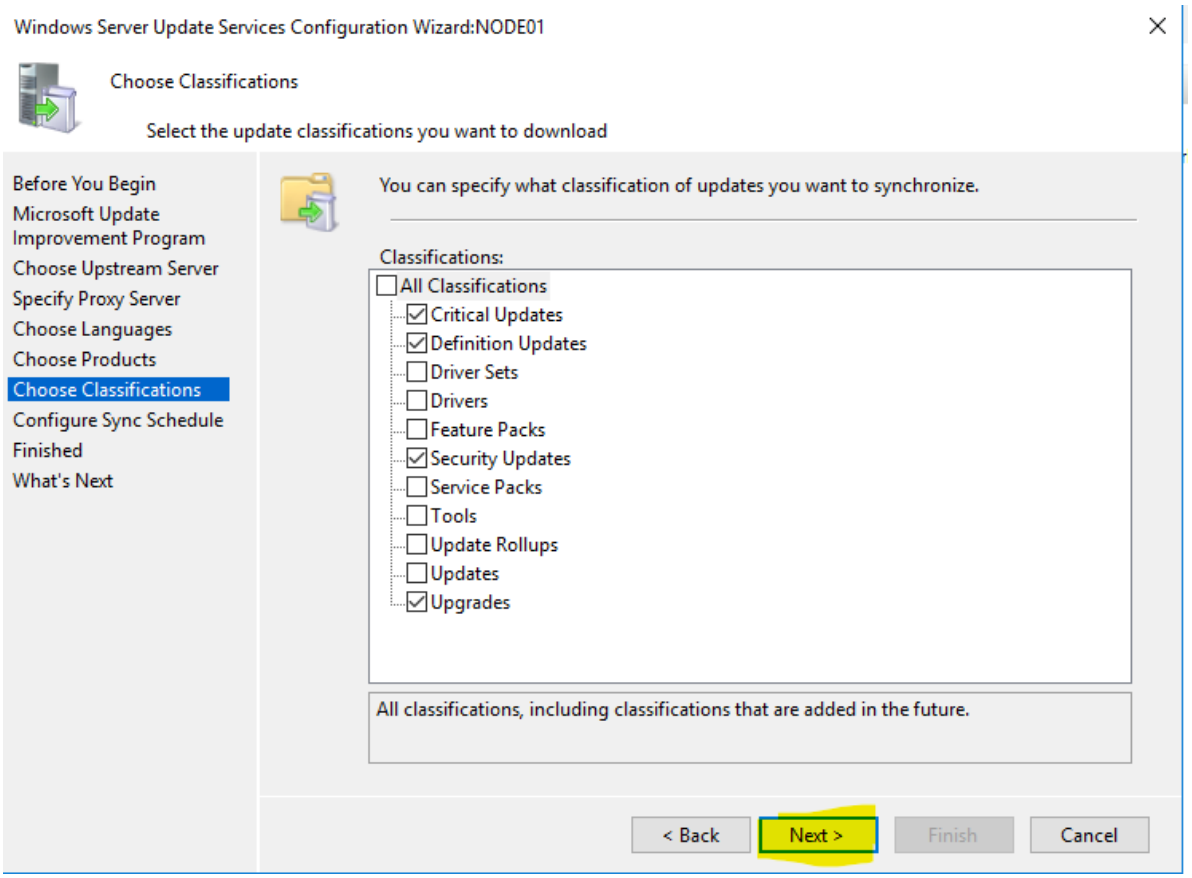
Select English language:



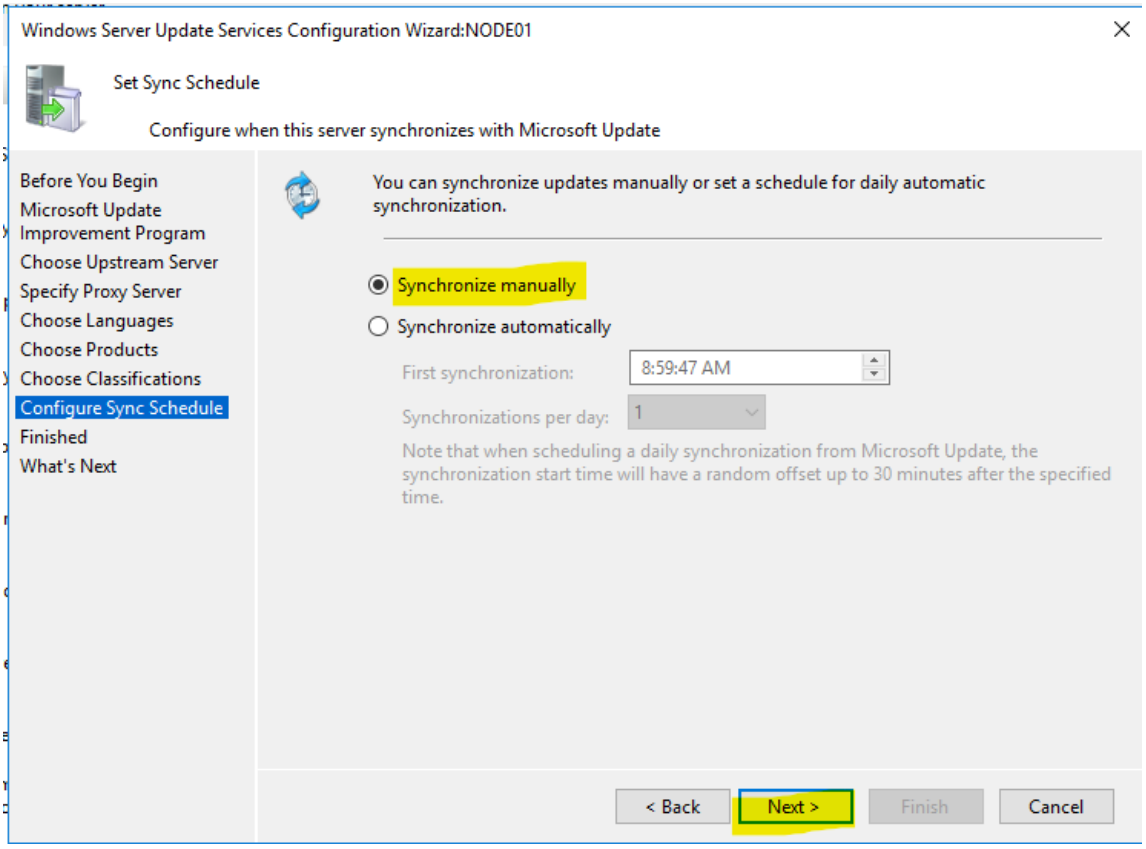
Select appropriate product (depending upon requirement):



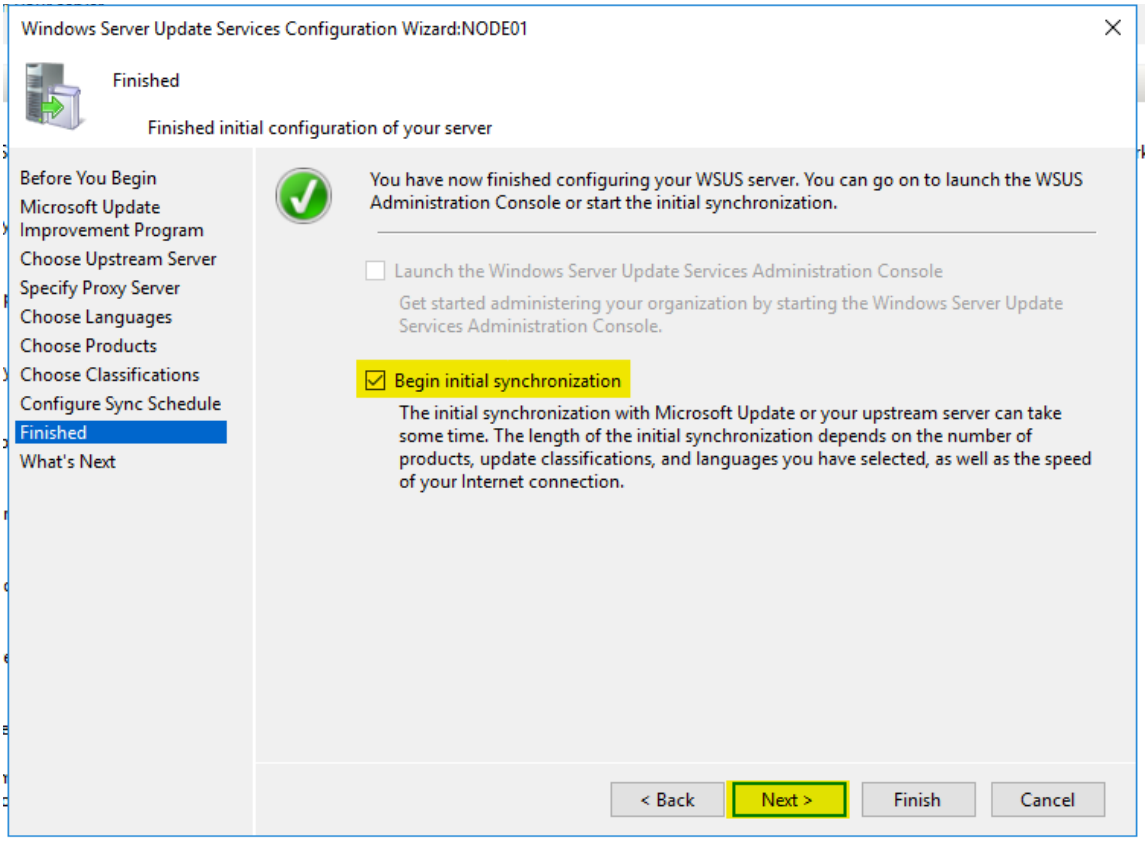
Select the required classification:



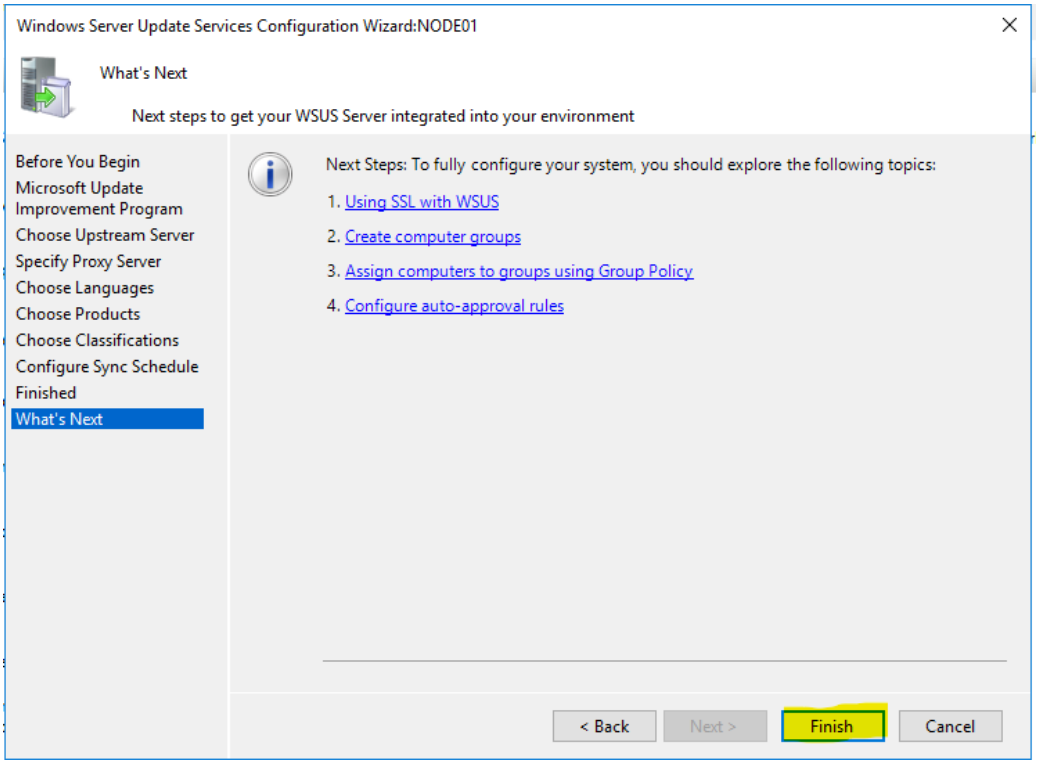
Select the sync time. We will select Manually as we will be using GPO for the updates:



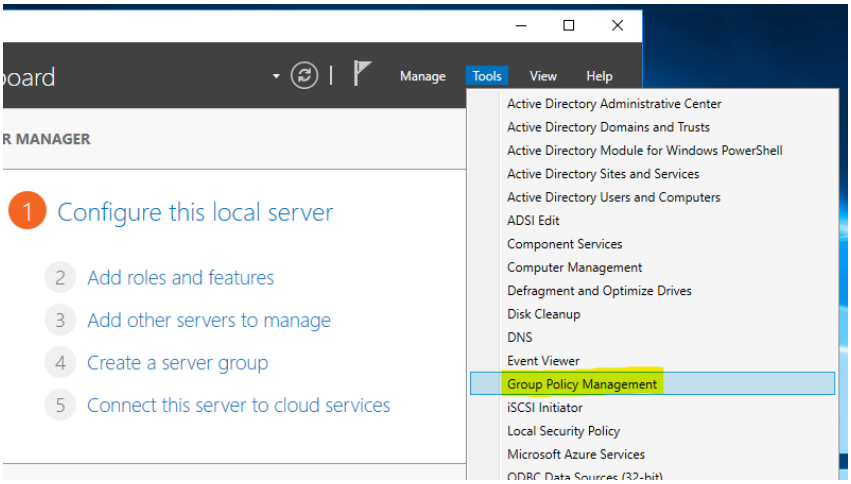
Check “Begin initial sync”:



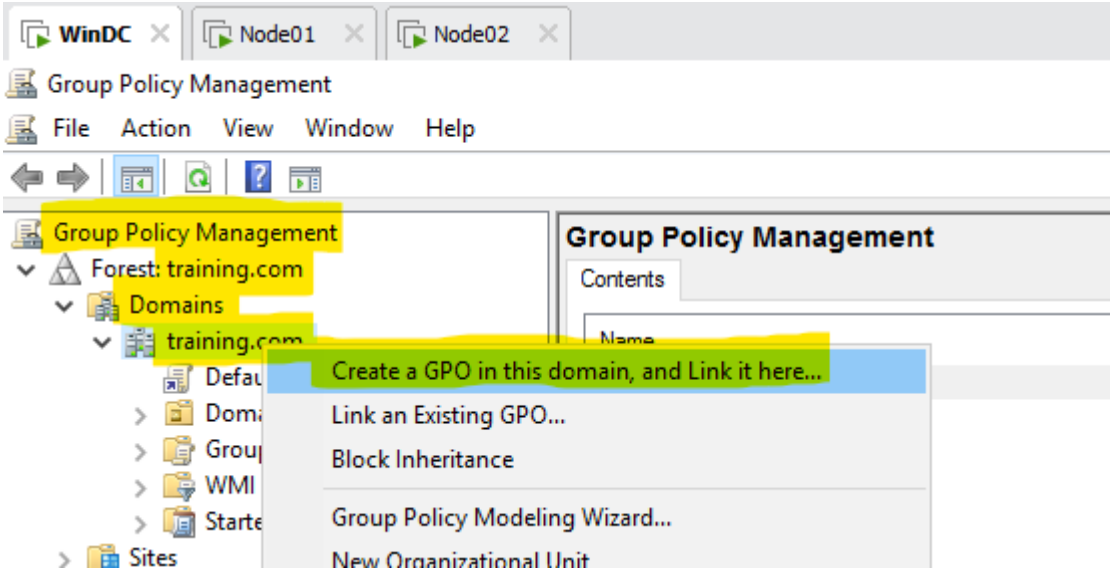
Finish the configuration:



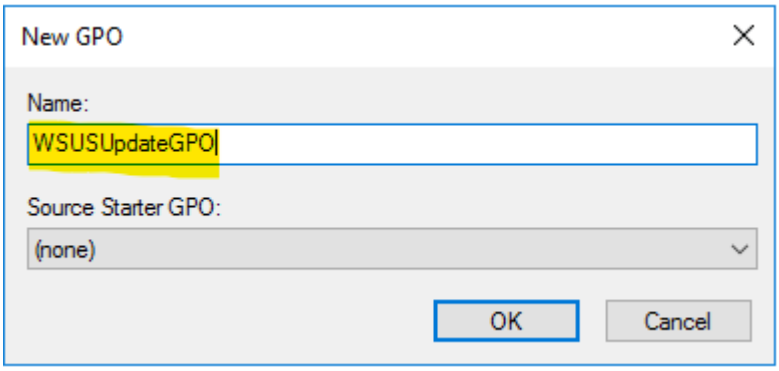
Configuring Group Policy for WSUS on DC machine:



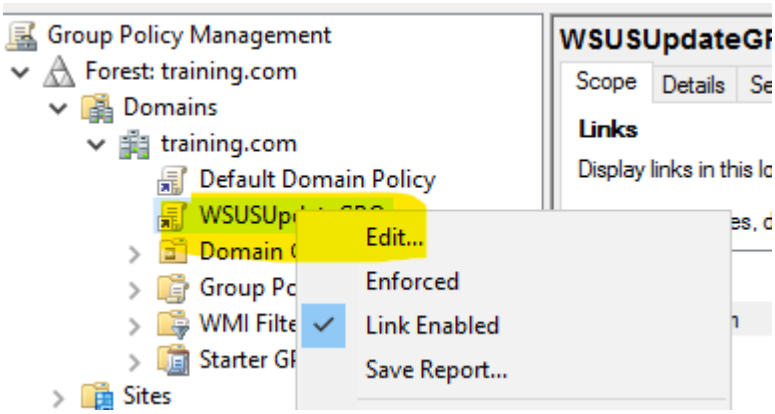
Create a new GPO:



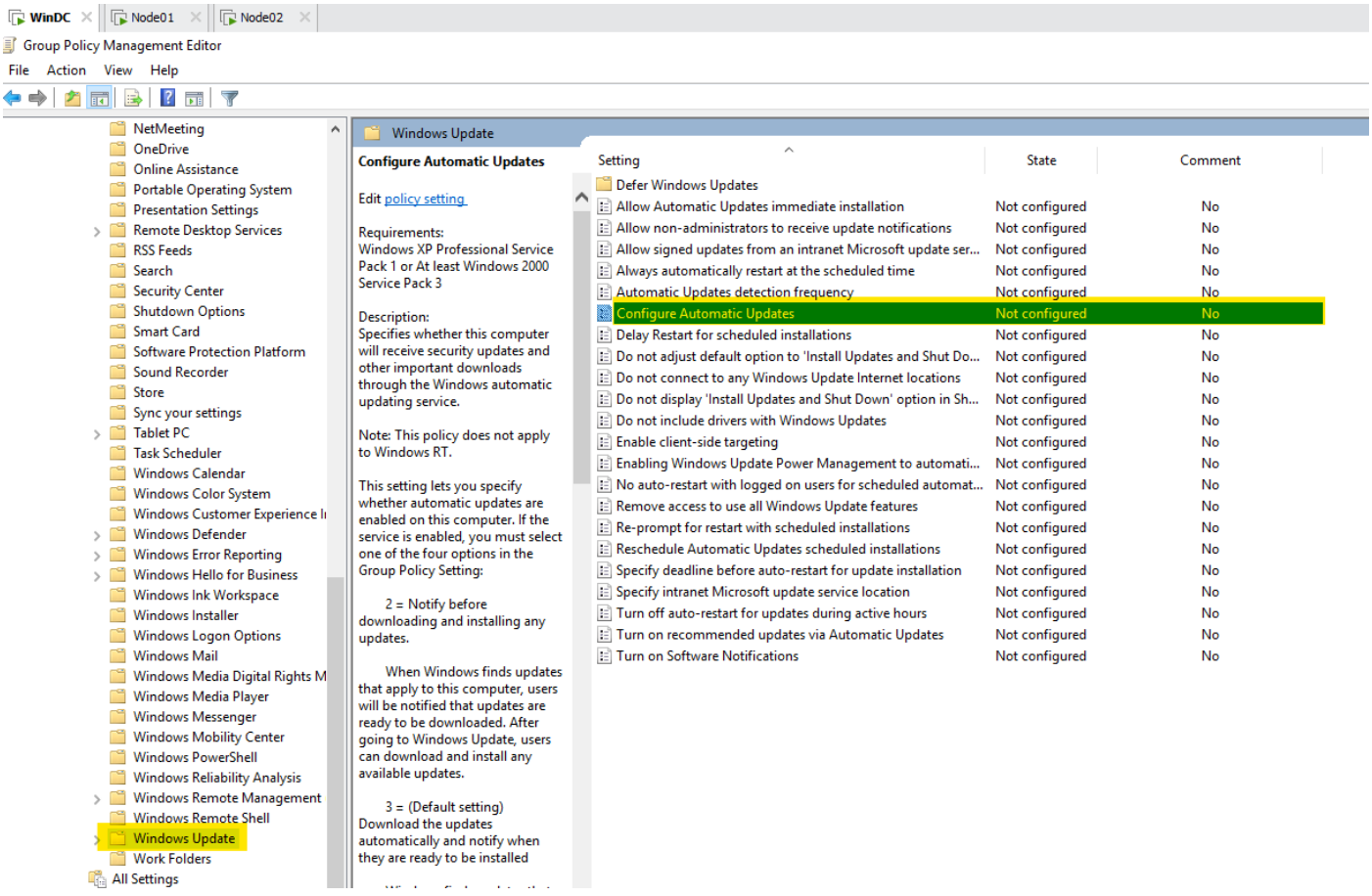
Give any name to it.



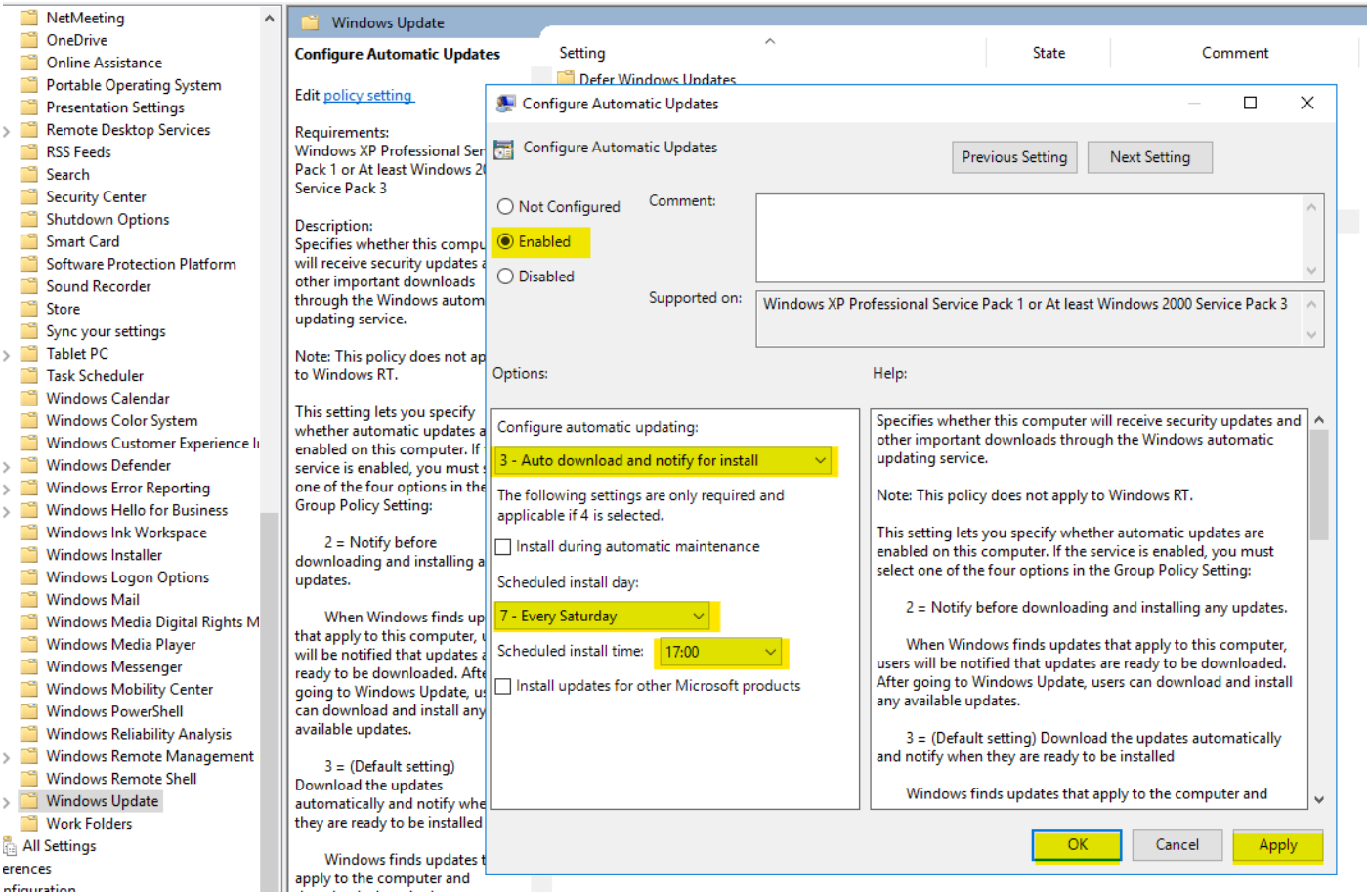
Right click and edit it:



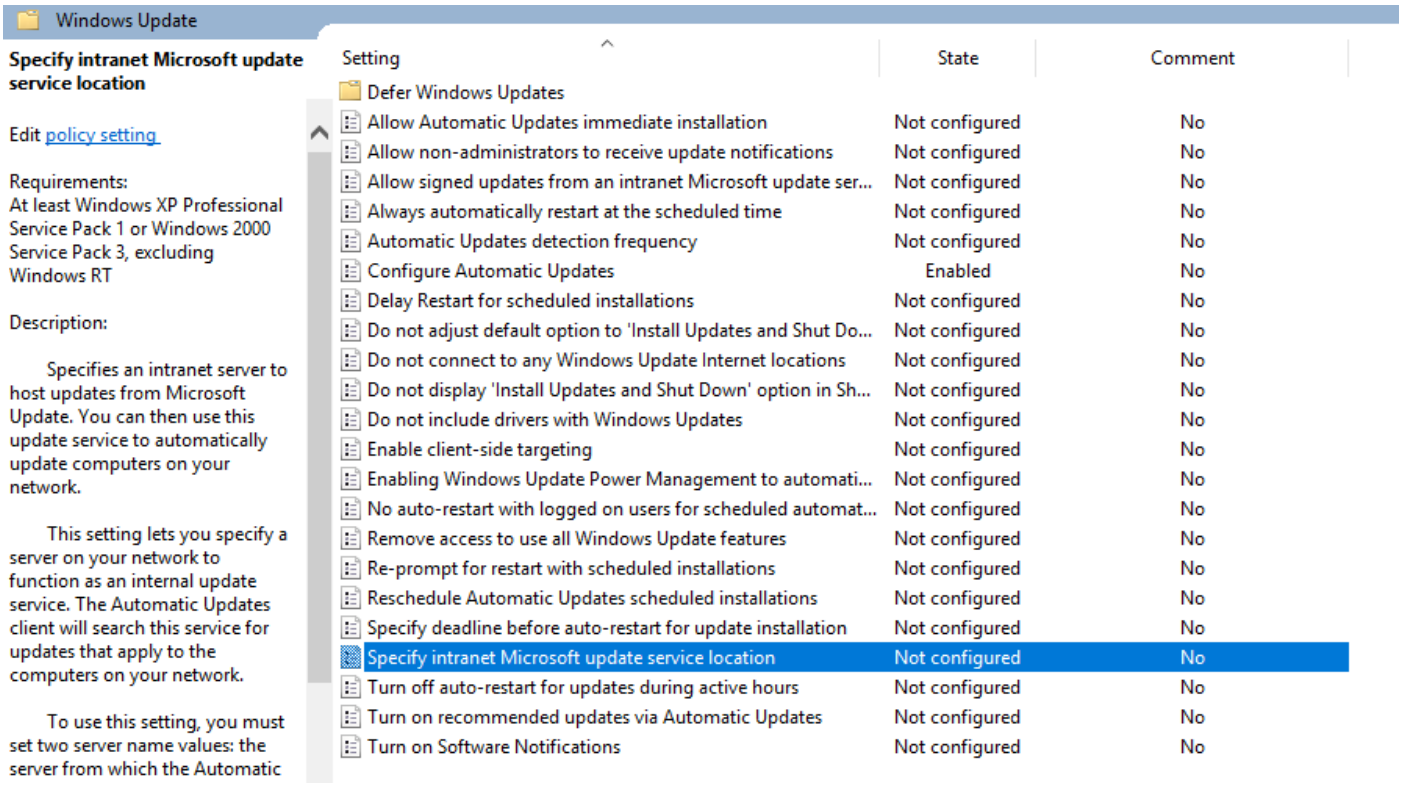
Go to: Computer configuration → Policies → Administrative Templates → Windows Components → Windows updates



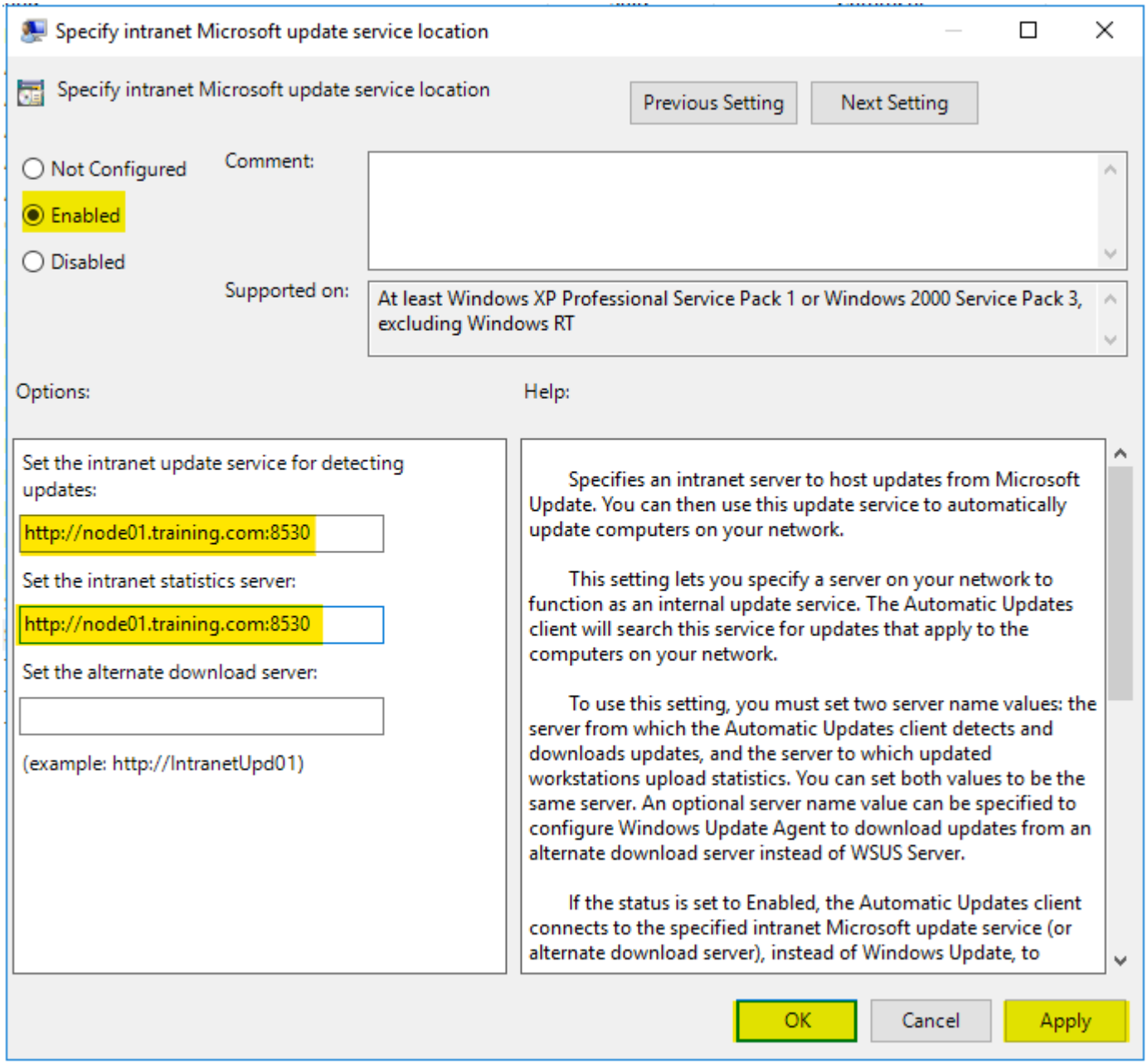
Double-click on the policy & fill details:



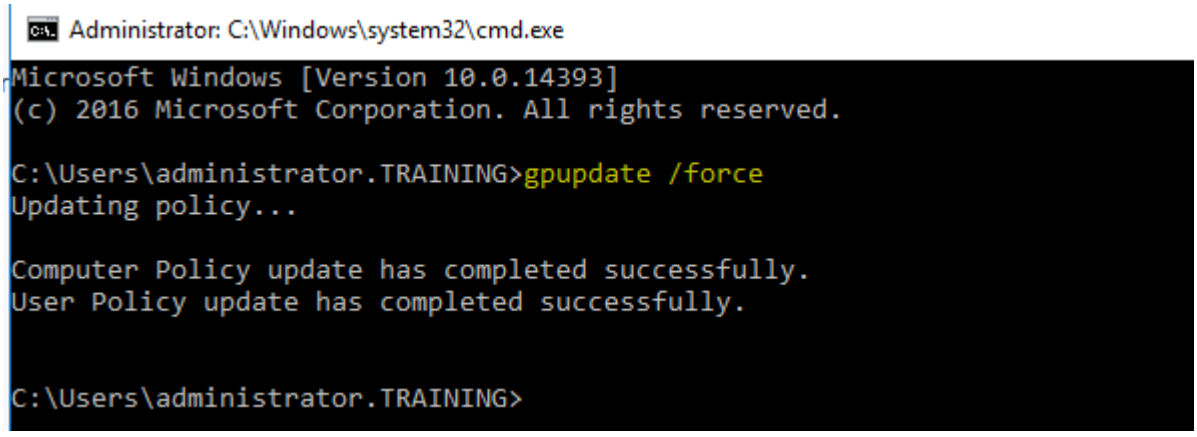
Next Specify Intranet Microsoft Update Service Location (within same GPO):



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



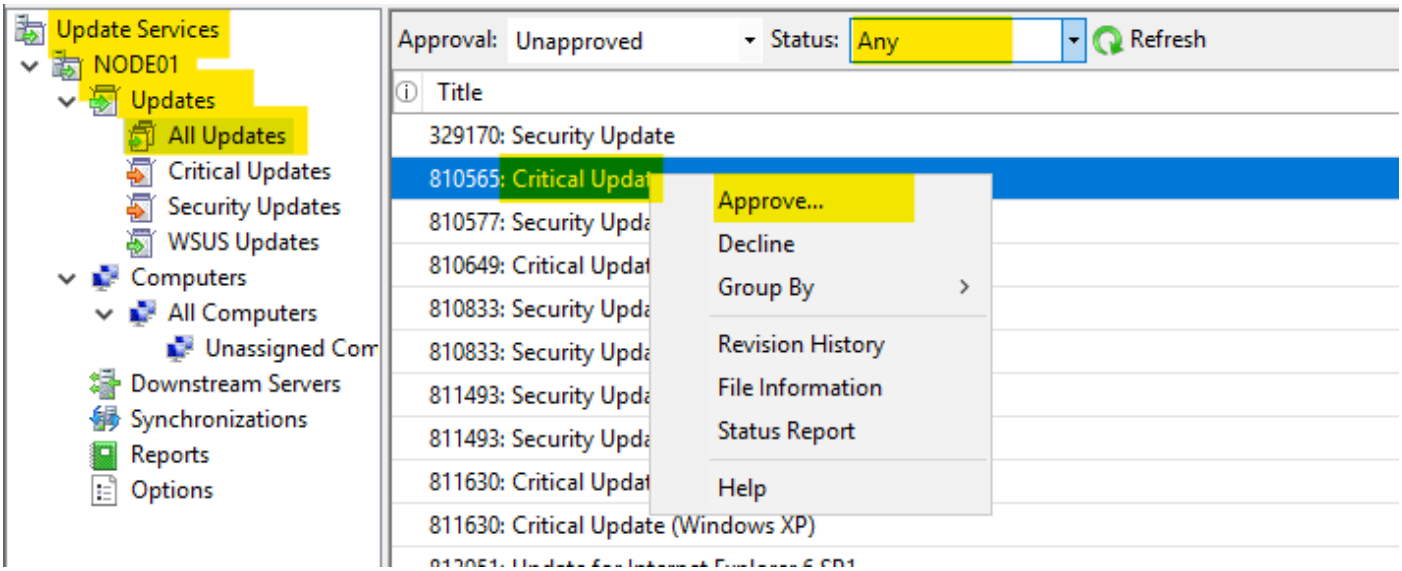
Now on clients, update the group policy:



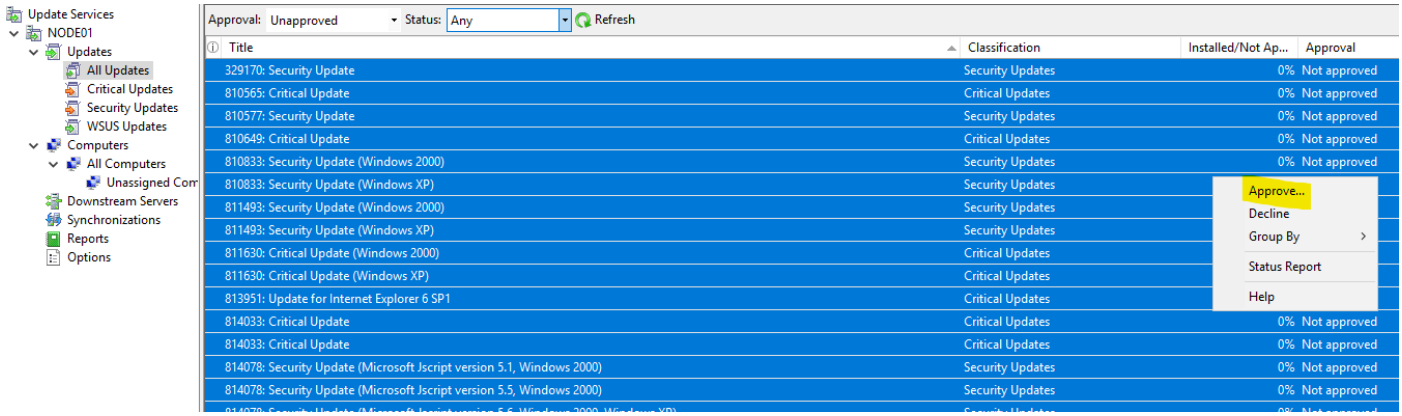
Listing the policy on client side (cmd: gpresult /r):

```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\administrator.TRAINING>gpresult /r

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

Created on 5/5/2025 at 4:57:06 AM


RSOP data for TRAINING\Administrator on NODE01 : Logging Mode
-------------------------------------------------------------

OS Configuration:            Member Server
OS Version:                  10.0.14393
Site Name:                   Default-First-Site-Name
Roaming Profile:             N/A
Local Profile:               C:\Users\administrator.TRAINING
Connected over a slow link?: No


COMPUTER SETTINGS
------------------
    CN=NODE01,CN=Computers,DC=training,DC=com
    Last time Group Policy was applied: 5/5/2025 at 4:55:52 AM
    Group Policy was applied from:      windc.training.com
    Group Policy slow link threshold:   500 kbps
    Domain Name:                        TRAINING
    Domain Type:                        Windows 2008 or later

    Applied Group Policy Objects
    ----------------------------
        Default Domain Policy
        WSUSUpdateGPO
```

To approve the updates:



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



########## That's all. ##########

Link: https://www.prajwaldesai.com/install-configure-wsus-on-windows-server-2019/

DNS

Configuring the DNS Server Role on Windows Server

Steps to Install and Configure DNS Server Role:

1. Open Server Manager → Click Add Roles and Features.
2. Choose:
    - Role-based or feature-based installation
    - Select your server
3. In Server Roles, check DNS Server
4. Click Next → Complete the wizard and install.
5. Once installed, open DNS Manager (dnsmgmt.msc) to configure zones.

Configuring DNS Zones

A DNS zone is a distinct part of the domain namespace that is delegated to a DNS server for management.

🔹 Types of Zones:

Zone Type	Description
Primary Zone	Read/write copy of the zone; maintained on the master DNS server.
Secondary Zone	Read-only copy from another DNS server (used for redundancy/load balancing).
Stub Zone	Contains only NS, SOA, and A records to locate authoritative DNS servers.
Forward Lookup Zone	Maps hostnames to IP addresses.
Reverse Lookup Zone	Maps IP addresses to hostnames.

Types of DNS Records:

Record Type	Description	Example
A (Address Record)	Maps a domain name to an IPv4 address.	`example.com → 192.168.1.1`
AAAA (IPv6 Address Record)	Maps a domain name to an IPv6 address.	`example.com → 2001:db8::1`
CNAME (Canonical Name Record)	Maps a domain alias to a real domain name.	`www.example.com → example.com`
MX (Mail Exchange Record)	Specifies mail servers for email delivery.	`mail.example.com → 192.168.2.2`
TXT (Text Record)	Stores arbitrary text, often used for security (SPF, DKIM).	SPF, DKIM, DMARC records
NS (Name Server Record)	Defines authoritative name servers for a domain.	`example.com → ns1.example.com`
PTR (Pointer Record)	Reverse DNS lookup (IP to domain).	`192.168.1.1 → example.com`
SRV (Service Record)	Specifies servers for services like SIP or LDAP.	`_sip._tcp.example.com`
SOA (Start of Authority)	Contains domain admin info and zone settings.	Includes serial number, refresh time, etc.

AD DS Replication

AD DS replication is the process through which domain controllers (DCs) synchronize Active Directory data (like users, groups, computers, GPOs, etc.) with each other to ensure consistency and availability across the domain or forest.

Key Concepts

- *Multimaster Replication*
    - Every domain controller can accept changes and replicate them to others.
    - There's no single master for most operations (except FSMO roles).
- *Replication Scopes*
    - Intra-site replication: Between DCs in the same site; fast and frequent.
    - Inter-site replication: Between DCs in different sites; uses compression, schedules, and site links to optimize WAN traffic.

What Gets Replicated?

- Users, groups, OUs
- Group Policies
- DNS data (if integrated with AD)
- Computer accounts
- Security permissions

How Replication Works

- Change Notification: When a change occurs on one DC, it notifies its replication partners.
- Replication Partners: Use connection objects to exchange changes.
- Update Sequence Number (USN) and High-Watermark Vector Table track which changes each DC has seen.
- Knowledge Consistency Checker (KCC): Automatically creates and adjusts replication topology.

Group Policy Object (GPO)