

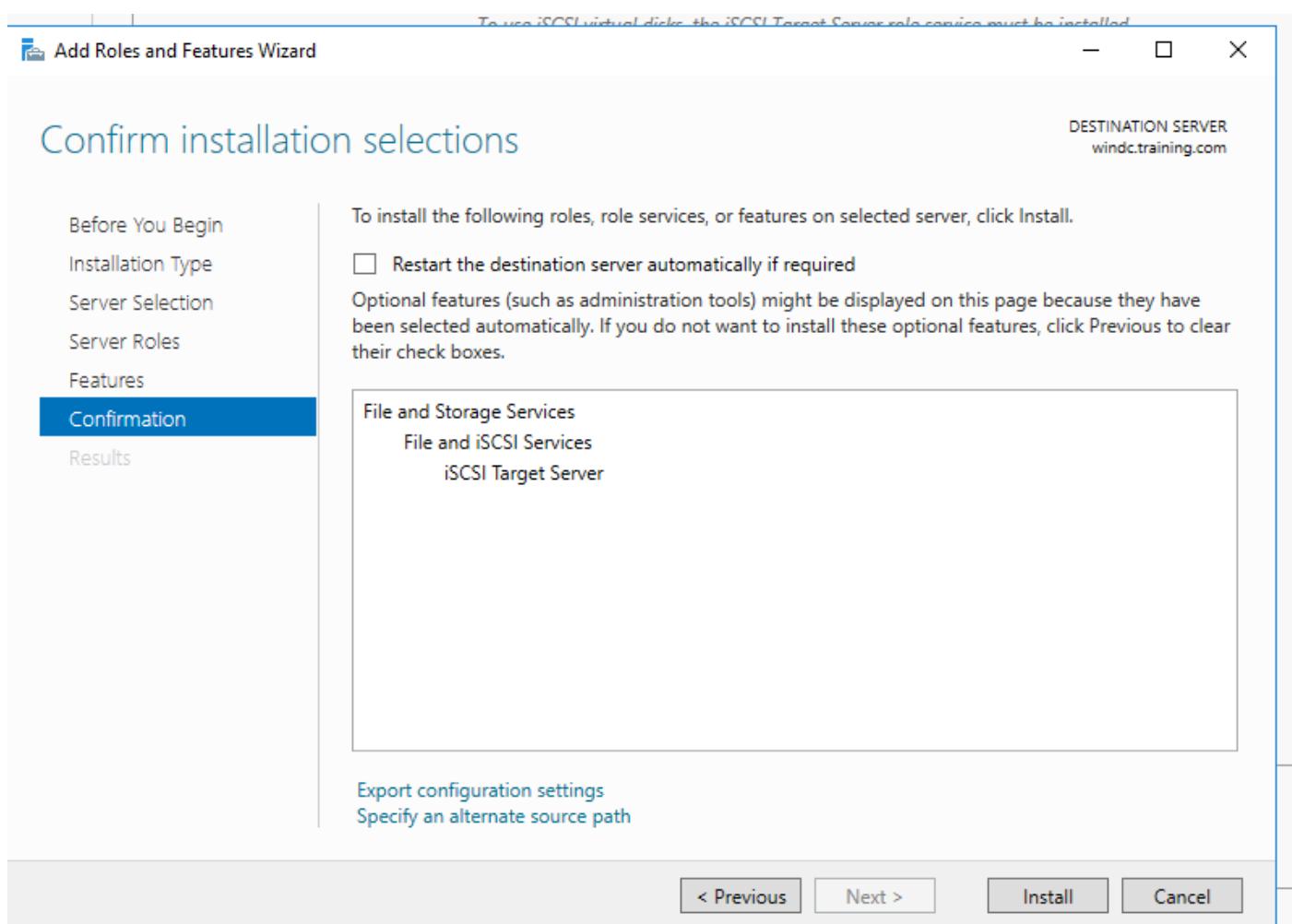
Installing iSCSI:

Installing iSCSI on DC

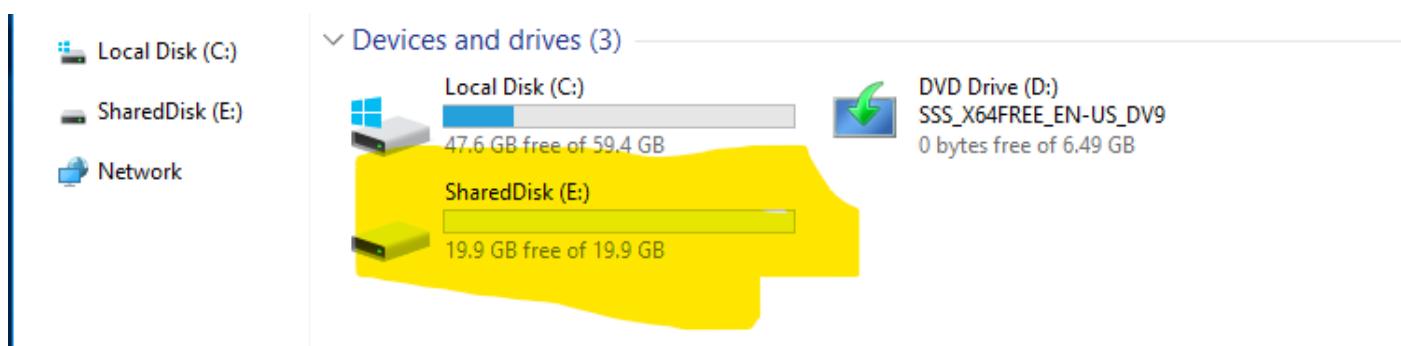
The screenshot shows the Windows Server Manager interface. In the left navigation pane, under 'File and Storage Services', the 'iSCSI' option is selected, highlighted with a yellow box. The main content area displays the 'iSCSI VIRTUAL DISKS' section, which states 'No data available.' Below this, a message reads: 'To use iSCSI virtual disks, the iSCSI Target Server role service must be installed.' A yellow box highlights the text 'To install iSCSI Target Server, start the Add Roles and Features Wizard.' At the top right, there are 'Manage', 'Tools', 'View', and 'Help' buttons.

The screenshot shows the 'Add Roles and Features Wizard' window. The title bar says 'Add Roles and Features Wizard'. On the left, a navigation pane lists steps: 'Before You Begin', 'Installation Type', 'Server Selection', 'Server Roles' (which is selected and highlighted with a blue box), 'Features', 'Confirmation', and 'Results'. The main content area is titled 'Select one or more roles to install on the selected server.' It shows a 'Roles' list with several options. Under 'File and Storage Services', the 'iSCSI Target Server' checkbox is checked and highlighted with a yellow box. Other checked items include 'File Server (Installed)' and 'Storage Services (Installed)'. Buttons at the bottom include '< Previous', 'Next >', 'Install', and 'Cancel'.

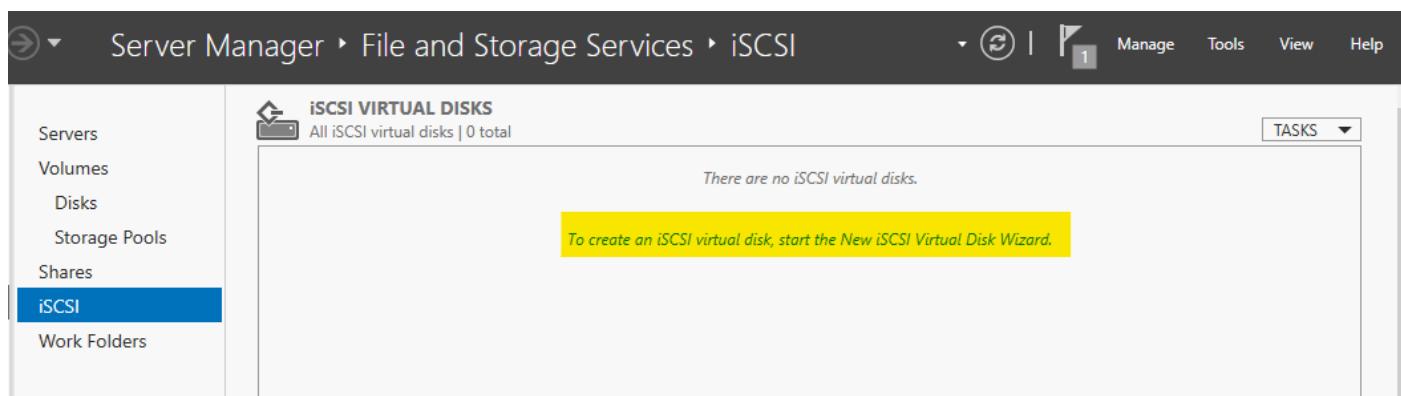
Install:



Adding a new 20GB disk:



Creating iSCSI virtual disk:



Selecting the disk:

New iSCSI Virtual Disk Wizard

Select iSCSI virtual disk location

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

Server:

Server Name	Status	Cluster Role	Owner Node
windc	Online	Not Clustered	

Tip: The list is filtered to show only servers with the iSCSI Target Server role installed.

Storage location:

Select by volume:

Volume	Free Space	Capacity	File System
C:	47.7 GB	59.5 GB	NTFS
E:	19.9 GB	20.0 GB	NTFS

The iSCSI virtual disk will be saved at \iSCSIVirtualDisk on the selected volume.

Type a custom path:

Creating a name for the volume:

Specify iSCSI virtual disk name

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

Name:

Description:

Path:

Specifying the disk type:

Specify iSCSI virtual disk size

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

Free space: 19.9 GB
Size: GB

Fixed size
This type of disk provides better performance and is recommended for servers running applications with a high level of disk activity. The virtual hard disk is created using the size of the fixed virtual hard disk. It does not change when data is added or deleted.
 Clear the virtual disk on allocation
Note: Un-selecting is NOT RECOMMENDED. Clearing a disk to zero will remove any fragments of data that remained on underlying storage, thus protecting from information leaks.

Dynamically expanding
This type of disk provides better use of physical storage space and is recommended for servers running applications that are not disk intensive. The .vhdx file is small when the disk is created and grows as data is written to it.

Differencing
This type of disk is associated in a parent-child relationship with another disk that you want to leave intact. You can make changes to this virtual hard disk without affecting the parent disk and easily revert the changes later.

Parent virtual disk path:

Assigning a new iSCSI target:

Assign iSCSI target

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

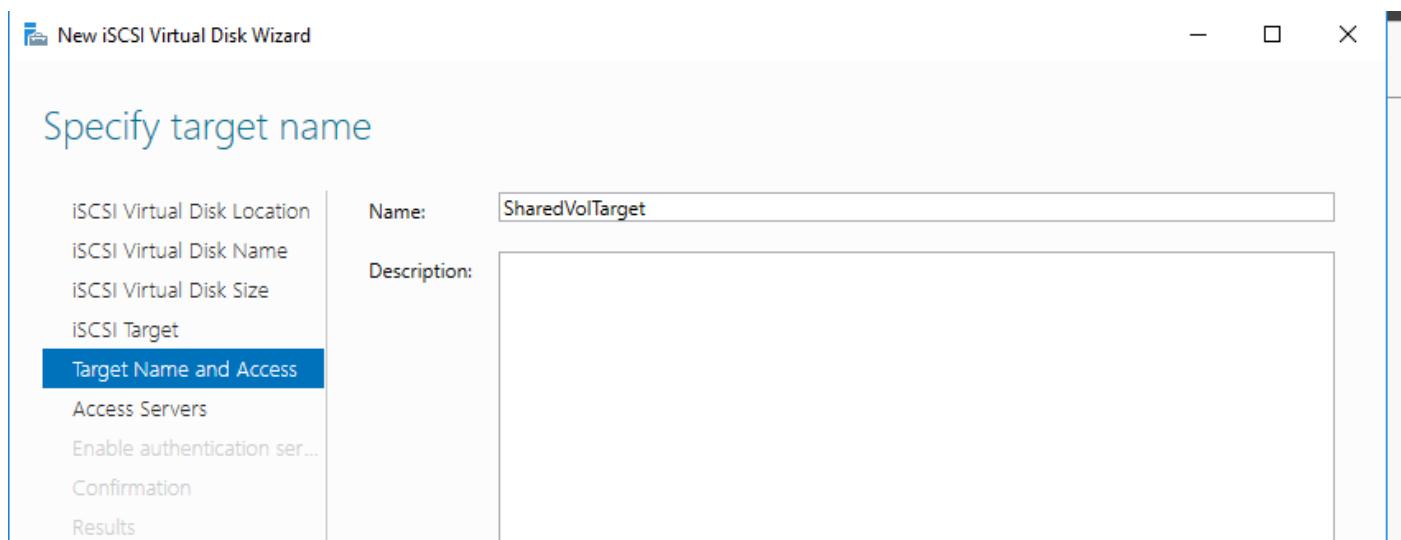
Assign this iSCSI virtual disk to an existing iSCSI target or create a new target for it.

Existing iSCSI target:

Target Name	Initiator IDs	Description

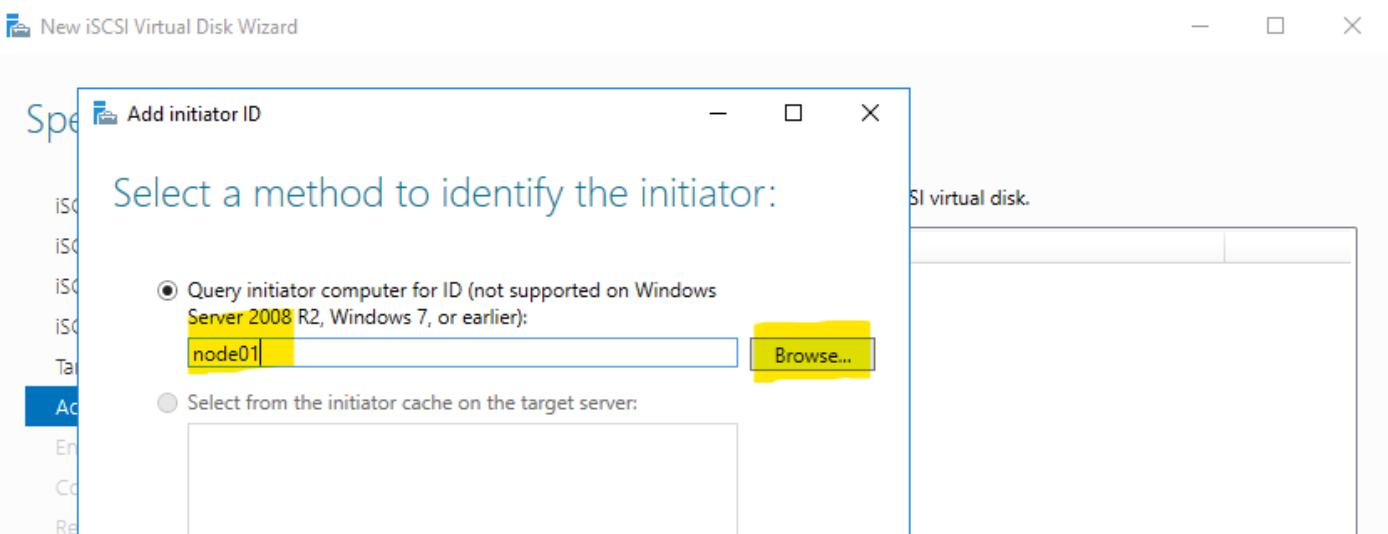
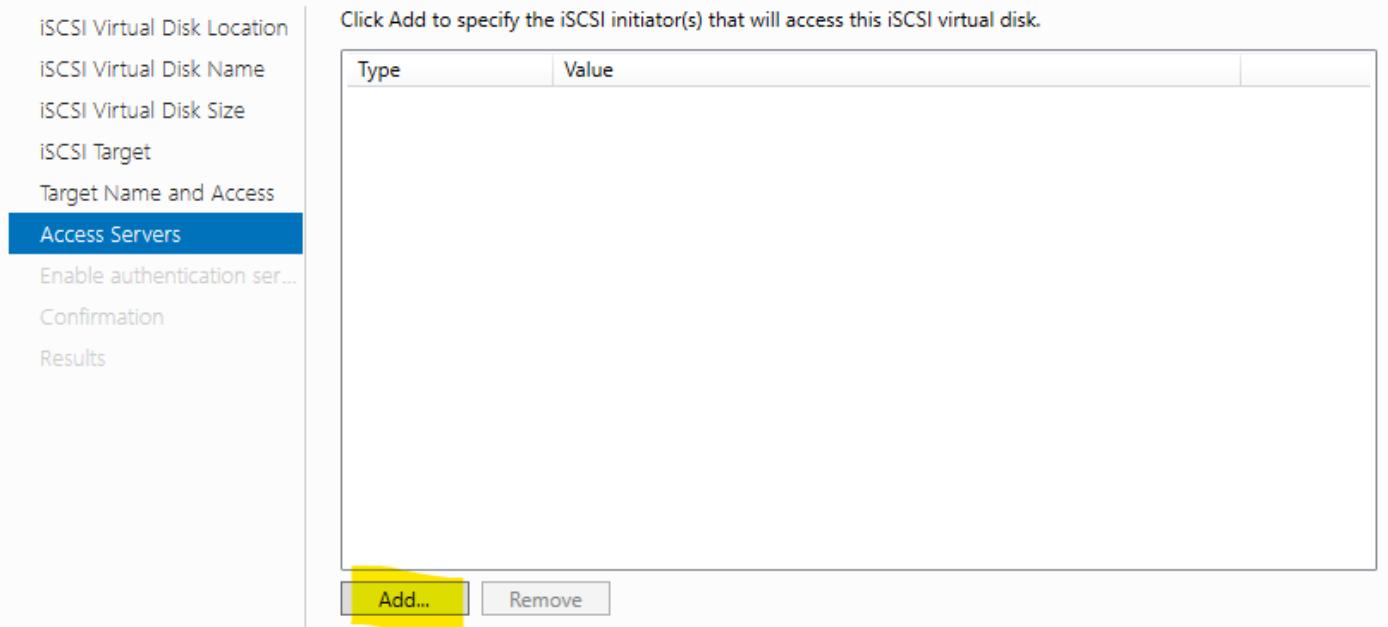
New iSCSI target

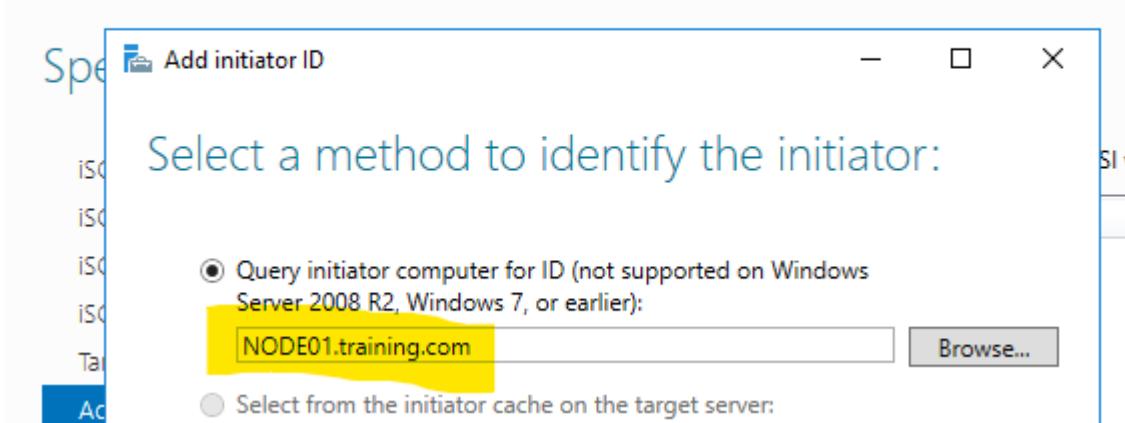
Adding target name:



Adding access server:

Specify access servers





Adding both nodes:

Specify access servers

- 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

Click Add to specify the iSCSI initiator(s) that will access this iSCSI virtual disk.

Type	Value
IQN	iqn.1991-05.com.microsoft:node01.training.com
IQN	iqn.1991-05.com.microsoft:node02.training.com

Leave CHAP:

Enable Authentication

- 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

Optionally, enable the CHAP protocol to authenticate initiator connections, or enable reverse CHAP to allow the initiator to authenticate the iSCSI target.

Enable CHAP:

User name:

Password:

Confirm password:

Enable reverse CHAP:

User name:

Password:

Confirm password:

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

S

V

View results

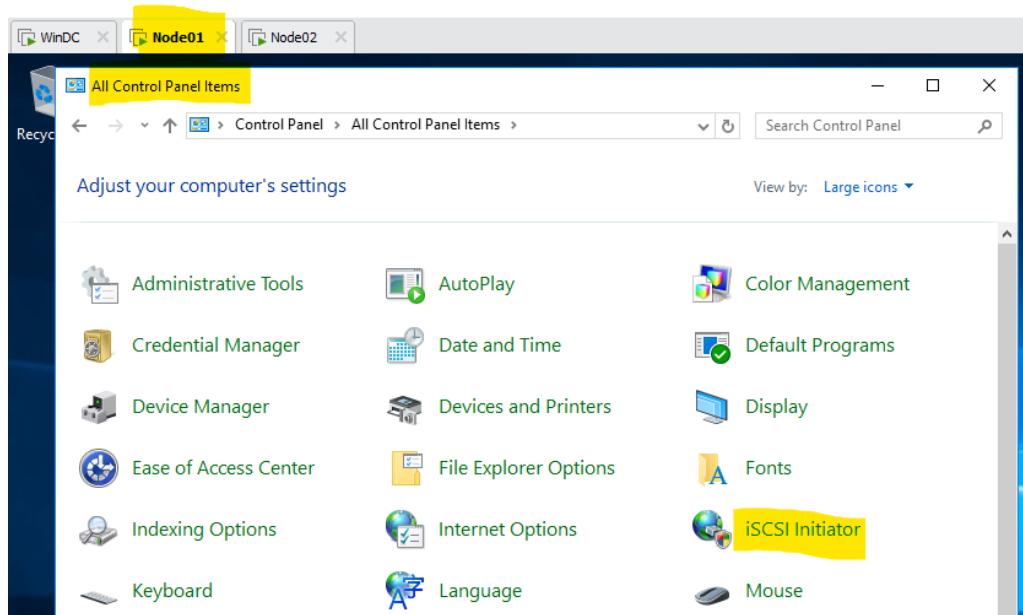
ISCSI Virtual Disk Location
ISCSI Virtual Disk Name
ISCSI Virtual Disk Size
ISCSI Target
Target Name and Access
Access Servers
Enable authentication ser...
Confirmation

Results

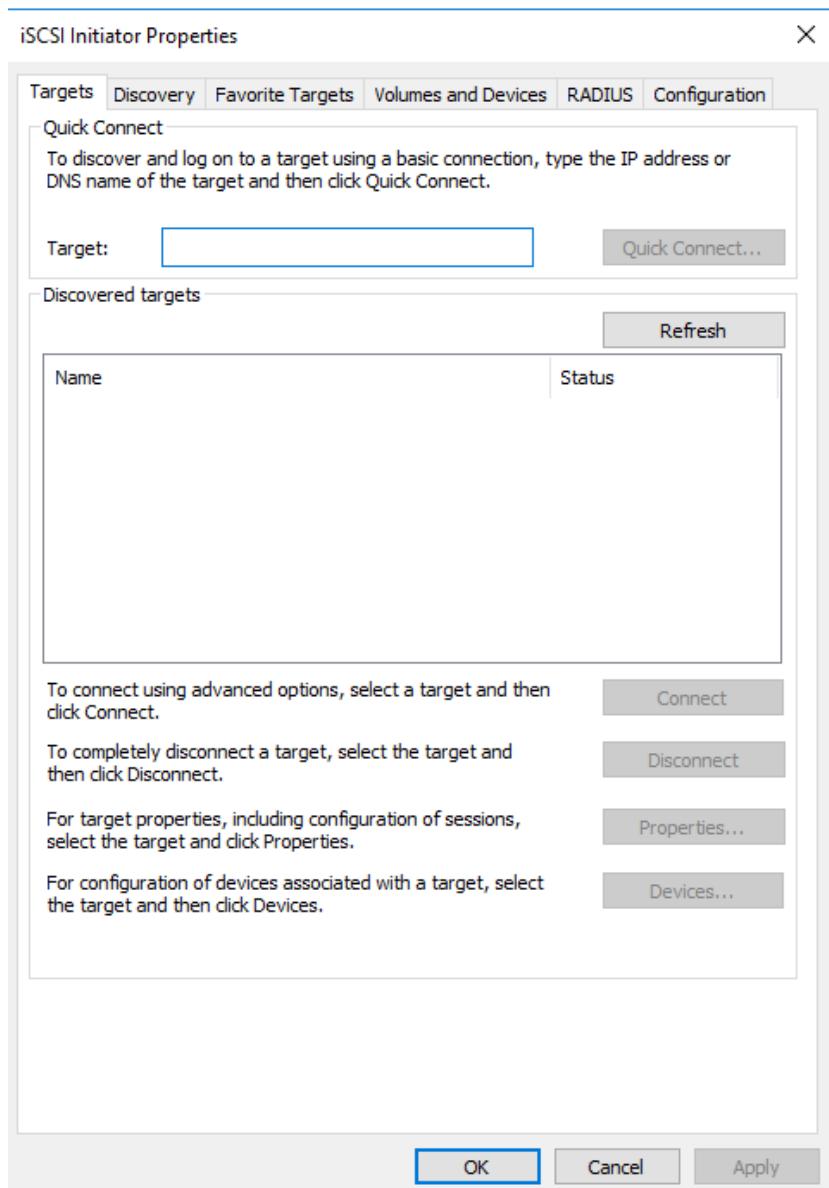
ISCSI virtual disk was created successfully.

Task	Progress	Status
Create iSCSI virtual disk	<div style="width: 100%; background-color: #0070C0;"></div>	Completed
Create iSCSI target	<div style="width: 100%; background-color: #0070C0;"></div>	Completed
Set target access	<div style="width: 100%; background-color: #0070C0;"></div>	Completed
Assign iSCSI virtual disk to target	<div style="width: 100%; background-color: #0070C0;"></div>	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:

Targets Discovery Favorite Targets Volumes and Devices RADIUS Configuration

- Quick Connect
To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect.

Target: windc Quick Connect...

- Discovered targets

Switch volume & device tab & clock auto-configure:

iSCSI Initiator Properties ×

Targets Discovery Favorite Targets **Volumes and Devices** RADIUS Configuration

If a program or service uses a particular volume or device, add that volume or device to the list below, or click Auto Configure to have the iSCSI initiator service automatically configure all available devices.

This will bind the volume or device so that on system restart it is more readily available for use by the program or service. This is only effective if the associated target is on the Favorite Targets List.

Volume List:

Volume/mount point/device
\\?\scsi#disk&ven_msft&prod_virtual_hd#1&1c121344&0&000000#{53f56307-b6bf...

To automatically configure all available devices, click Auto Configure.

Auto Configure

Open “disk management portal” and create disk:

WinDC **Node01** Node02

Disk Management

File Action View Help

Re

Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free
	Simple	Basic		Healthy (R...)	450 MB	450 MB	100 %
	Simple	Basic		Healthy (E...)	99 MB	99 MB	100 %
(C):	Simple	Basic	NTFS	Healthy (B...)	59.45 GB	48.84 GB	82 %
SSS_X64FREE_EN-...	Simple	Basic	UDF	Healthy (P...)	6.49 GB	0 MB	0 %

Disk 0
Basic
59.98 GB
Online

450 MB
Healthy (Recovery Partition)

99 MB
Healthy (EFI System Pa

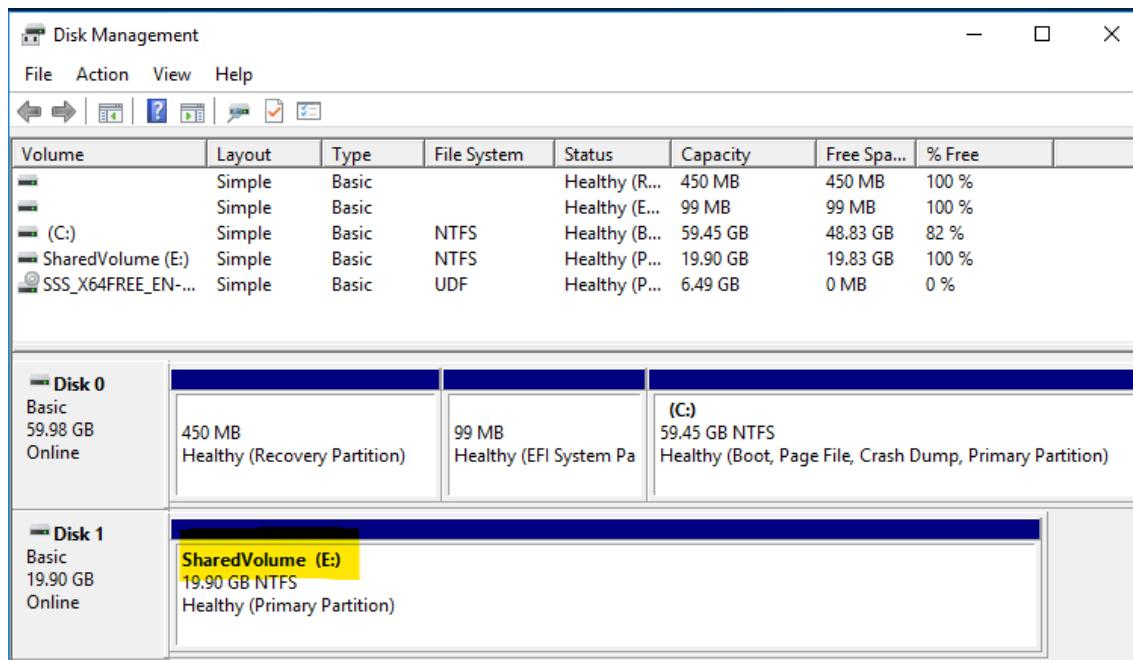
(C)
59.45 GB NTFS
Healthy (Boot, Page File, Crash Dump, Primary Partition)

Disk 1
Unknown
19.90 GB
Offline

19.90 GB
Unallocated

■ Unallocated ■ Primary partition

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 iSCSI, 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.

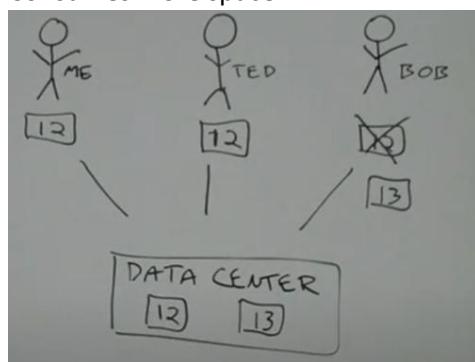
Real-World Analogy:

- **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.

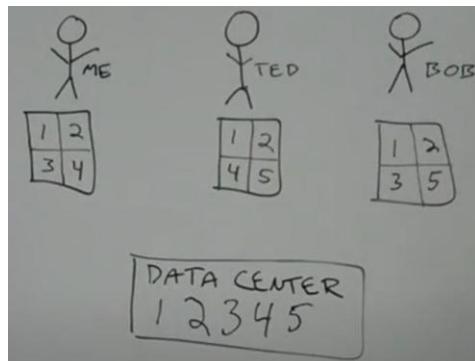
Data Deduplication in Windows Server 2016

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.



- 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:

The screenshot shows the 'Select destination server' step of the 'Add Roles and Features Wizard'. The 'Server Selection' tab is selected. On the right, a table lists a single server: node01.training.com (IP 192.168.10.11) running Microsoft Windows Server 2016 Datacenter Evaluation.

Name	IP Address	Operating System
node01.training.com	192.168.10.11	Microsoft Windows Server 2016 Datacenter Evaluation

Installing feature:

The screenshot shows the 'Select features' step of the 'Add Roles and Features Wizard'. The 'Features' tab is selected. In the 'Features' list, 'Failover Clustering' is checked and highlighted with a yellow box. The 'Description' column provides information about Failover Clustering.

Features	Description
<input type="checkbox"/> .NET Framework 3.5 Features	Failover Clustering allows multiple servers to work together to provide high availability of server roles. Failover Clustering is often used for File Services, virtual machines, database applications, and mail applications.
<input checked="" type="checkbox"/> .NET Framework 4.6 Features (2 of 7 installed)	
<input type="checkbox"/> Background Intelligent Transfer Service (BITS)	
<input type="checkbox"/> BitLocker Drive Encryption	
<input type="checkbox"/> BitLocker Network Unlock	
<input type="checkbox"/> BranchCache	
<input type="checkbox"/> Client for NFS	
<input type="checkbox"/> Containers	
<input type="checkbox"/> Data Center Bridging	
<input type="checkbox"/> Direct Play	
<input type="checkbox"/> Enhanced Storage	
<input checked="" type="checkbox"/> Failover Clustering	
<input type="checkbox"/> Group Policy Management	
<input type="checkbox"/> Host Guardian Hyper-V Support	
<input type="checkbox"/> I/O Quality of Service	
<input type="checkbox"/> IIS Hostable Web Core	
<input type="checkbox"/> Internet Printing Client	
<input type="checkbox"/> IP Address Management (IPAM) Server	
<input type="checkbox"/> iSNS Server service	

[< Previous](#) [Next >](#) [Install](#) [Cancel](#)

Confirm installation selections

DESTINATION SERVER
node01.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.

Failover Clustering

Remote Server Administration Tools

 Feature Administration Tools

 Failover Clustering Tools

 Failover Cluster Management Tools

 Failover Cluster Module for Windows PowerShell

Performing the same on Node02:

Select a server or a virtual hard disk on which to install roles and features.

- Select a server from the server pool
 Select a virtual hard disk

Server Pool

Filter:

Name	IP Address	Operating System
------	------------	------------------

node02.training.com	192.168.10.12	Microsoft Windows Server 2016 Datacenter Evaluation
---------------------	---------------	---

Select features

DESTINATION SERVER
node02.training.com

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select one or more features to install on the selected server.

Features

- ▷ .NET Framework 3.5 Features
- ▷ .NET Framework 4.6 Features (2 of 7 installed)
- ▷ Background Intelligent Transfer Service (BITS)
 - ▷ BitLocker Drive Encryption
 - ▷ BitLocker Network Unlock
 - ▷ BranchCache
 - ▷ Client for NFS
 - ▷ Containers
 - ▷ Data Center Bridging
 - ▷ Direct Play
 - ▷ Enhanced Storage
- ▷ Failover Clustering

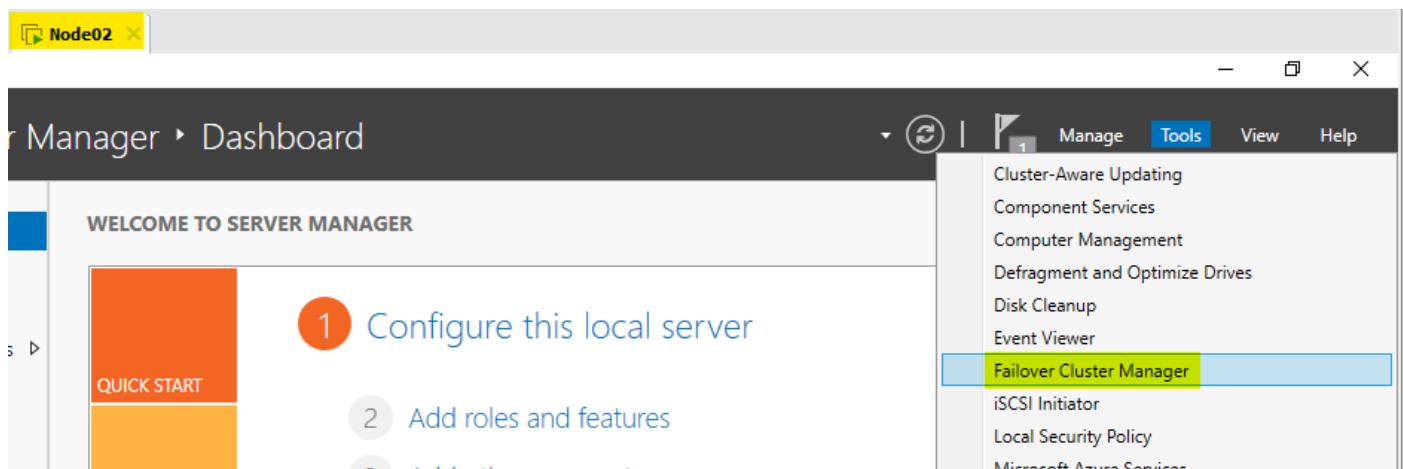
Description

Failover Clustering allows multiple servers to work together to provide high availability of server roles.

Failover Clustering is often used for File Services, virtual machines, database applications, and mail applications.

Testing the failover clustering:

Switch to dashboard page → tools



Validating configuration:

The screenshot shows the Failover Cluster Manager interface. The left pane has sections for 'Overview' and 'Clusters'. The 'Clusters' section displays a table with columns: Name, Role Status, Node Status, and Event. A message at the bottom says 'No items found.' The right pane contains an 'Actions' list with options: Validate Configuration... (highlighted in yellow), Create Cluster..., Connect to Cluster..., View, Refresh, Properties, and Help.

Click on Next on “before you begin”:

The screenshot shows the 'Validate a Configuration Wizard' window. The title bar says 'Validate a Configuration Wizard'. The main area is titled 'Before You Begin'. On the left, a sidebar lists: 'Before You Begin' (selected), 'Select Servers or a Cluster', 'Testing Options', 'Confirmation', 'Validating', and 'Summary'. The main content area contains the following text:
This wizard runs validation tests to determine whether this configuration of servers and attached storage is set up correctly to support failover. A cluster solution is supported by Microsoft only if the complete configuration (servers, network, and storage) passes all tests in this wizard. In addition, all hardware components in the cluster solution must be "Certified for Windows Server 2016."
If you want to validate a set of unclustered servers, you need to know the names of the servers.
Important: the storage connected to the selected servers will be unavailable during validation tests.
If you want to validate an existing failover cluster, you need to know the name of the cluster or one of its nodes.
You must be a local administrator on each of the servers that you want to validate.
To continue, click Next.

[More about cluster validation tests](#)
 Do not show this page again

At the bottom right are 'Next >' and 'Cancel' buttons.

Select servers or a cluster: (browse)

The screenshot shows a search interface for selecting servers or clusters. A search bar at the top contains the text "node". Below it is a "Check Names" button and a "Browse..." button. To the right are "Add" and "Remove" buttons. A modal window titled "Multiple Names Found" is displayed, stating "More than one object matched the name 'node'. Select one or more names from this list, or reenter the name." It lists two matching names: "NODE01" and "NODE02", each with its description and folder path.

The screenshot shows the "Select Servers or a Cluster" dialog. On the left, a sidebar lists steps: "Before You Begin", "Select Servers or a Cluster" (which is selected), "Testing Options", "Confirmation", "Validating", and "Summary". The main area has sections for "Enter name:" (containing "wipro-cluster-01") and "Selected servers:" (containing "node01.training.com" and "node02.training.com"). To the right are "Browse...", "Add", and "Remove" buttons.

Testing option → Running all tests

The screenshot shows the "Testing Options" dialog. The sidebar includes "Before You Begin", "Select Servers or a Cluster", "Testing Options" (selected), "Confirmation", "Validating", and "Summary". The main content area describes the testing process, mentions cluster configuration, and provides two options for running tests: "Run all tests (recommended)" (selected) and "Run only tests I select". At the bottom is a link "More about cluster validation tests" and navigation buttons: "< Previous", "Next >", and "Cancel".

Validate:

Validate a Configuration Wizard

Confirmation

Before You Begin
Select Servers or a Cluster
Testing Options
Confirmation
Validating
Summary

You are ready to start validation.
Please confirm that the following settings are correct:

Servers to Test	Category
node01.training.com	Inventory
node02.training.com	Inventory
Tests Selected by the User	Category
List Fibre Channel Host Bus Adapters	Inventory
List iSCSI Host Bus Adapters	Inventory
List SAS Host Bus Adapters	Inventory
List BIOS Information	Inventory

To continue, click Next.

< Previous **Next >** Cancel

Wait...

Validate a Configuration Wizard

Validating

Before You Begin
Select Servers or a Cluster
Testing Options
Validating
Confirmation
Summary

The following validation tests are running. Depending on the test selection, this may take a significant amount of time.

Progress	Test	Result
100%	Validate Disk Arbitration	The test passed.
100%	Validate Disk Failover	The test passed.
100%	Validate File System	The test passed.
100%	Validate Microsoft MPIO-based disks	The test passed.
100%	Validate Multiple Arbitration	The test passed.
100%	Validate SCSI device Vital Product Data (VPD)	The test passed.
100%	Validate SCSI-3 Persistent Reservation	The test passed.
0%	Validate Simultaneous Failover	Taking Test Disk 0 off

Test is currently running.

Cancel



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	Result
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
List Fibre Channel Host Bus Adapters	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:



Failover Cluster Validation Report

Node: node01.training.com **Result:** Validated
Node: node02.training.com **Result:** 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>.

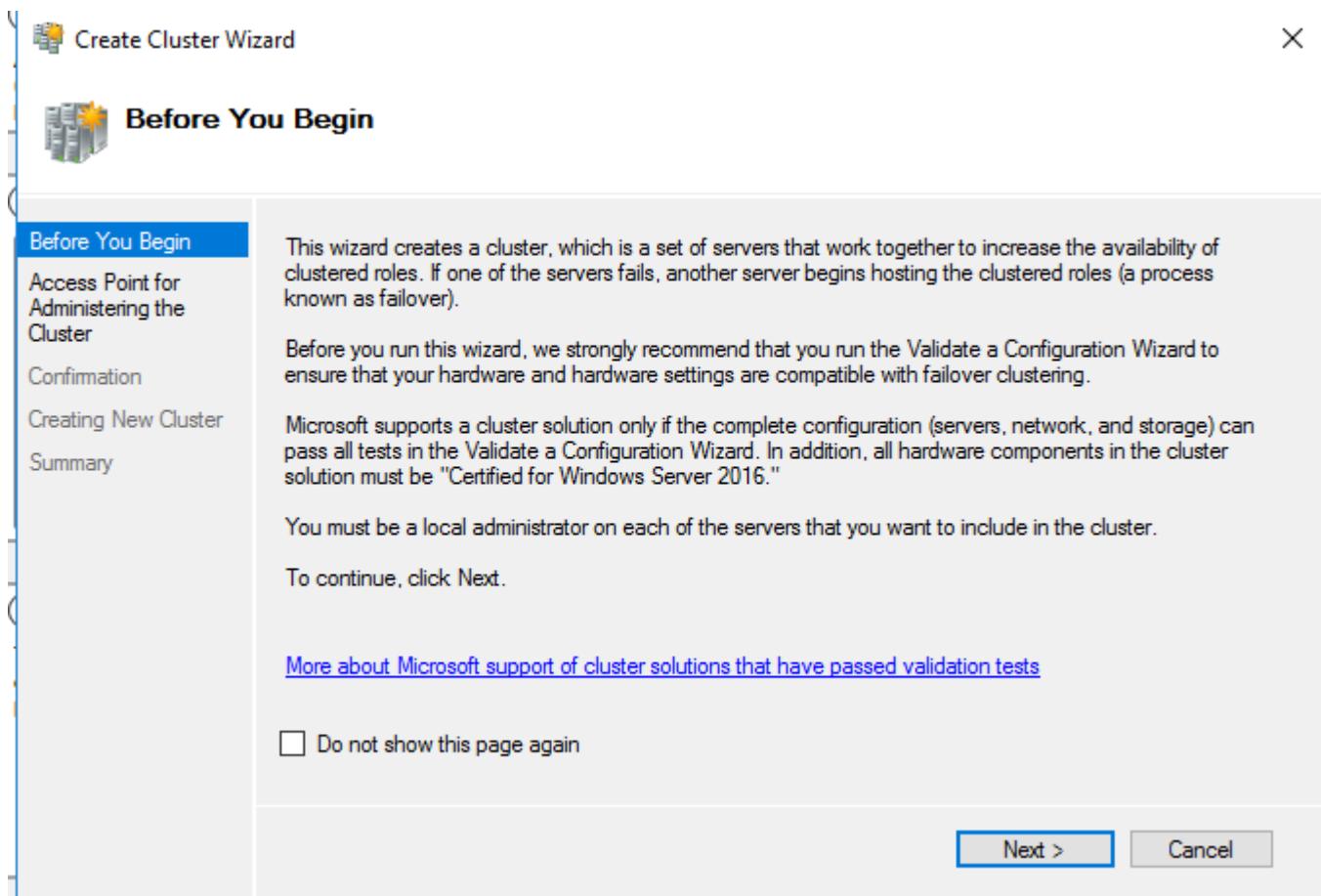
Results by Category

Name	Result Summary	Description
Inventory		Success
Network		Warning
Storage		Success
System Configuration		Success

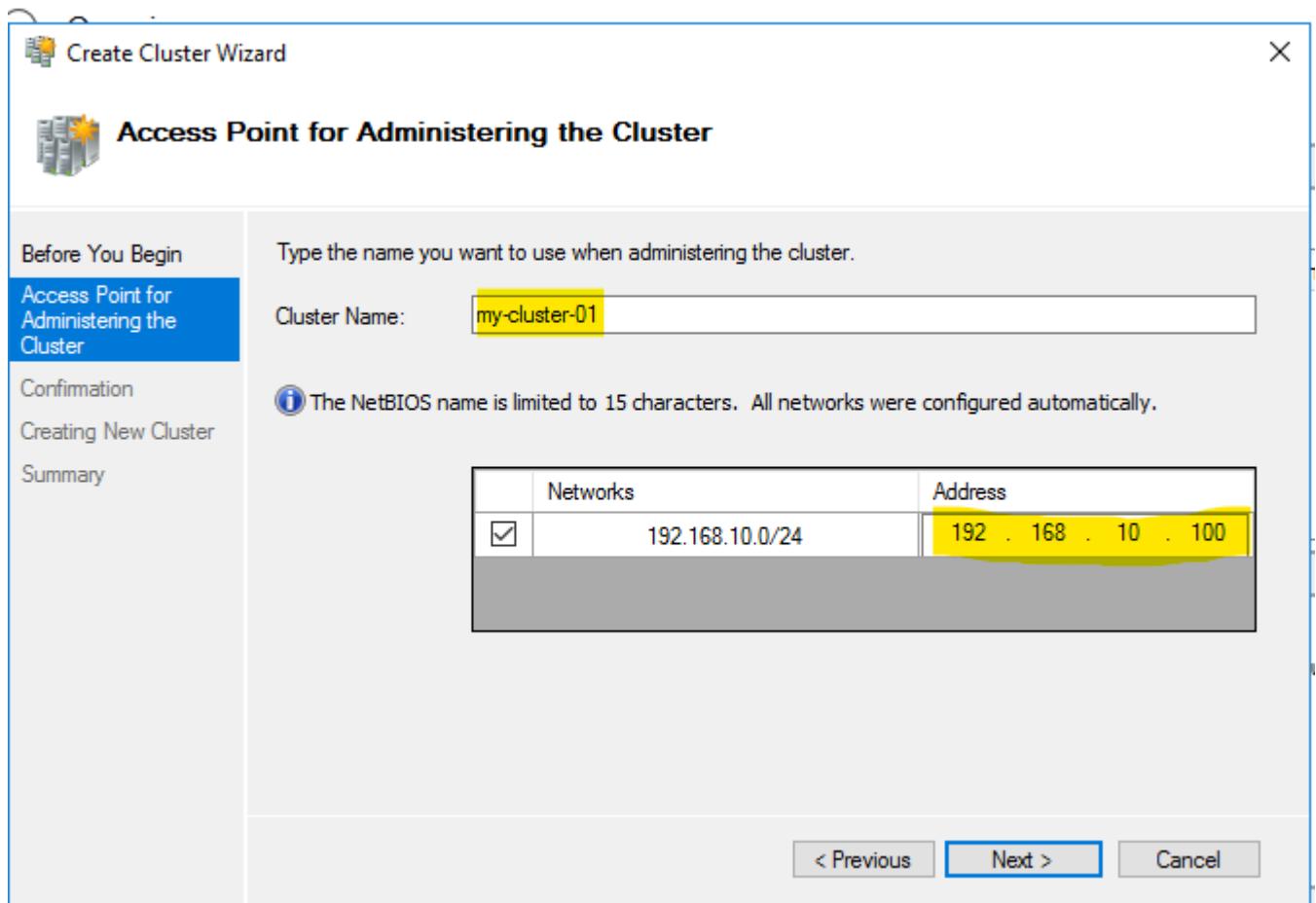
Inventory

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

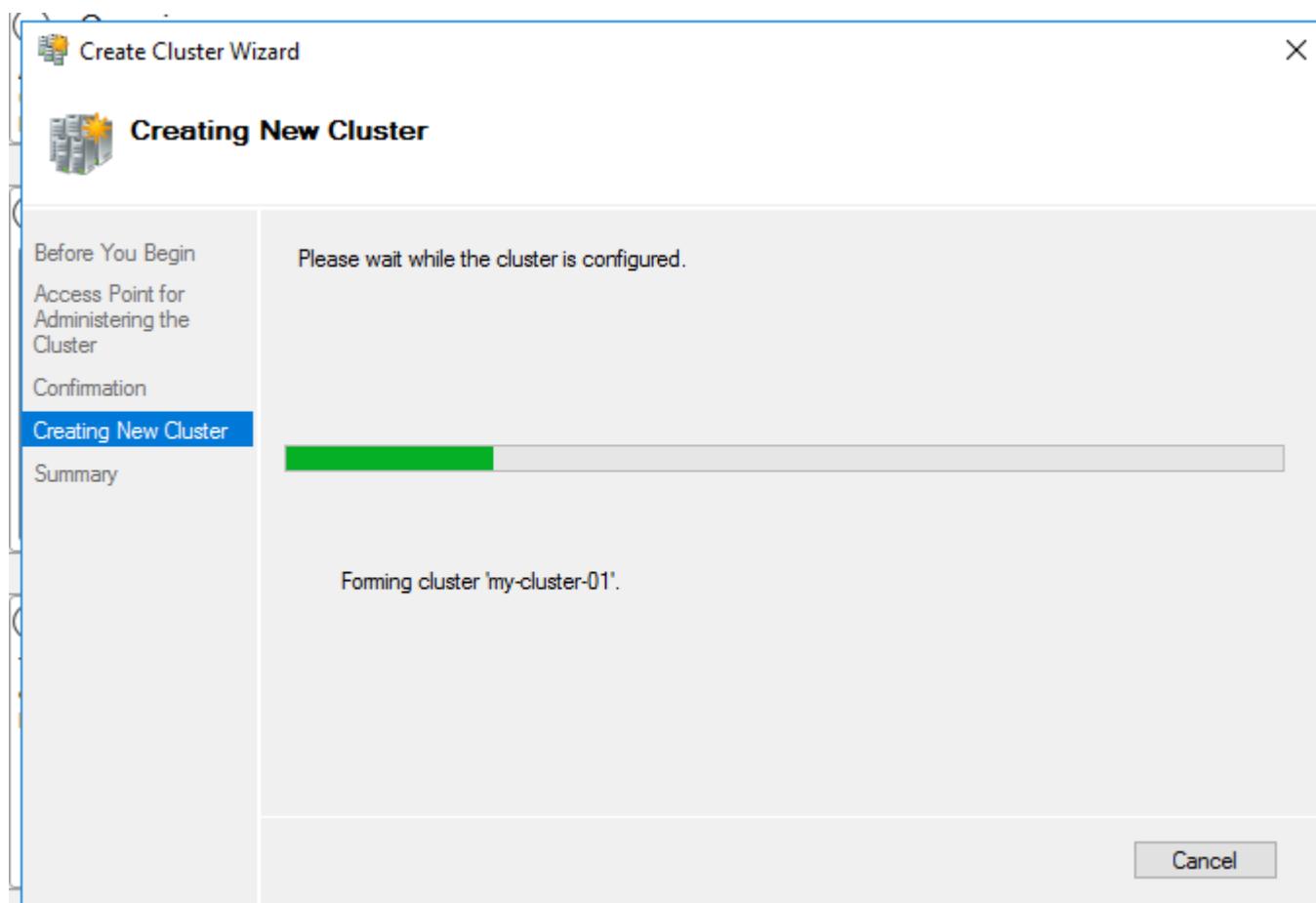
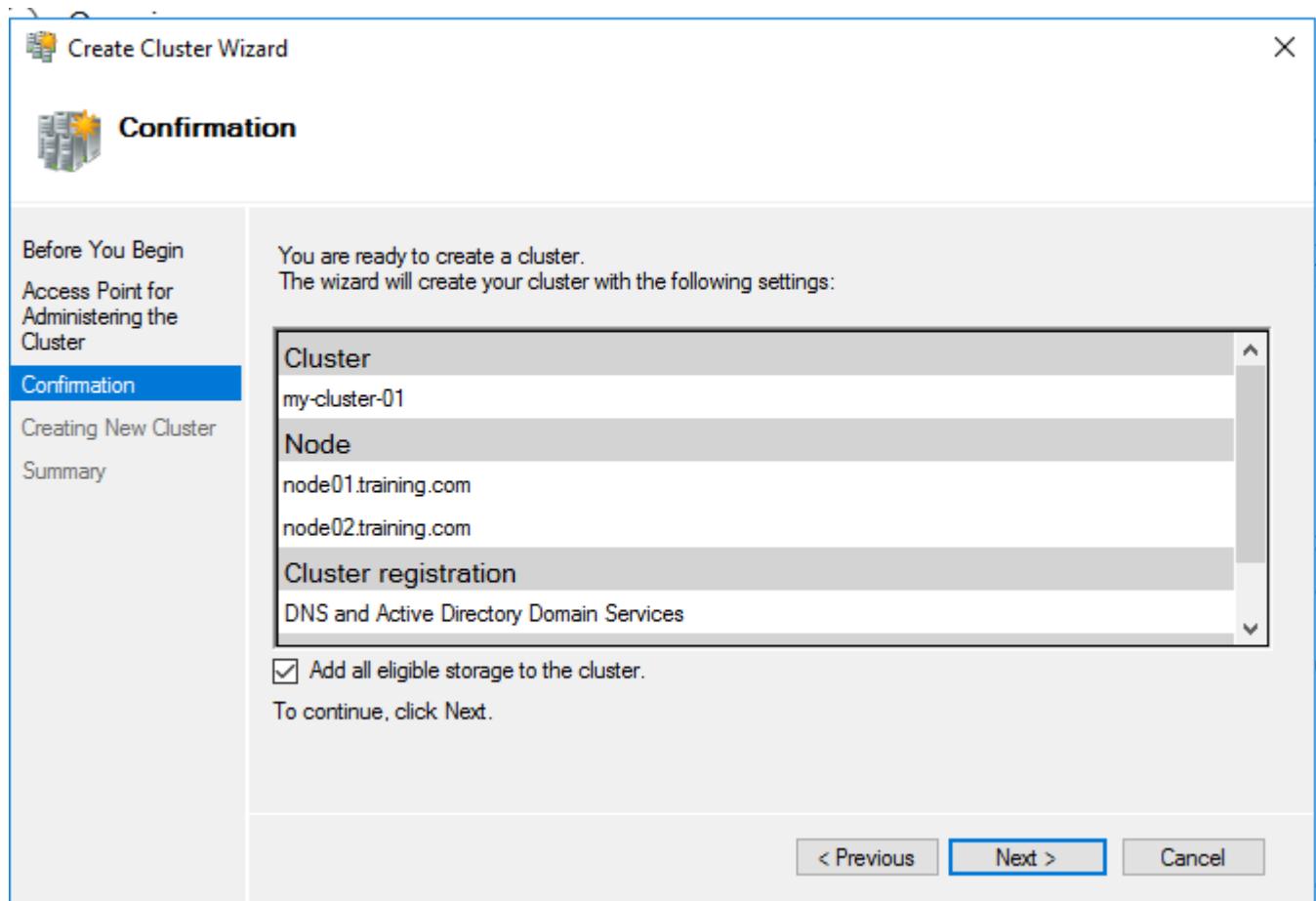
Creating cluster wizard:



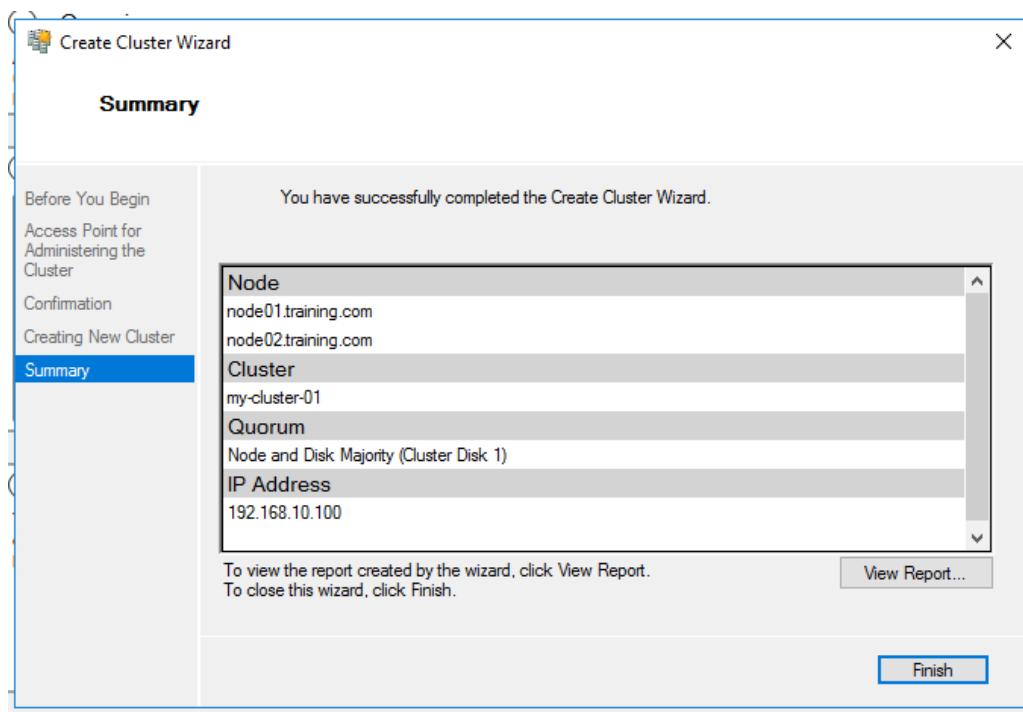
Setting cluster Name & IP address:



Confirmation:



Summary:



View report:

The screenshot shows a Microsoft report titled 'Create Cluster' with the Microsoft logo at the top. The report details the configuration of a new cluster:

Cluster:	my-cluster-01
Node:	node01.training.com
Node:	node02.training.com
Quorum:	Node and Disk Majority (Cluster Disk 1)
IP Address:	192.168.10.100
Cluster registration:	DNS and Active Directory Domain Services
Started	5/3/2025 1:05:40 PM
Completed	5/3/2025 1:06:03 PM

The report then lists the steps taken during the configuration process:

- Beginning to configure the cluster my-cluster-01.
- Initializing Cluster my-cluster-01.
- Validating cluster state on node node01.training.com.
- Searching the domain for computer object 'my-cluster-01'.
- Find a suitable domain controller for node node01.training.com.
- Check whether the computer object my-cluster-01 for node node01.training.com exists in the domain. Domain controller \\windc.training.com.
- Computer object for my-cluster-01 does not exist in the domain.
- Find a suitable domain controller for node node01.training.com.
- Check whether the computer object my-cluster-01 for node node01.training.com exists in the domain. Domain controller \\windc.training.com.
- Bind to domain controller \\windc.training.com.
- Check whether the computer object node01.training.com for node node01.training.com exists in the domain. Domain controller \\windc.training.com.
- Creating a new computer account (object) for 'my-cluster-01' in the domain.

Failover Cluster Manager

Cluster my-cluster-01.training.com

Summary of Cluster my-cluster-01
my-cluster-01 has 0 clustered roles and 2 nodes.

Name: my-cluster-01.training.com **Networks:** Cluster Network 1
Current Host Server: node01 **Subnets:** 1 IPv4 and 0 IPv6
Recent Cluster Events: None in the last hour **Storage Spaces Direct (S2D):** Disabled
Witness: Cluster Disk 1

Configure
Configure high availability for a specific clustered role, add one or more servers (nodes), or copy roles from a cluster running Windows Server 2016 or supported previous versions of Windows Server.

- [Configure Role...](#)
- [Validate Cluster...](#)
- [Add Node...](#)
- [Copy Cluster Roles...](#)
- [Cluster-Aware Updating...](#)

Failover cluster topics on the Web

Actions

- my-cluster-01.training.com
- Configure Role...
- Validate Cluster...
- View Validation Report
- Add Node...
- Close Connection
- Reset Recent Events
- More Actions
- View
- Refresh
- Properties
- Help

Navigate

- [Roles](#)
- [Nodes](#)
- [Storage](#)
- [Networks](#)
- [Cluster Events](#)

Cluster Core Resources

Name	Status	Information
Storage		
Cluster Disk 1	Online	
Server Name		
Name: my-cluster-01	Online	

Listing disks:

Failover Cluster Manager

my-cluster-01.training.com

- Roles
- Nodes
- Storage
 - Disks
 - Pools
 - Enclosures
- Networks
- Cluster Events

Disk (1)

Name	Status	Assigned To	Owner Node	Disk Number	Partition Style
Cluster Disk 1	Online	Disk Witness in Quorum	node01	1	MBR

Actions

- Add Disk
- Move Available Storage
- View
- Refresh
- Help

Listing nodes:

Failover Cluster Manager

my-cluster-01.training.com

- Roles
- Nodes
- Storage
 - Disks
 - Pools
 - Enclosures
- Networks
- Cluster Events

Nodes (2)

Name	Status	Assigned Vote	Current Vote	Site	Rack
node01	Up	1	1		
node02	Up	1	1		

Actions

- Add Node...
- View
- Refresh
- Help

END of cluster

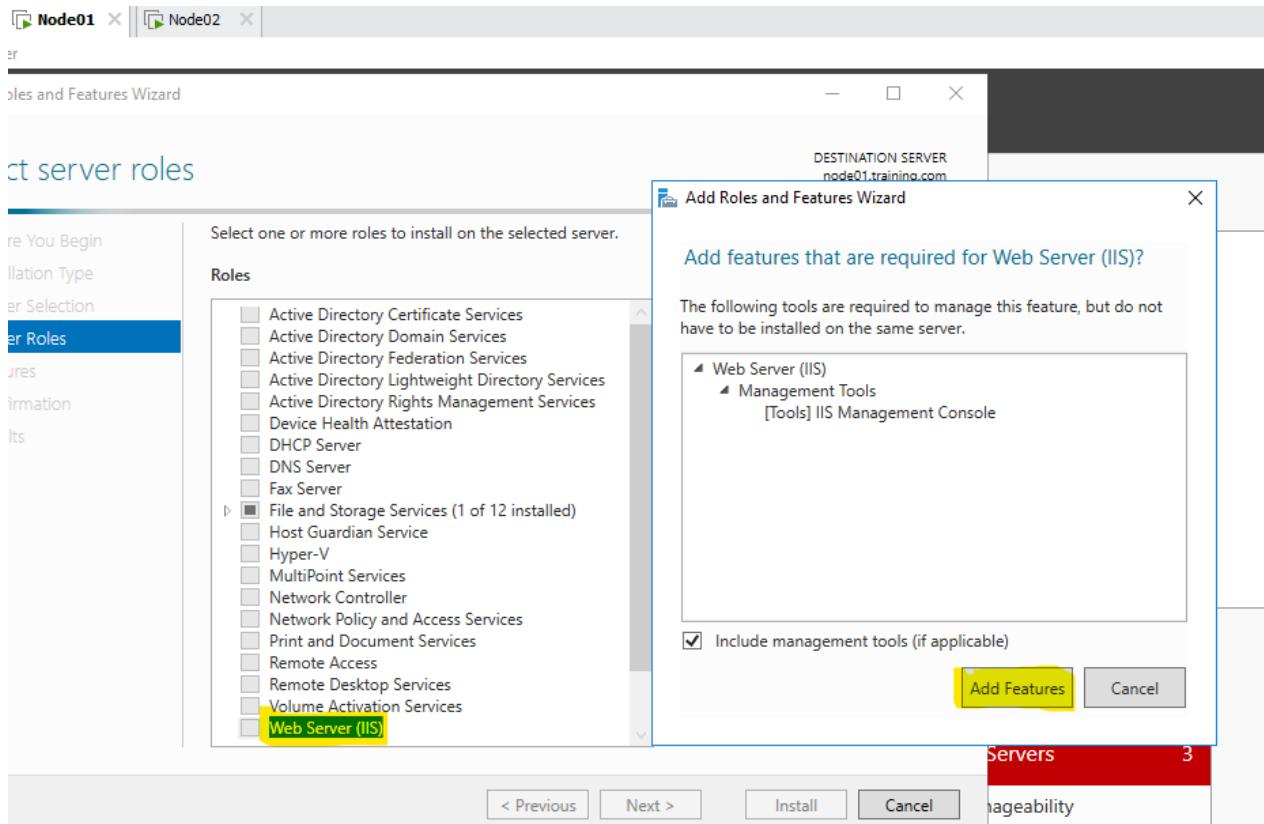
Network Load Balancing

Note: Uninstall/remove failover clustering before NLB and reboot

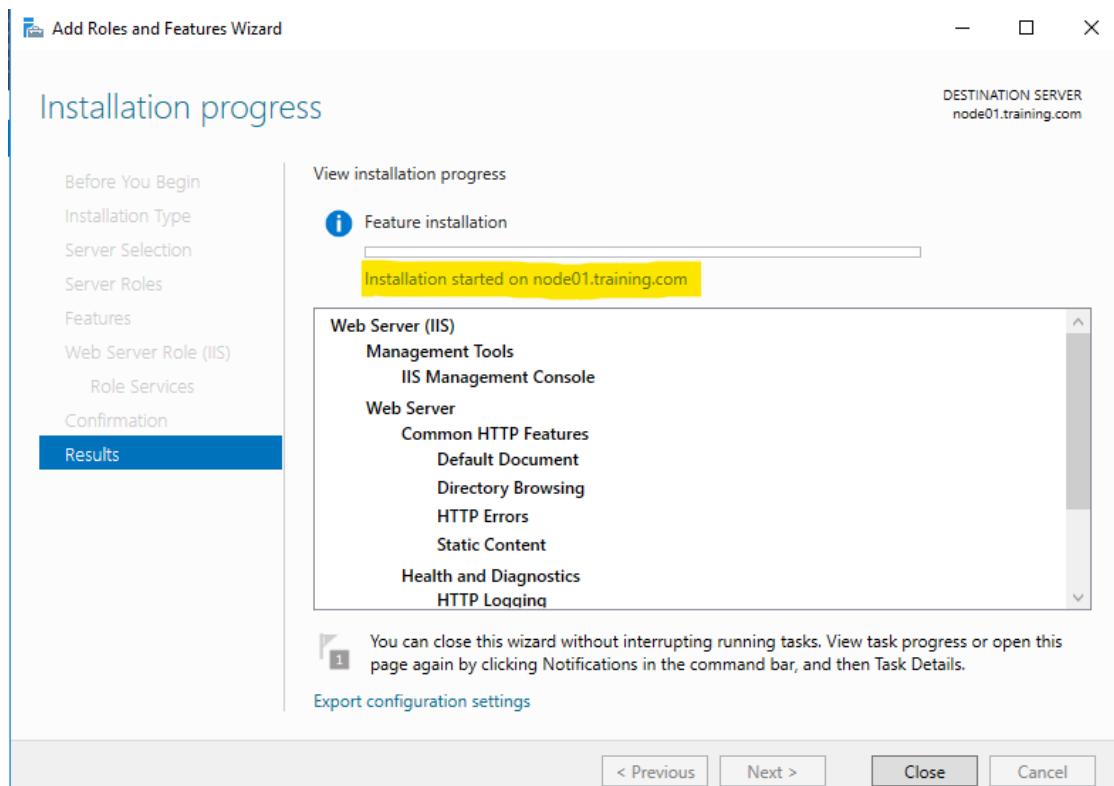
Installing IIS web server role on each Node (01 & 02):

Node 01:

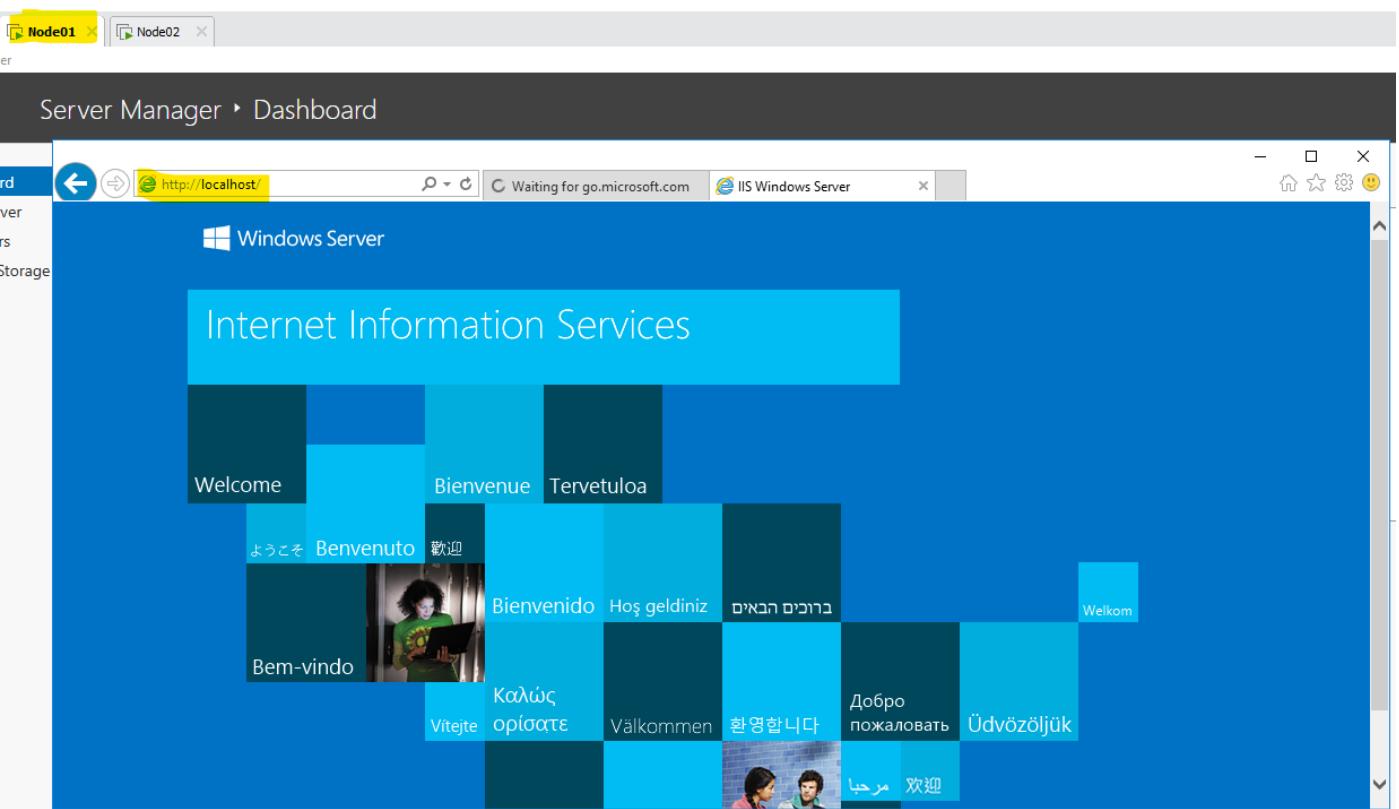
Server manager dashboard page:



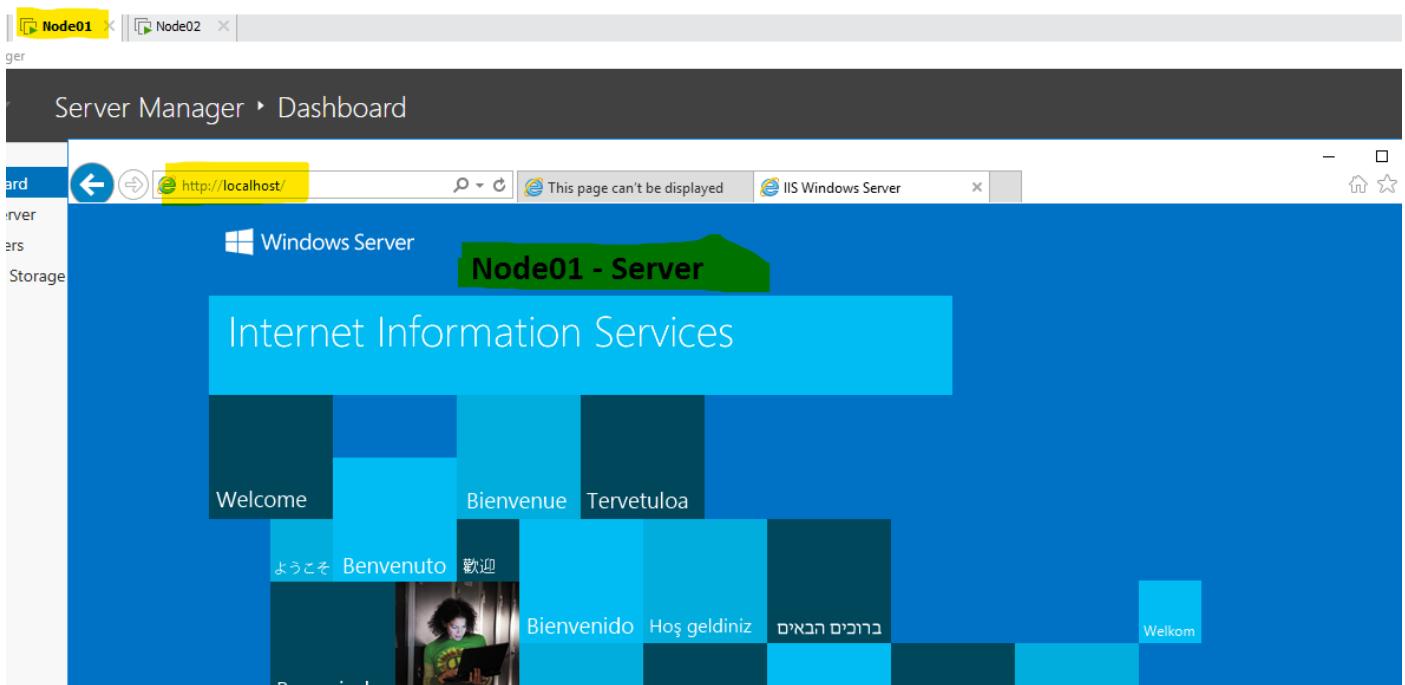
Wait...



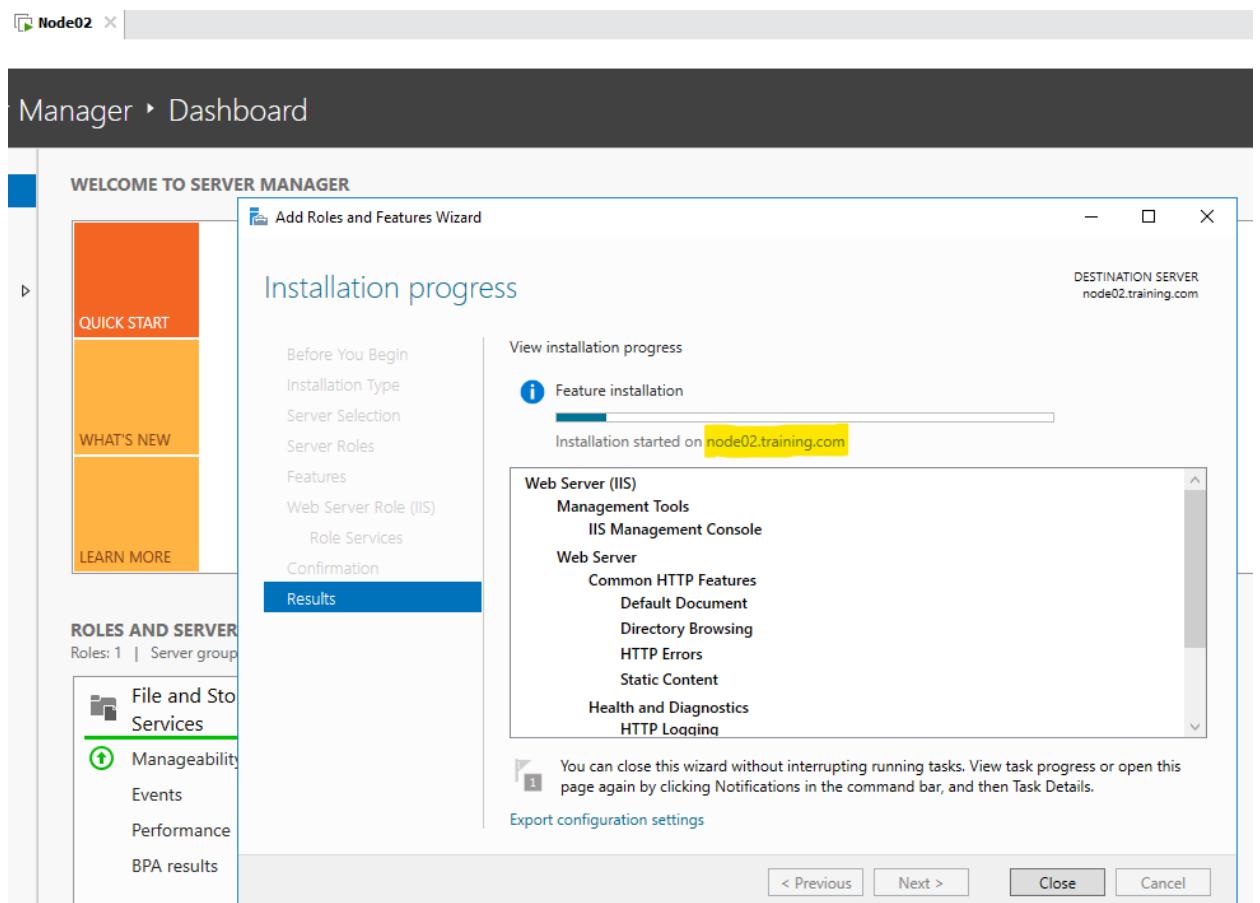
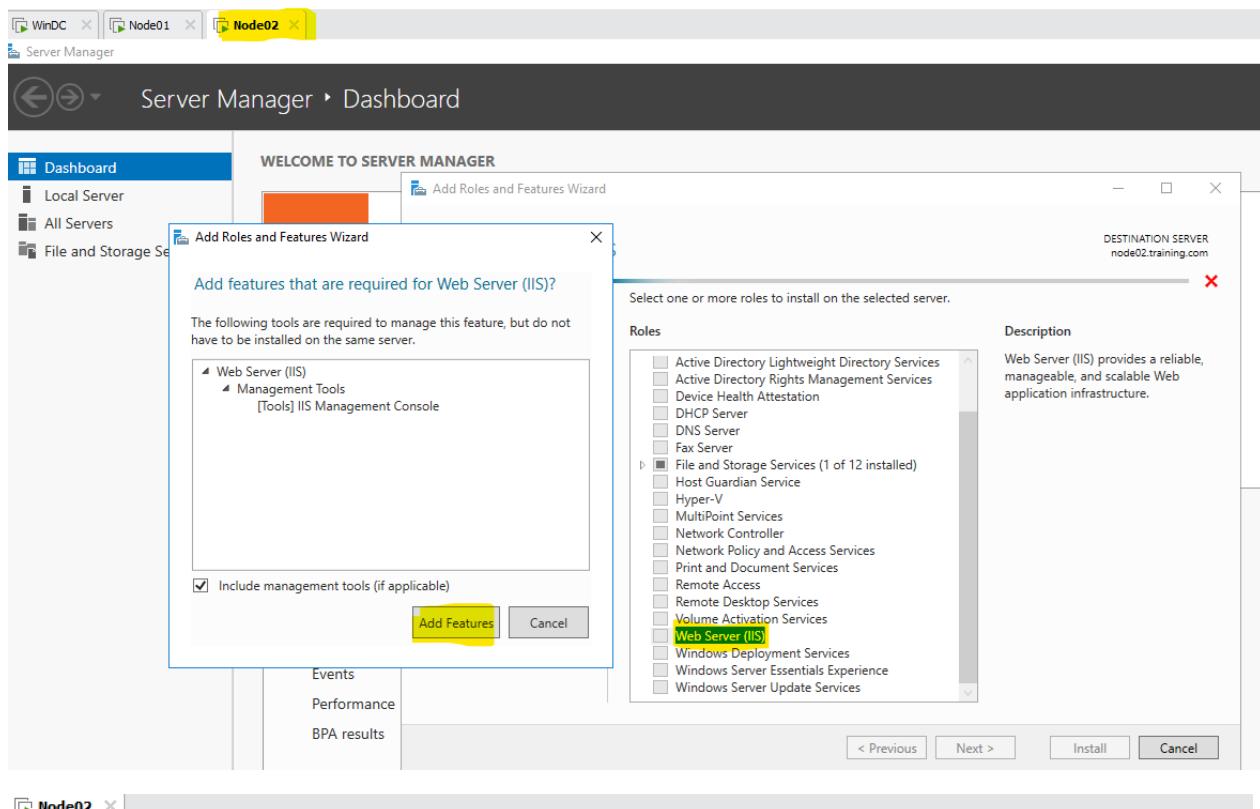
Verifying the installation using browser (<http://localhost>)



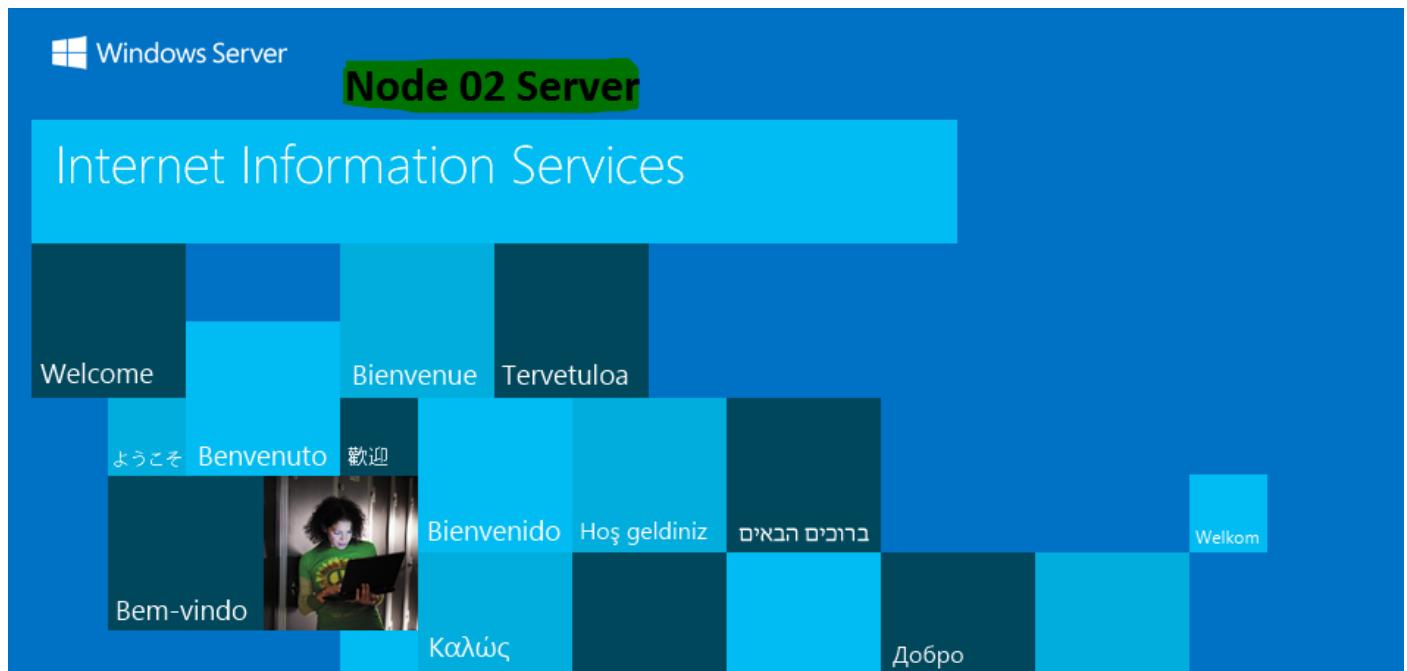
Edit the webpage or image file present on “C:\inetpub\wwwroot”:



Node 02:

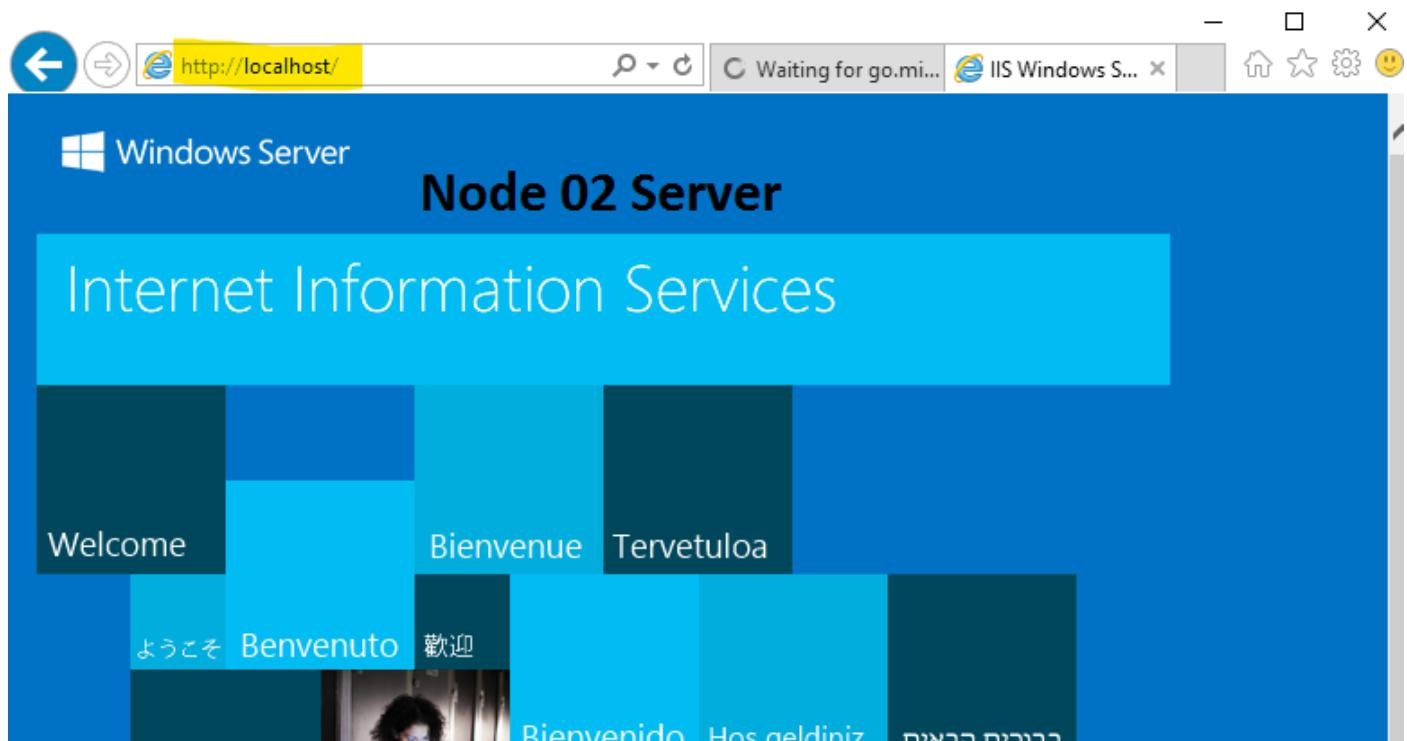


Edit the page at default HTML page or Image file on "C:\inetpub\wwwroot\"



Verify on localhost:

Open web browser and type "http://localhost/"



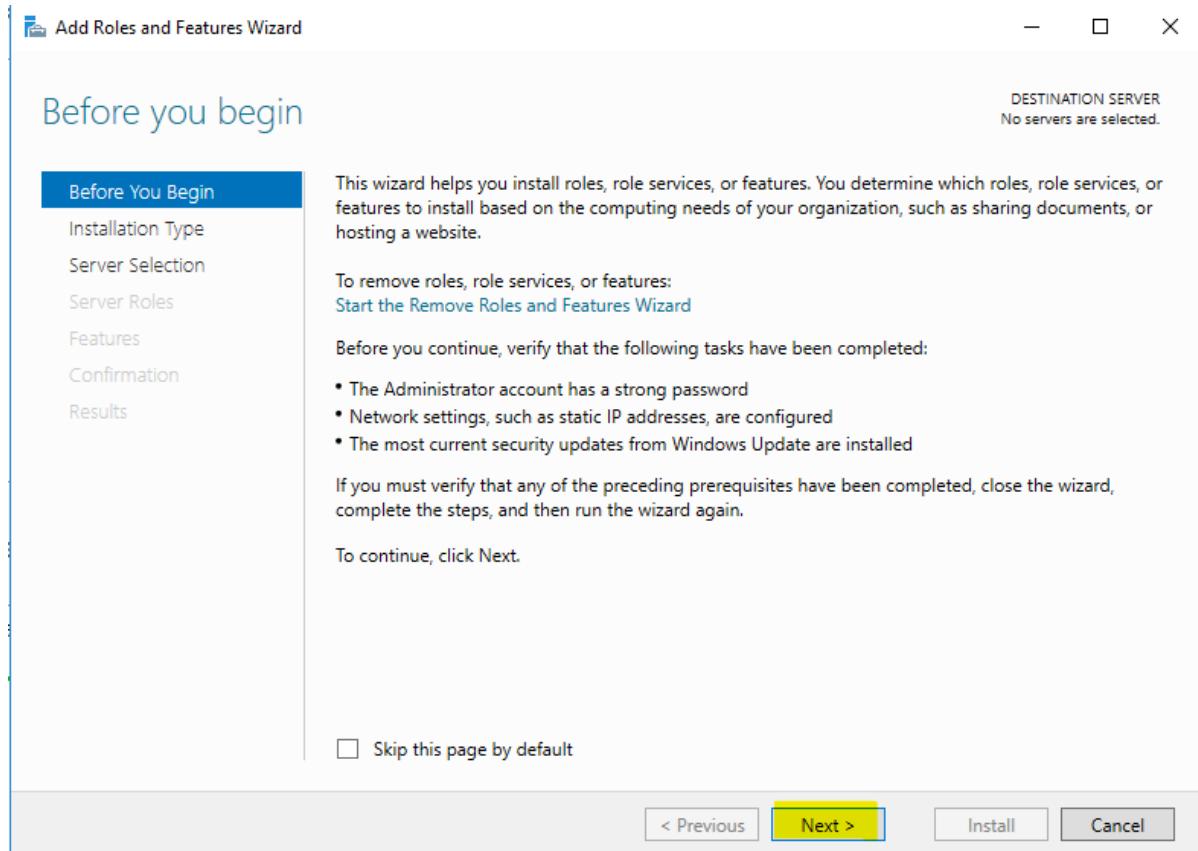
Now installing Network Load Balancer (NLB) on both Nodes 01 & 02:

Note: Uninstall/remove failover clustering before NLB

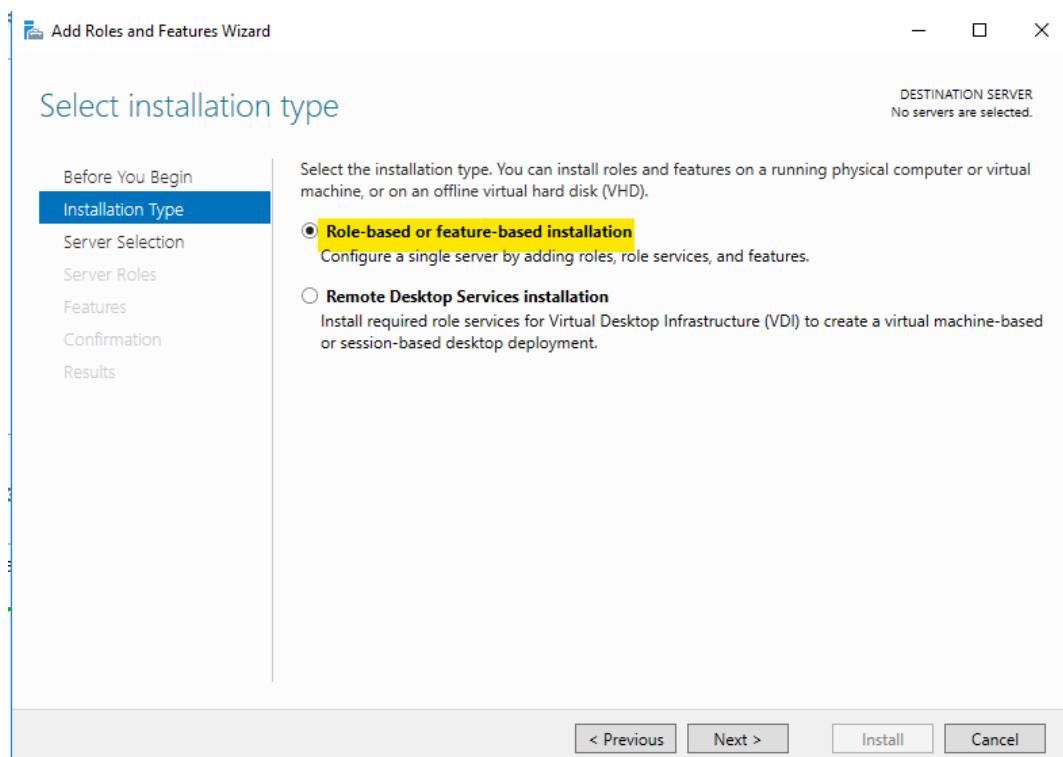
Node01:

Server Manager Dashboard → NLB role

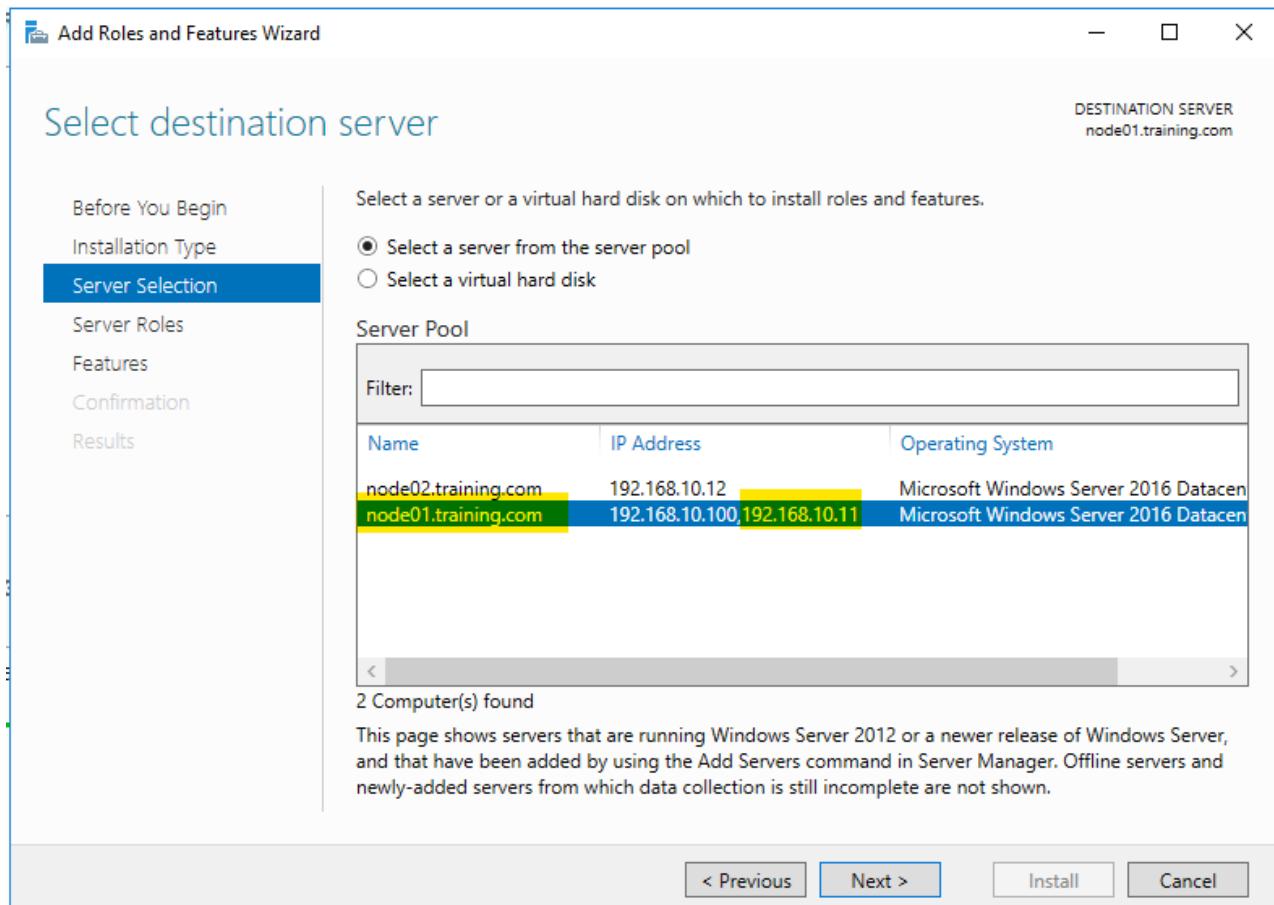
Skip 1st page:



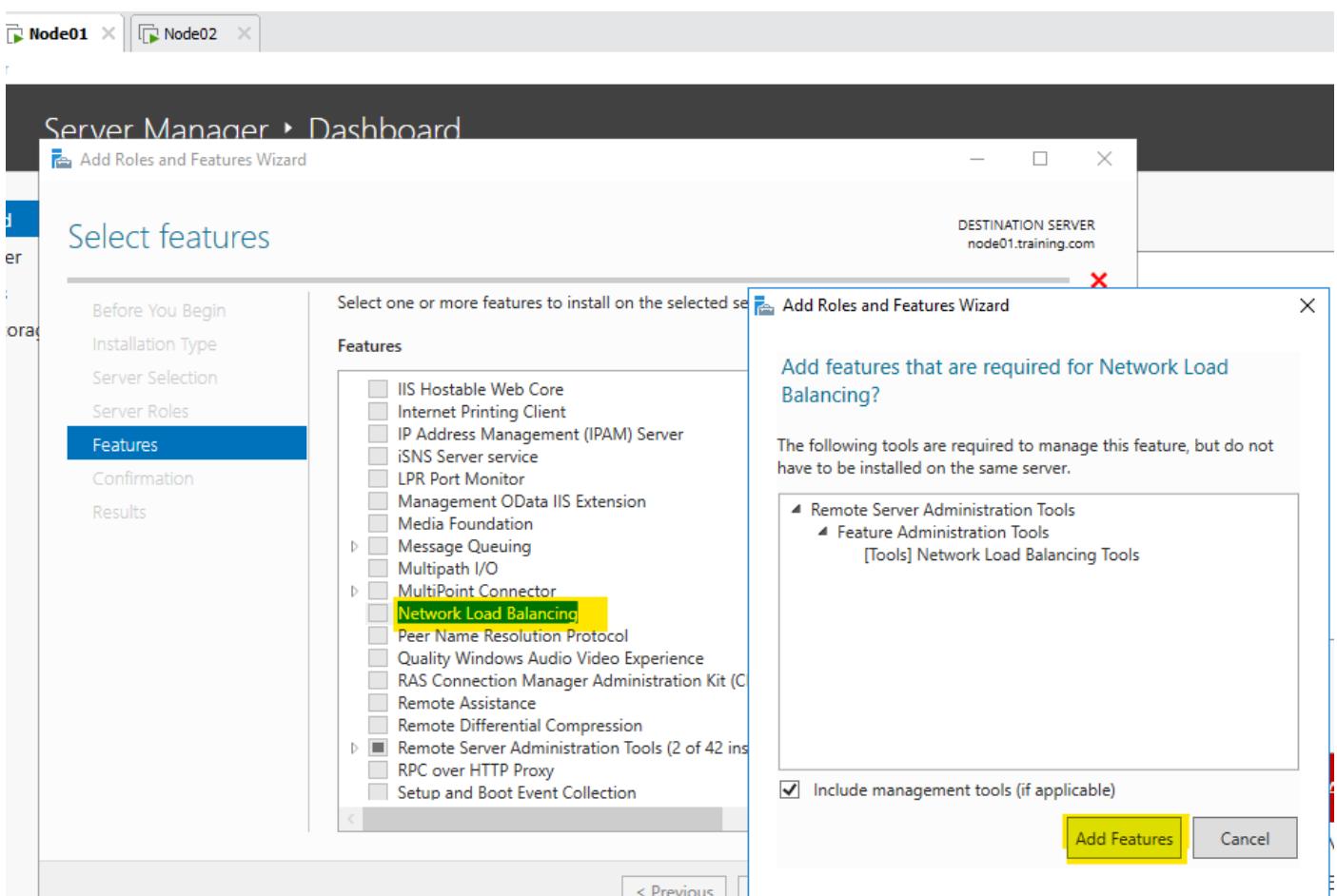
Select “Role-base or feature-based installation”:



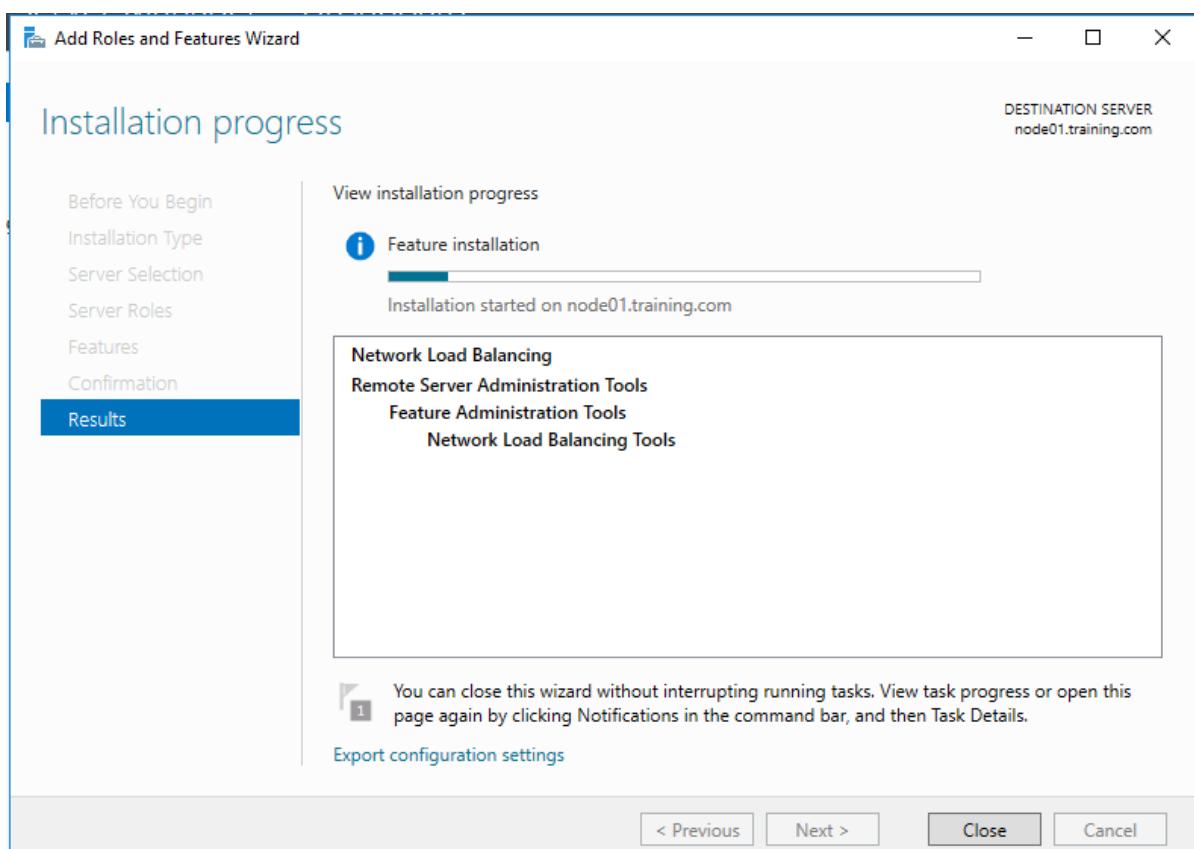
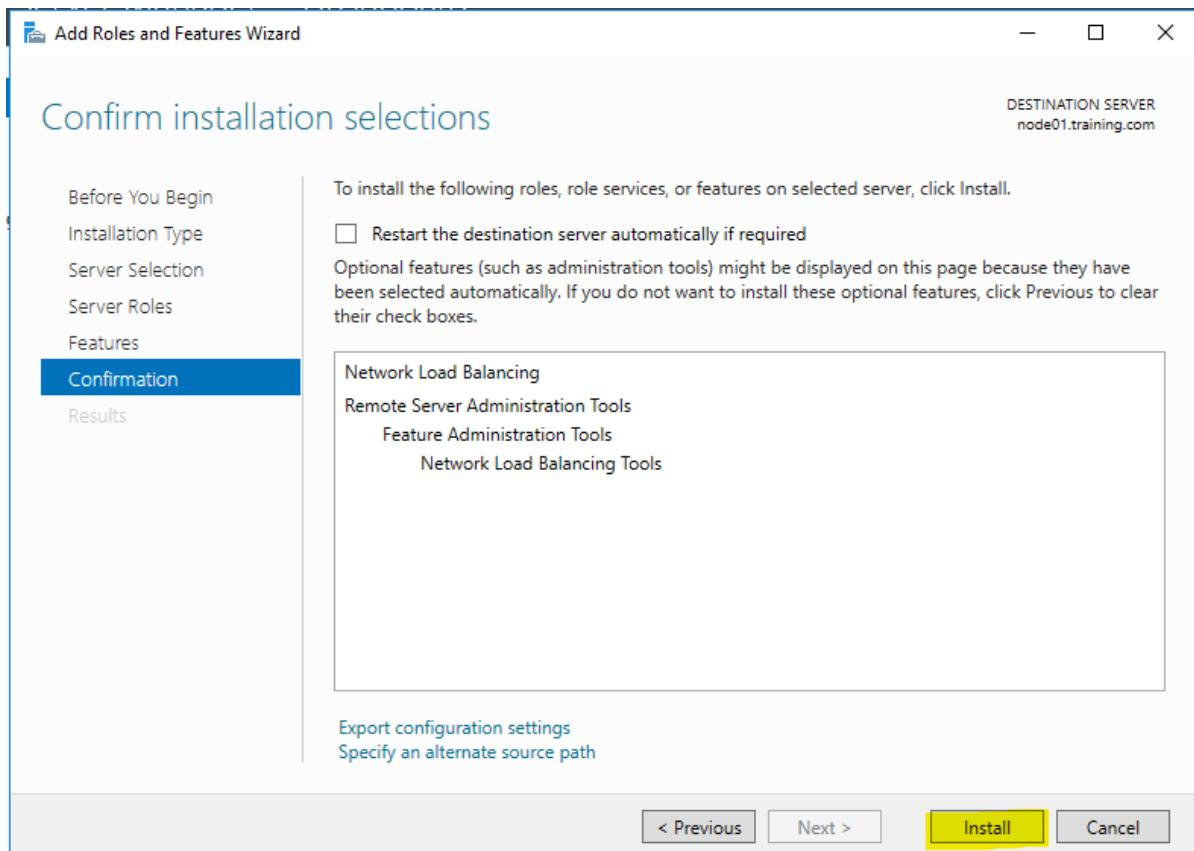
Select proper destination server:



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



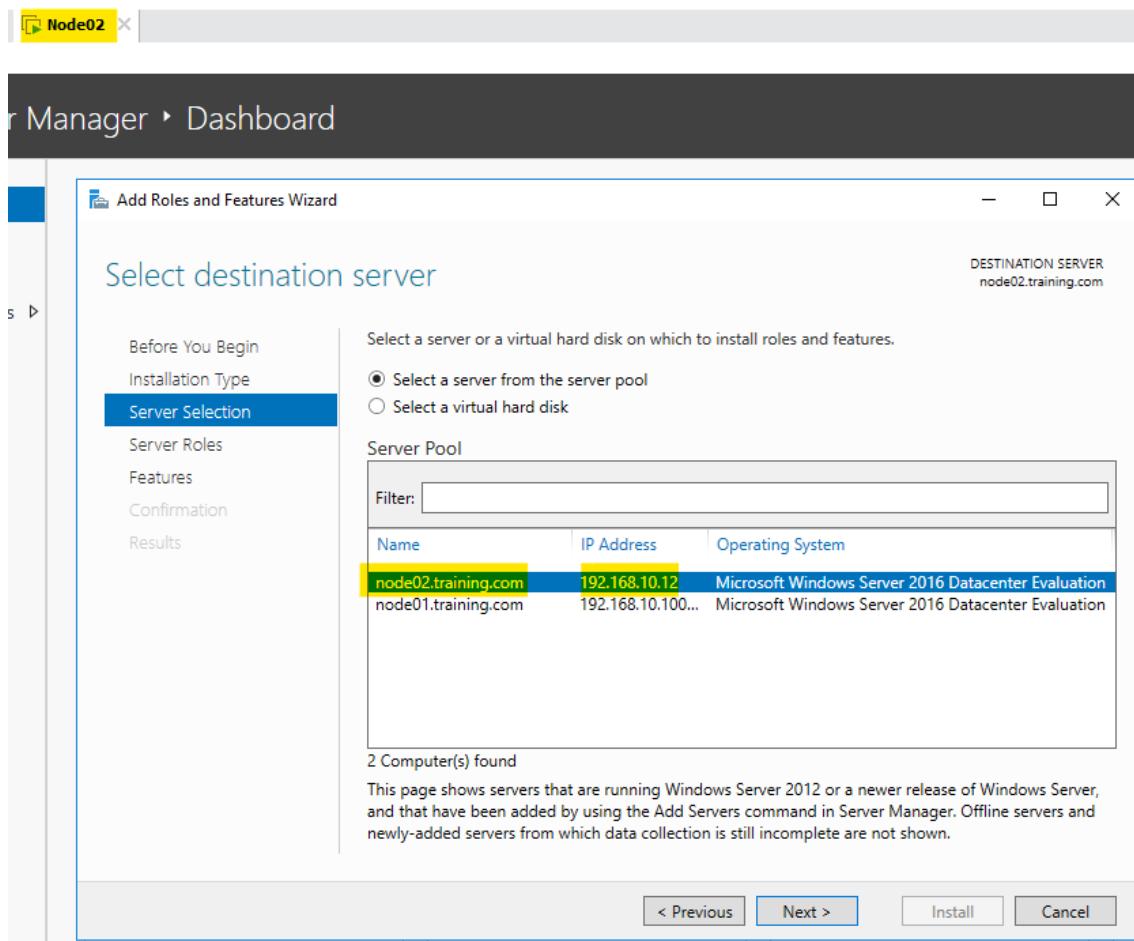
Click "install":



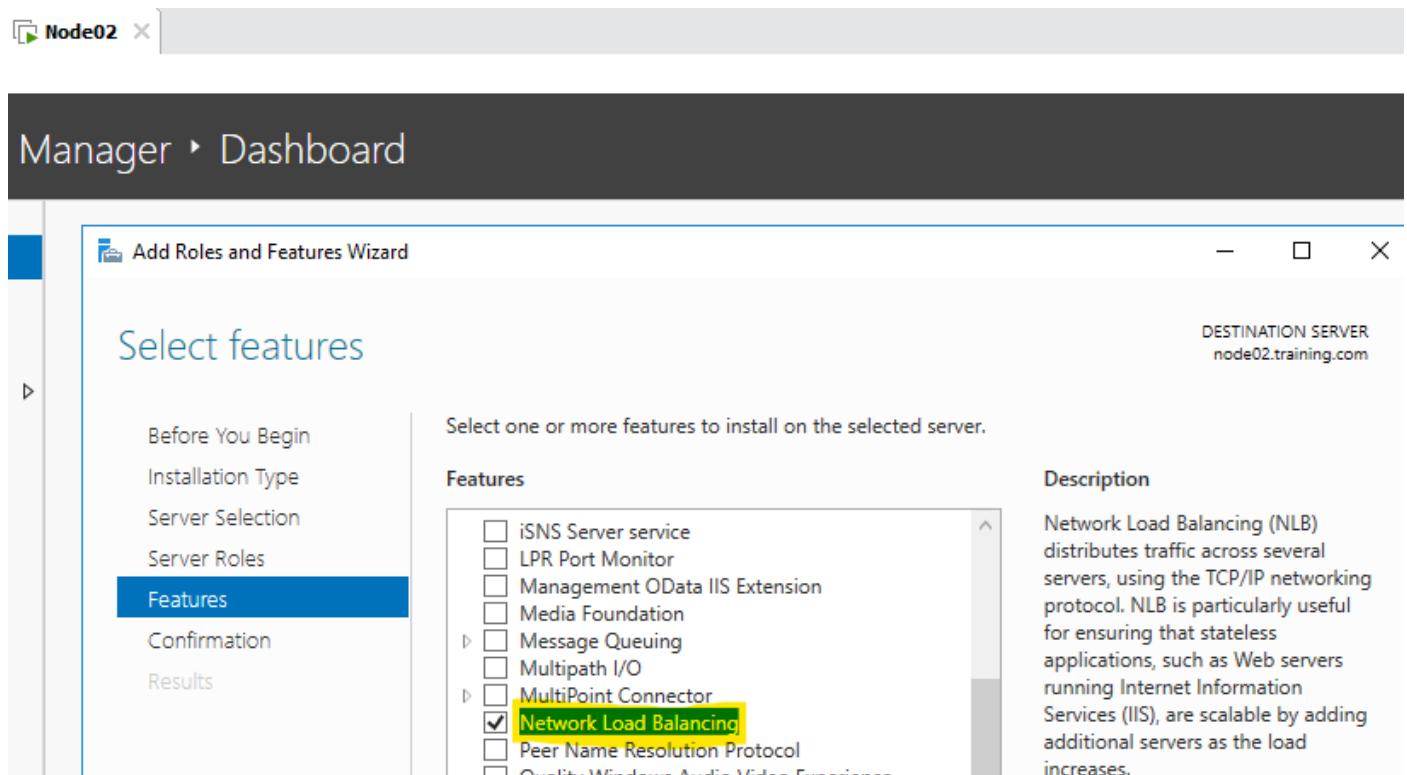
Node02:

Server Manager Dashboard → NLB role

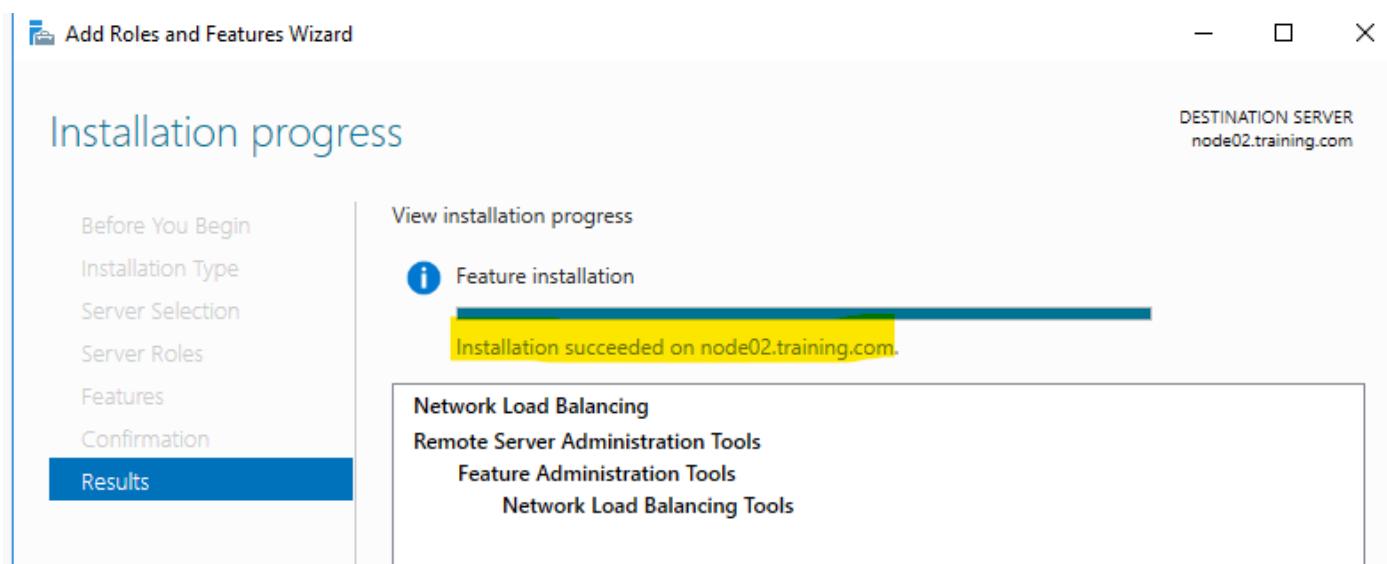
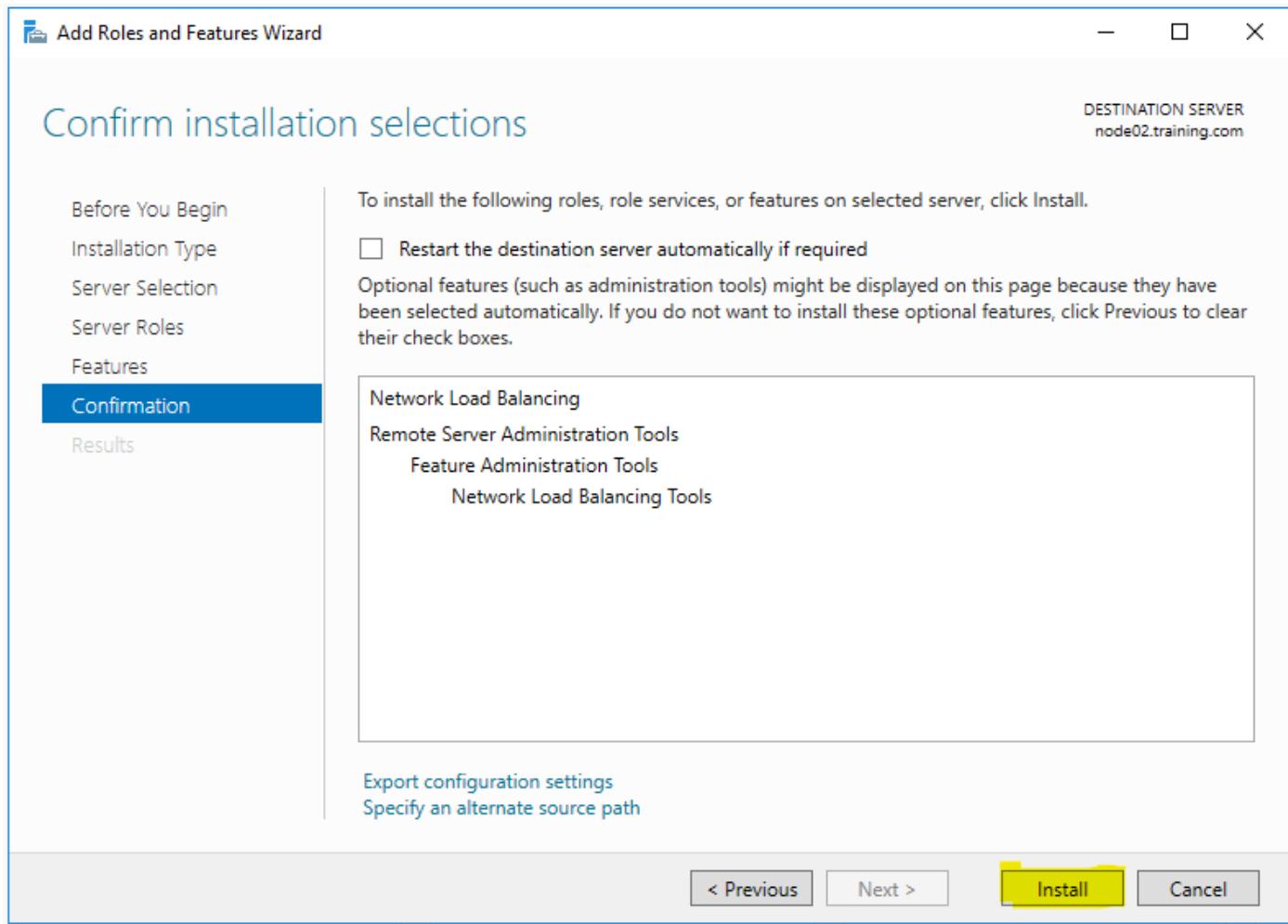
Skip 1st page:



Selecting Network Load Balancing (NLB):

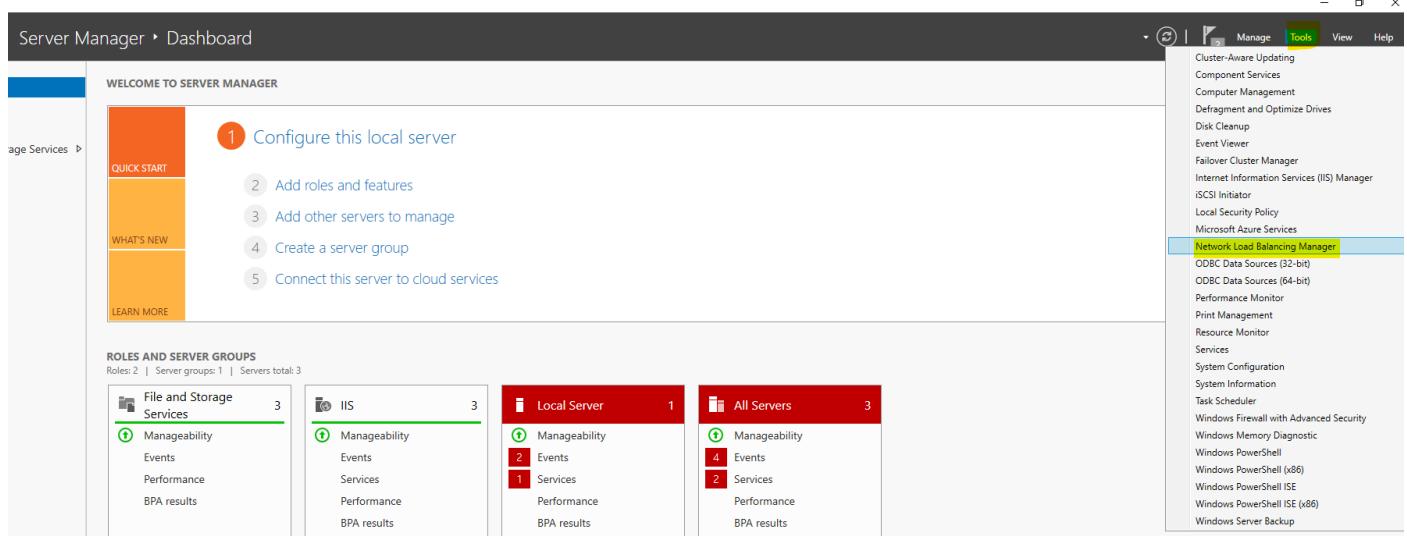


Install:

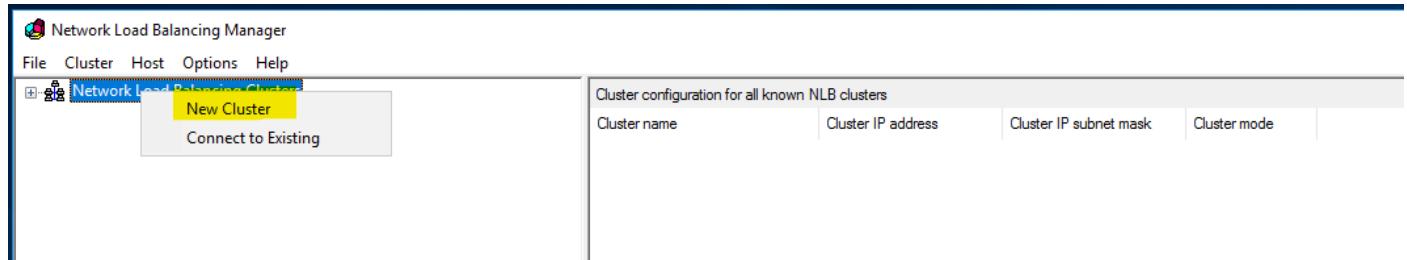


Configuring NLB on Node01:

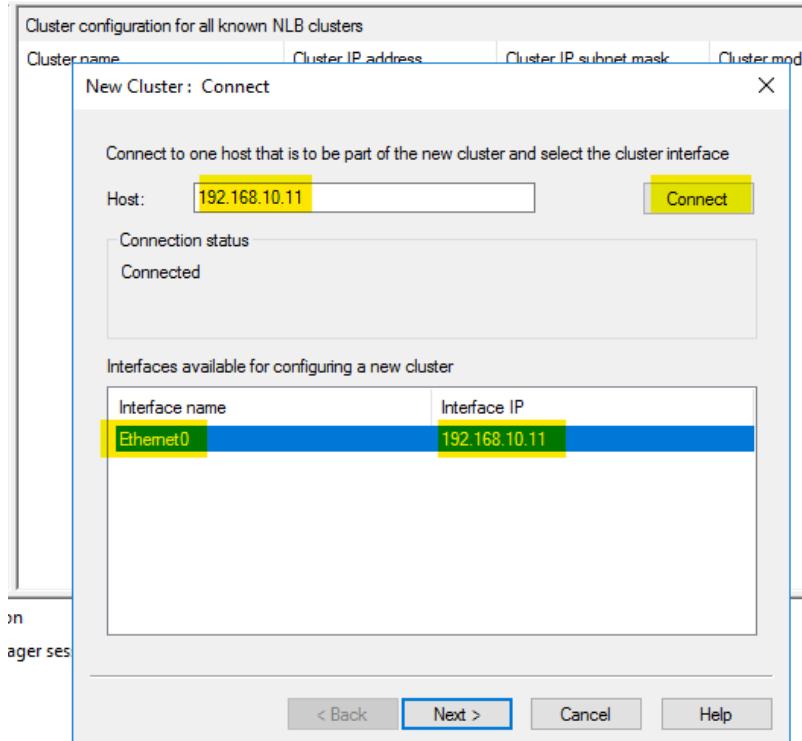
Server Manager Dashboard → Tools → Network Load balancing:



Right-click on the NLB clustering:

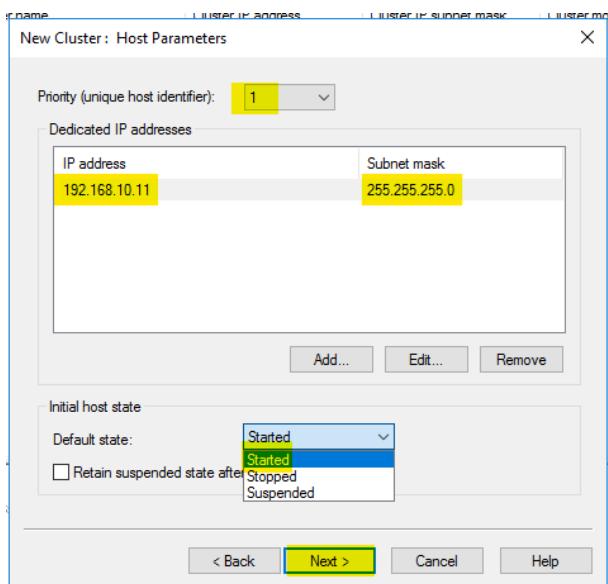


Enter Node01 (IP Address: 192.168.10.11) & click on "Connect"

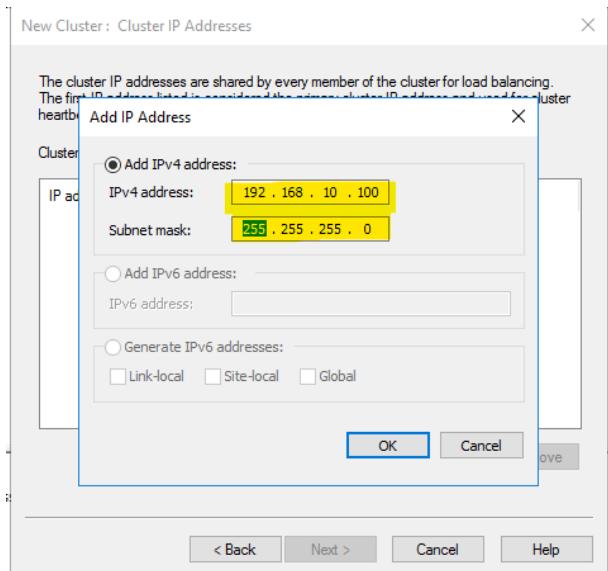


And click "Next"

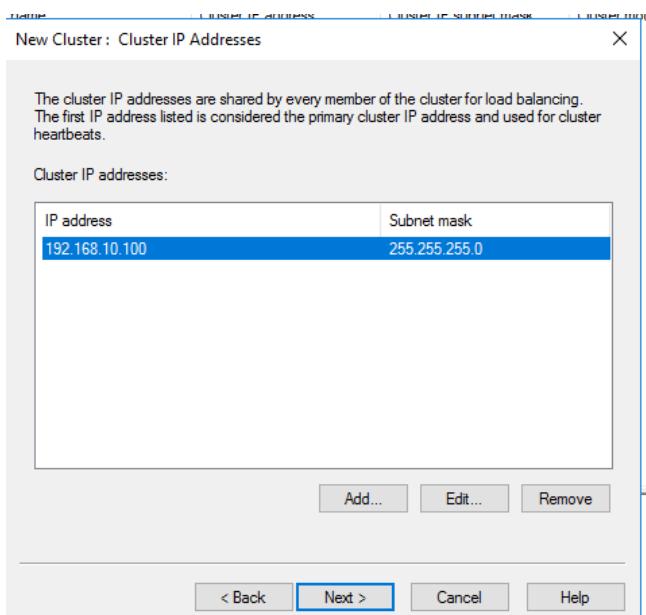
Verify "New Cluster: Host Parameters":



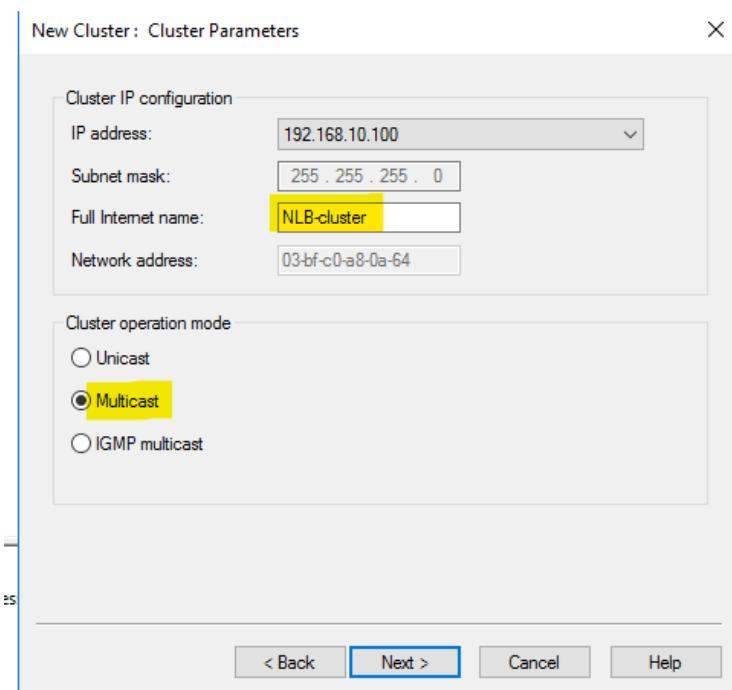
Add a new IP address (192.168.10.100) with subnet mask:



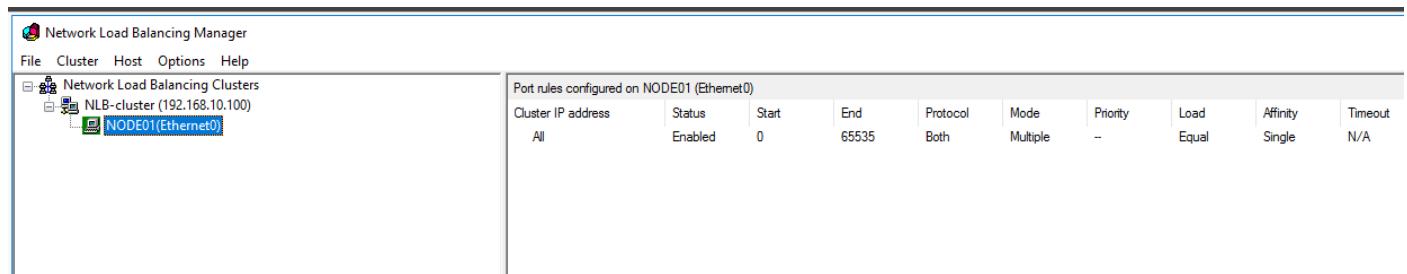
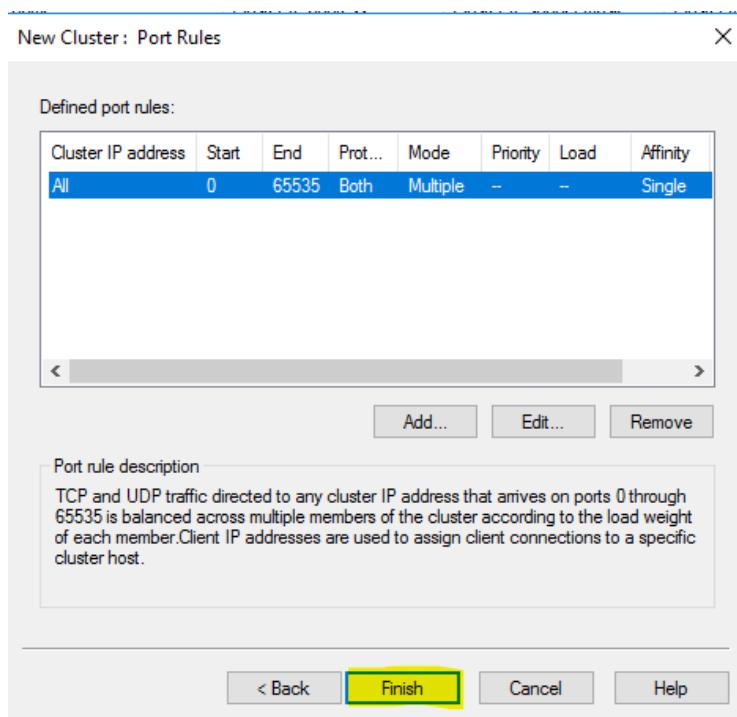
Next:



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



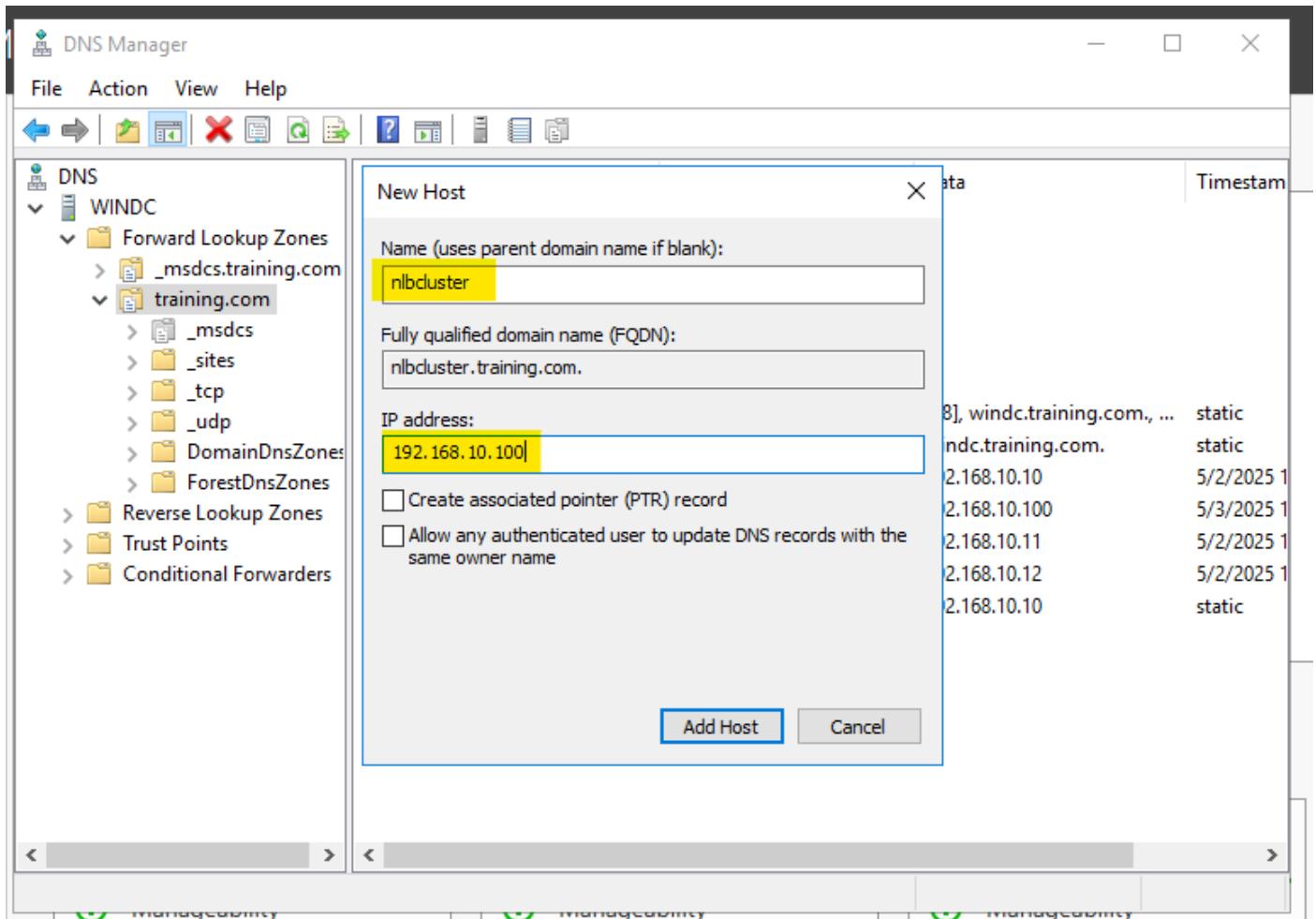
Click “Finish”:



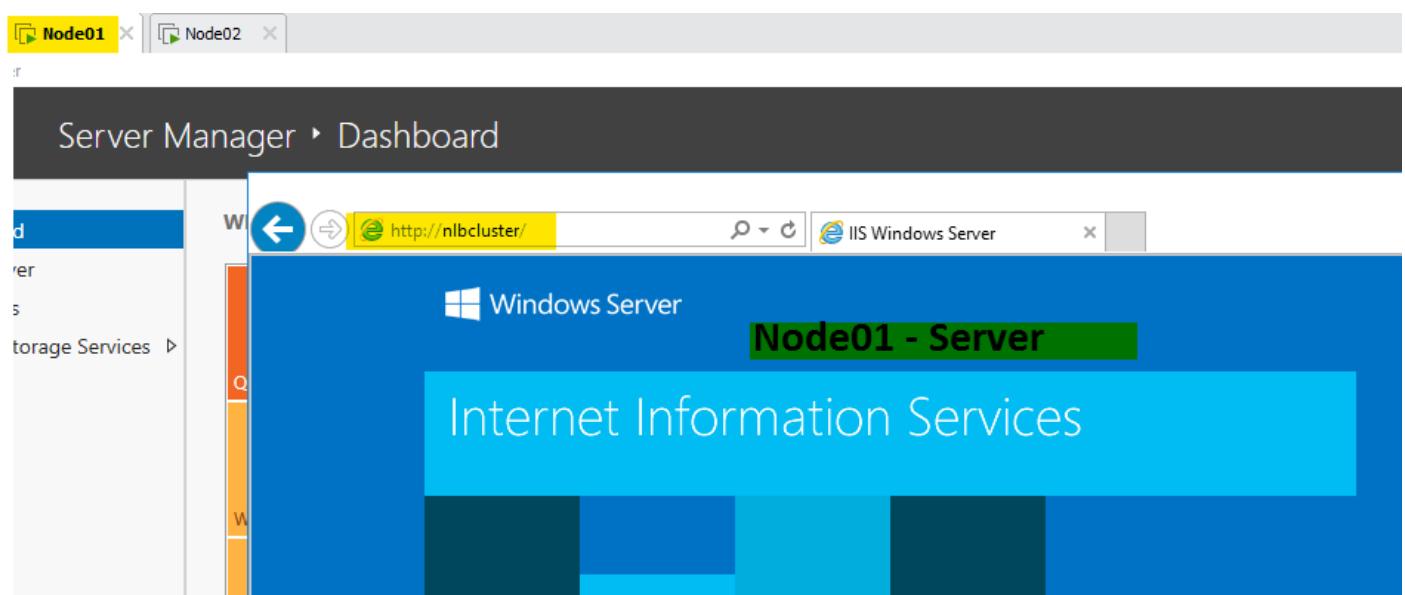
Now, create an A record in DNS server

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:

The screenshot shows the Windows Network Load Balancing Manager interface. On the left, under 'Network Load Balancing Clusters', there is a tree view with 'NLB-cluster (192.168.10.100)' expanded, and 'NODE01(Ethernet0)' selected. A context menu is open over this node, with 'Add Host To Cluster' highlighted. Other options in the menu include 'Delete Cluster', 'Cluster Properties', 'Refresh', 'Remove From View', 'Control Hosts', and 'Control Ports...'. To the right, a table titled 'Host configuration information for hosts in cluster NLB-cluster (192.168.10.100)' displays one host entry: 'NODE01(Ethernet0)' with status 'Converged', dedicated IP '192.168.10.11', subnet mask '255.255.255.0', host priority '1', and initial host state 'started'.

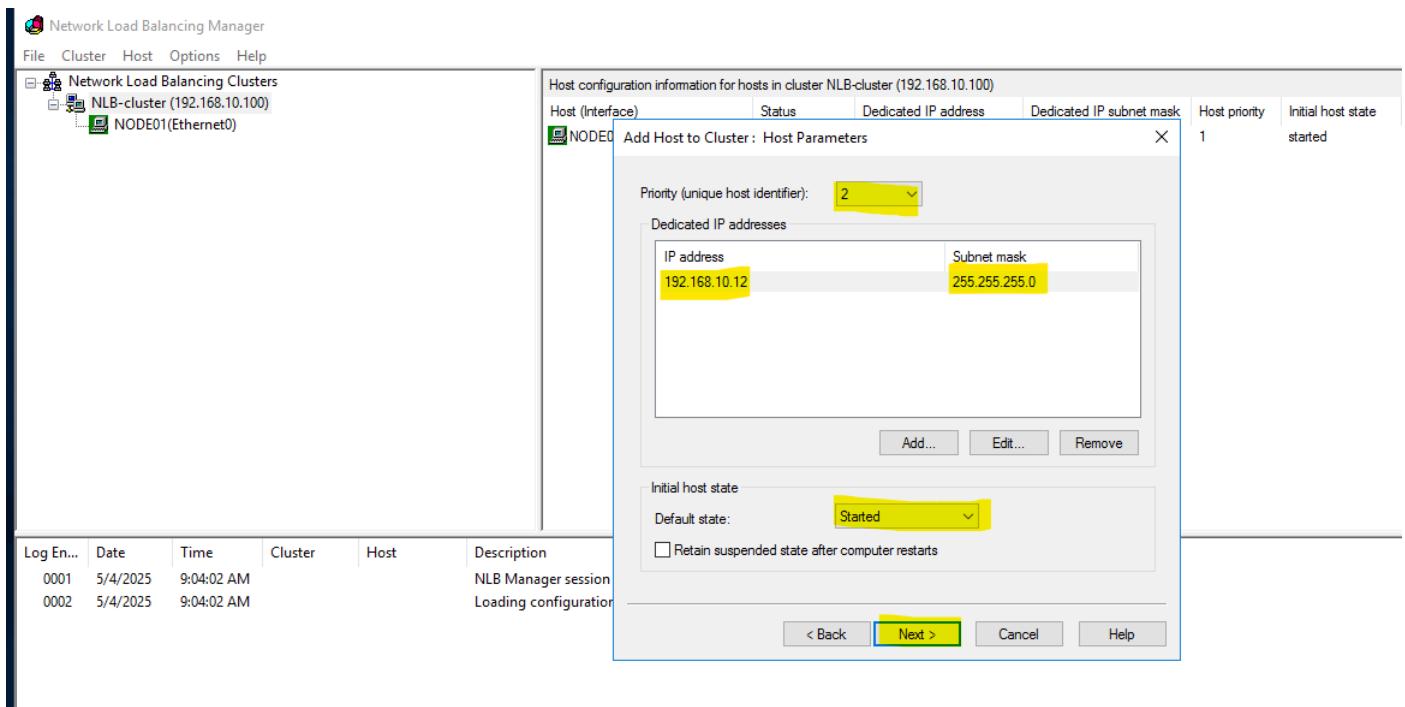
Which adding Node02(192.168.10.12), it is expected to see "Not Responding":

A modal dialog box titled 'Add Host to Cluster : Connect' is displayed. It contains a table with columns 'Host (Interface)', 'Status', 'Dedicated IP address', 'Dedicated IP subnet mask', and 'Host priority'. The 'Status' column for the entry 'NODE02' is highlighted with a yellow box and shows the text 'Not Responding'. Below the table, there is a message: 'Connect to the host that is to be added to the existing cluster'. A 'Host:' input field contains '192.168.10.12'. A 'Connect' button is to the right. Under 'Connection status', it says 'Connecting...'. At the bottom, a section titled 'Interfaces available for configuring the cluster' lists 'Interface name' and 'Interface IP' for 'Ethernet0' (IP 192.168.10.12).

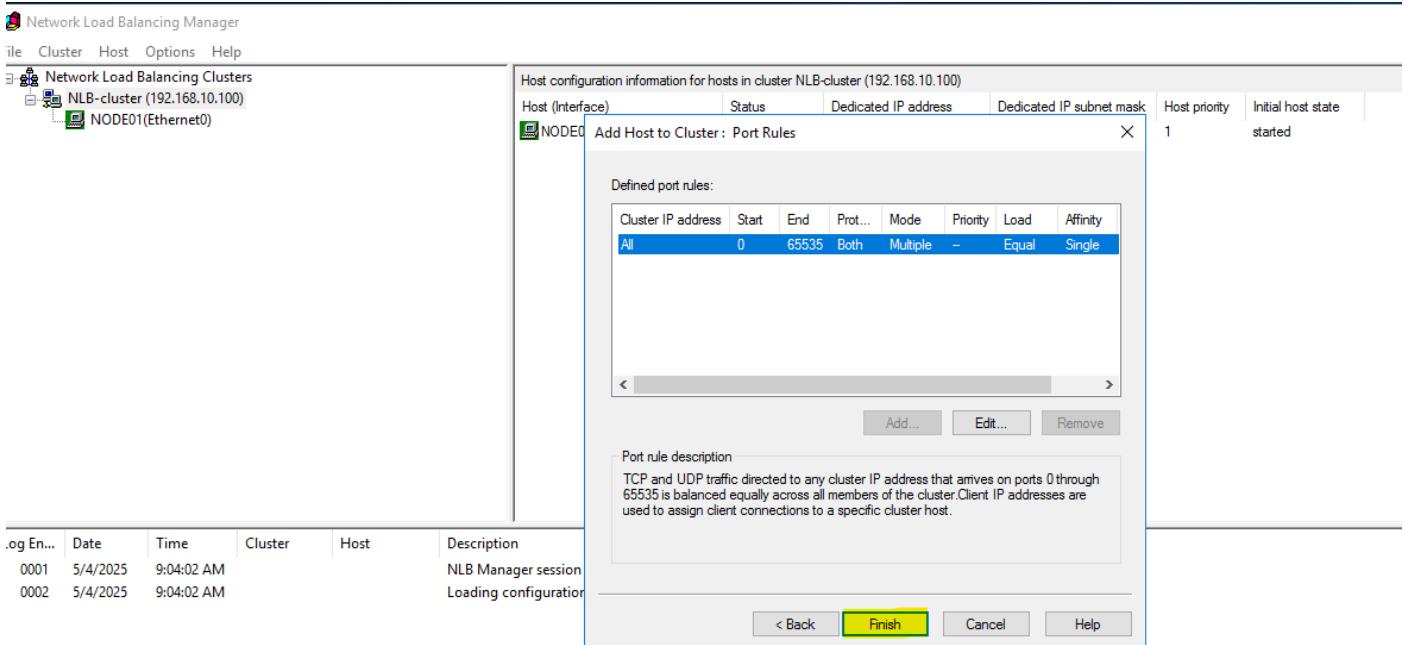
Click Next:

The screenshot shows the continuation of the 'Add Host to Cluster : Connect' process. The 'Host:' field now contains '192.168.10.12'. The 'Connection status' field shows 'Connected'. The 'Interface name' and 'Interface IP' for 'Ethernet0' (192.168.10.12) are listed in the 'Interfaces available for configuring the cluster' table. At the bottom of the dialog, there are buttons for '< Back', 'Next >', 'Cancel', and 'Help'. In the background, the main Network Load Balancing Manager window shows the cluster configuration and a log table at the bottom.

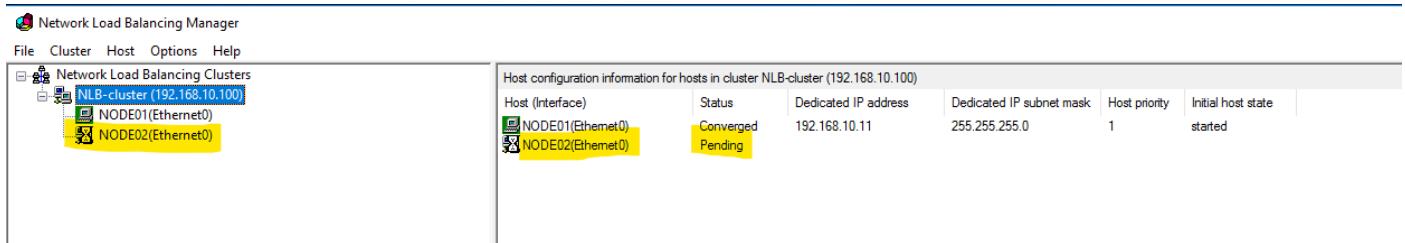
Verify the priority (as 2) & click Next:



Click finish:



Wait until status changes:



Else refresh the NLB cluster & verify:

The screenshot shows the Network Load Balancing Manager interface. In the left pane, under 'Network Load Balancing Clusters', there is one entry: 'NLB-cluster (192.168.10.100)'. Underneath it, two nodes are listed: 'NODE01(Ethernet0)' and 'NODE02(Ethernet0)'. In the main pane, a table titled 'Host configuration information for hosts in cluster NLB-cluster (192.168.10.100)' is displayed. It has columns for 'Host (Interface)', 'Status', 'Dedicated IP address', 'Dedicated IP subnet mask', 'Host priority', and 'Initial host state'. Two rows are present: 'NODE01(Ethernet0)' with status 'Converged', IP '192.168.10.11', subnet mask '255.255.255.0', priority '1', and state 'started'; and 'NODE02(Ethernet0)' with status 'Converged', IP '192.168.10.12', subnet mask '255.255.255.0', priority '2', and state 'started'.

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

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

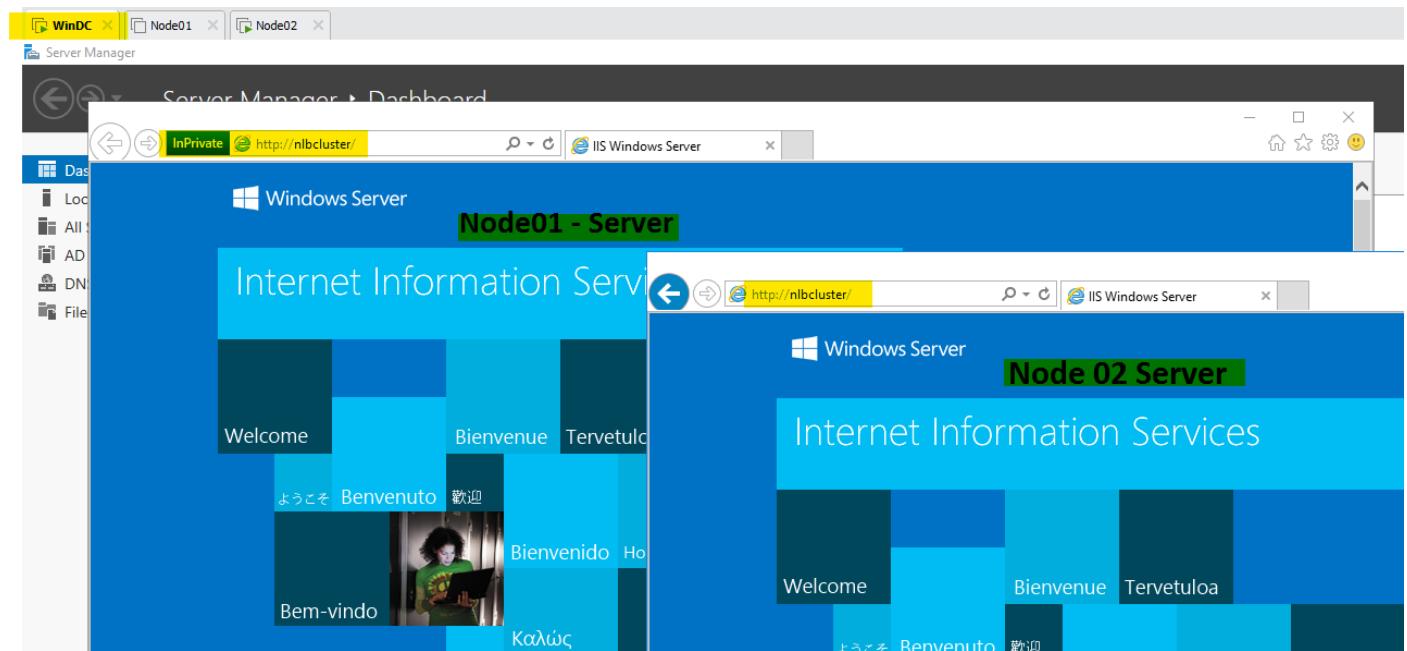
The screenshot shows a Microsoft Internet Explorer window titled 'Node02'. The address bar displays 'InPrivate http://nlbcluster/'. The main content is a 'Windows Server' landing page for 'Node 02 Server'. The page features a large blue header with the text 'Internet Information Services'. Below the header, there is a grid of international welcome messages. The grid includes the following text in various languages:

Welcome	Bienvenue	Tervetuloa	ようこそ	Benvenuto	歡迎	Bienvenido	Hos geldiniz	ברוכים הבאים	Bem-vindo	Καλώς	oirásaté	Vítejte	Välkommen	환영합니다	Добро	пожаловать	Üdvöz
Welcome	Bienvenue	Tervetuloa	ようこそ	Benvenuto	歡迎	Bienvenido	Hos geldiniz	ברוכים הבאים	Bem-vindo	Καλώς	oirásaté	Vítejte	Välkommen	환영합니다	Добро	пожаловать	Üdvöz

The page also features a small image of a person working on a laptop.

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 off 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)

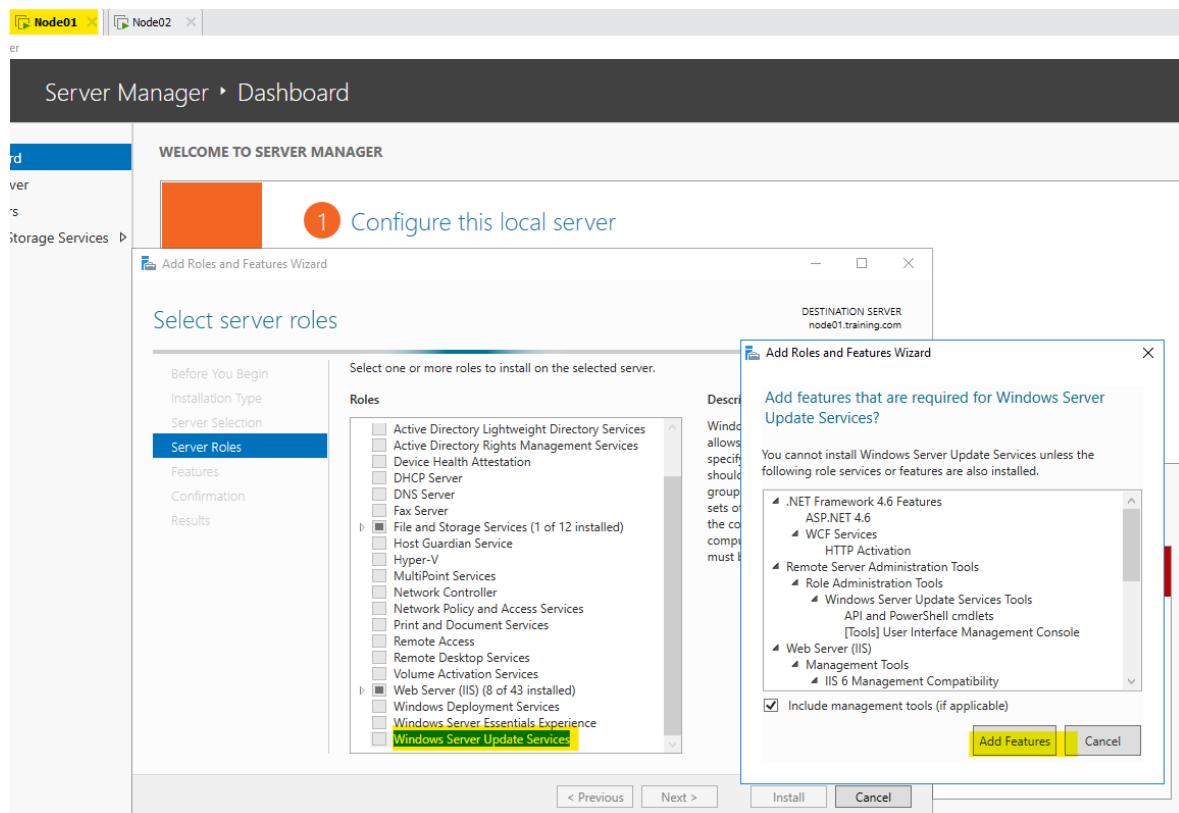
- WSUS can operate independently of a domain.
- Clients must be configured manually or via local group policy:
- Use gpedit.msc on each machine.
- Configure update server location (http://WSUS_Server:8530).
- No centralized client control via Group Policy Objects (GPO).
- Manual client grouping or use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

WSUS with a Domain (Recommended for Larger Environments)

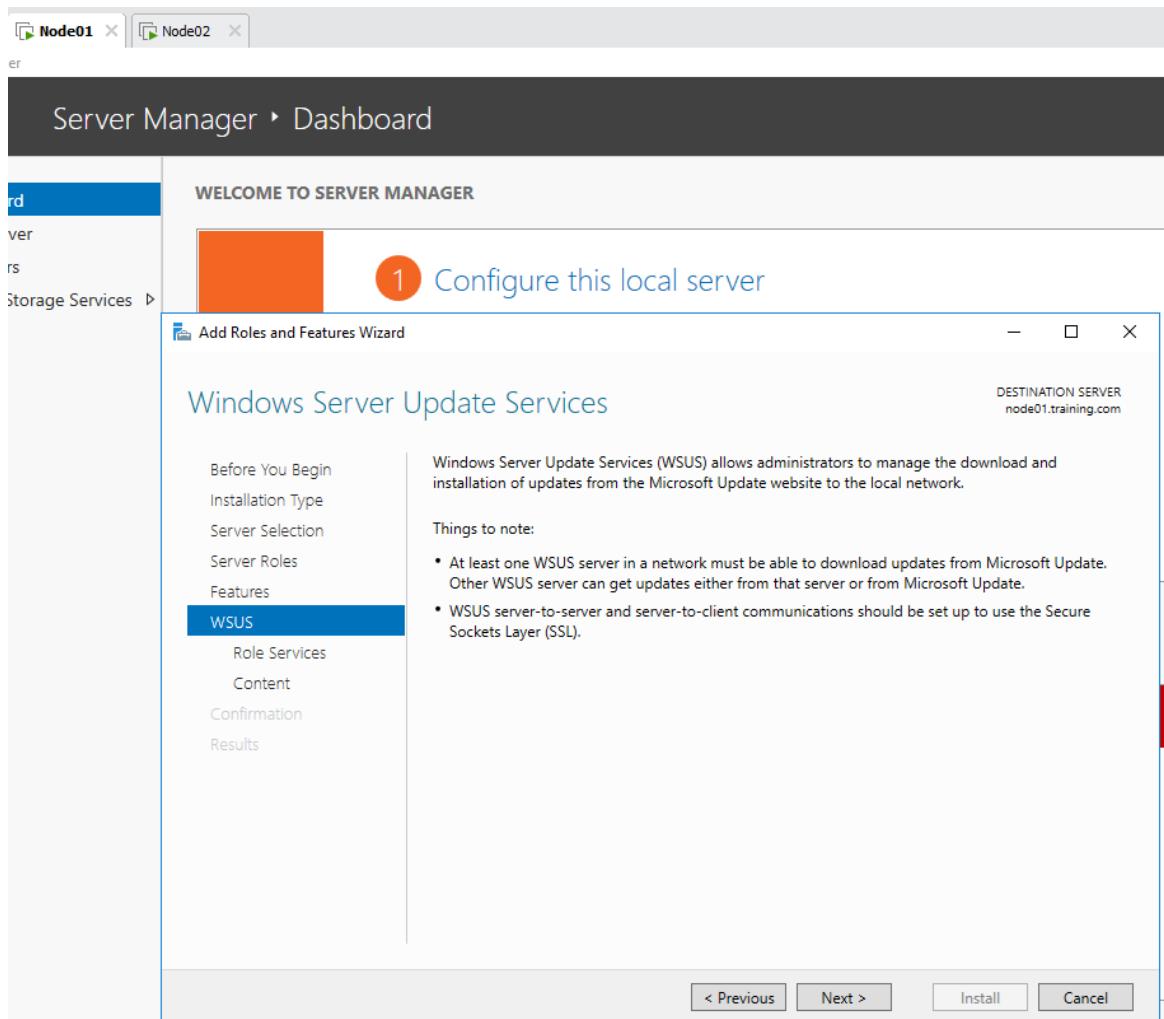
- Centralized management using Group Policy.
- Easier to:
 - Configure many clients at once.
 - Automate client grouping.
 - Enforce update compliance.
 - Ideal for enterprise or large network environments.

Steps to install WSUS on Node01:

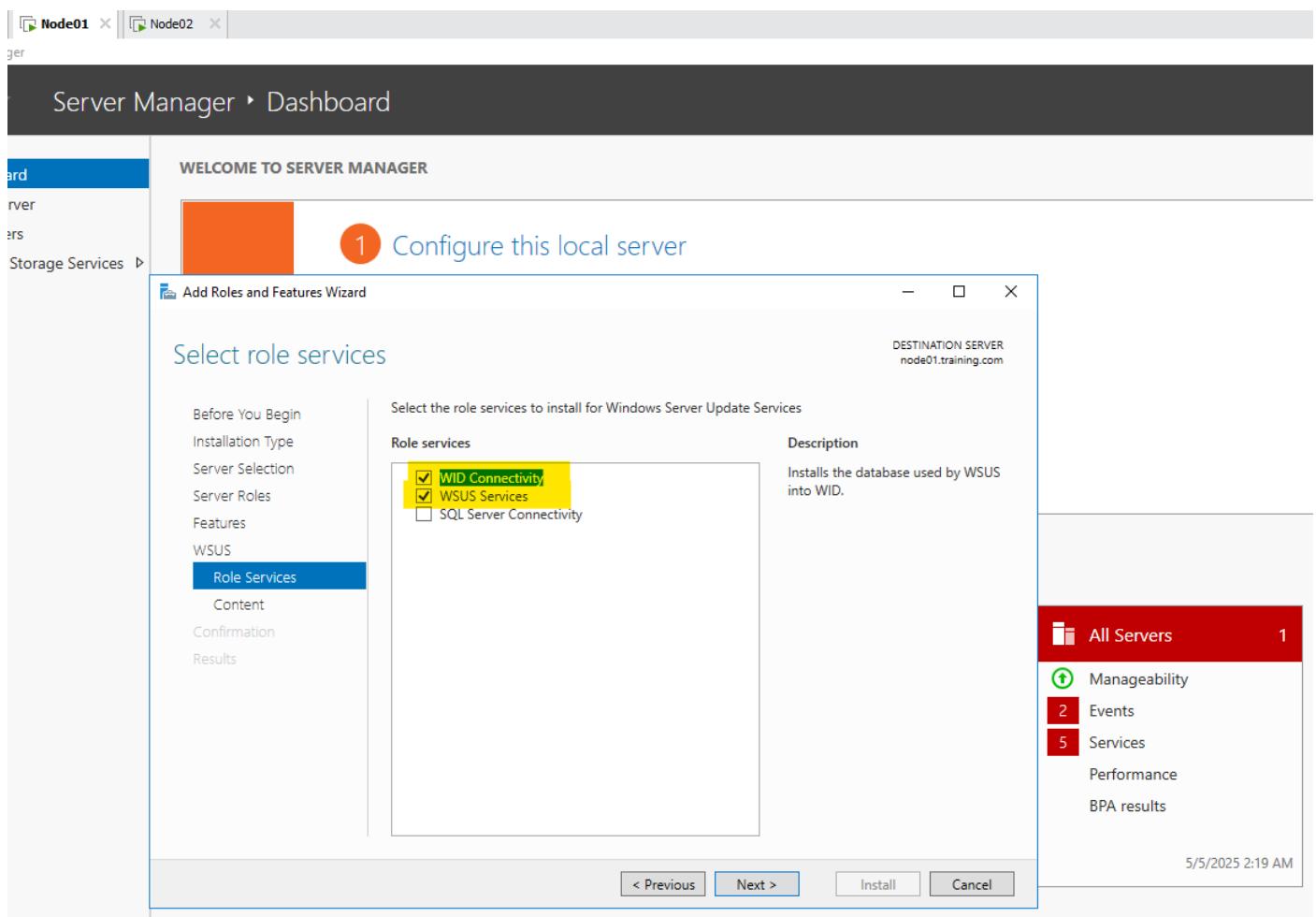
Server Manager → Manage → Add roles and features → Role (Windows Server Update Service)



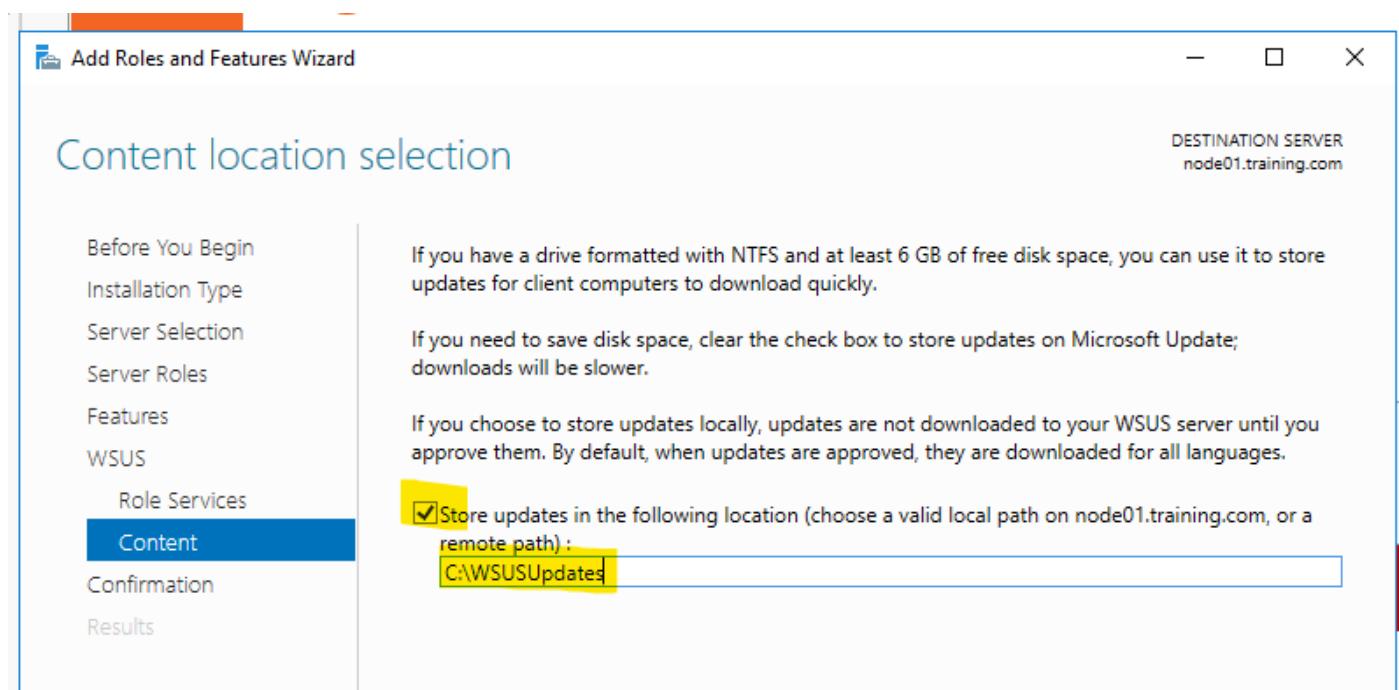
No features to be added:



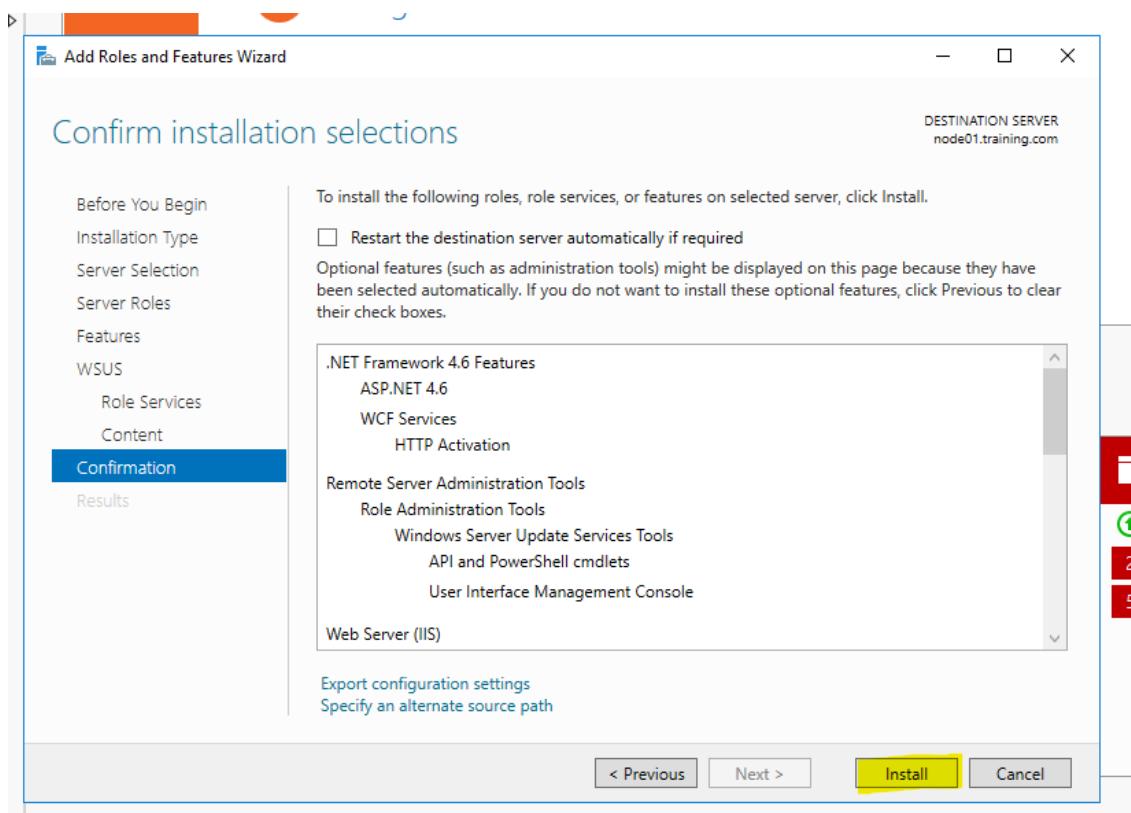
Select required role services:



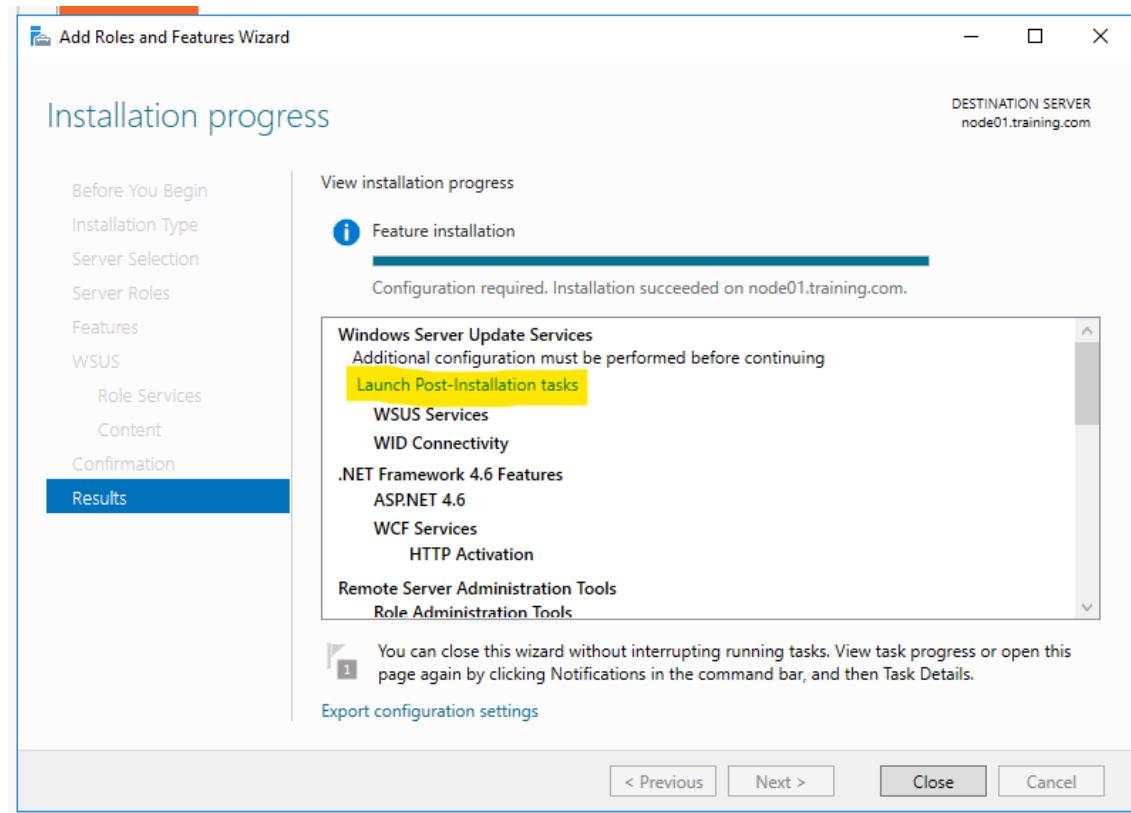
Adding path for storing updates (create new folder):



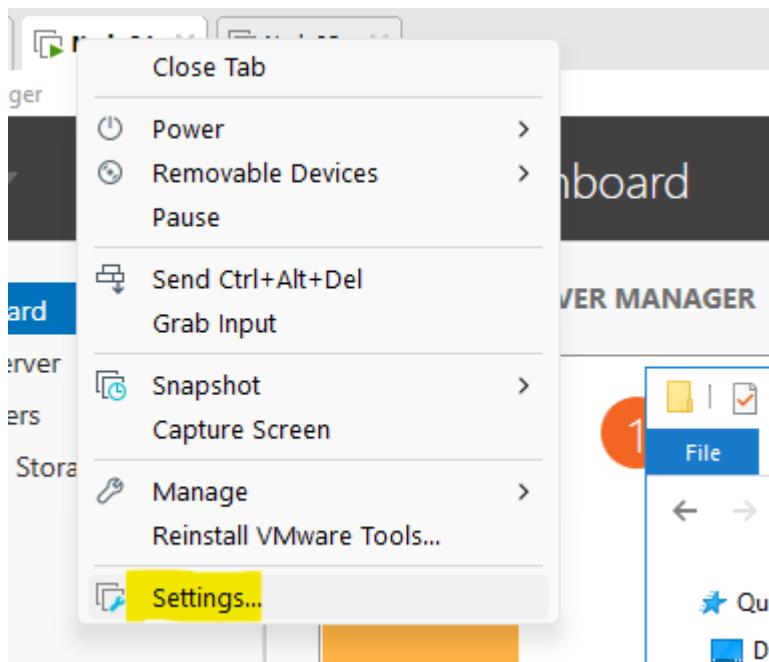
Install:



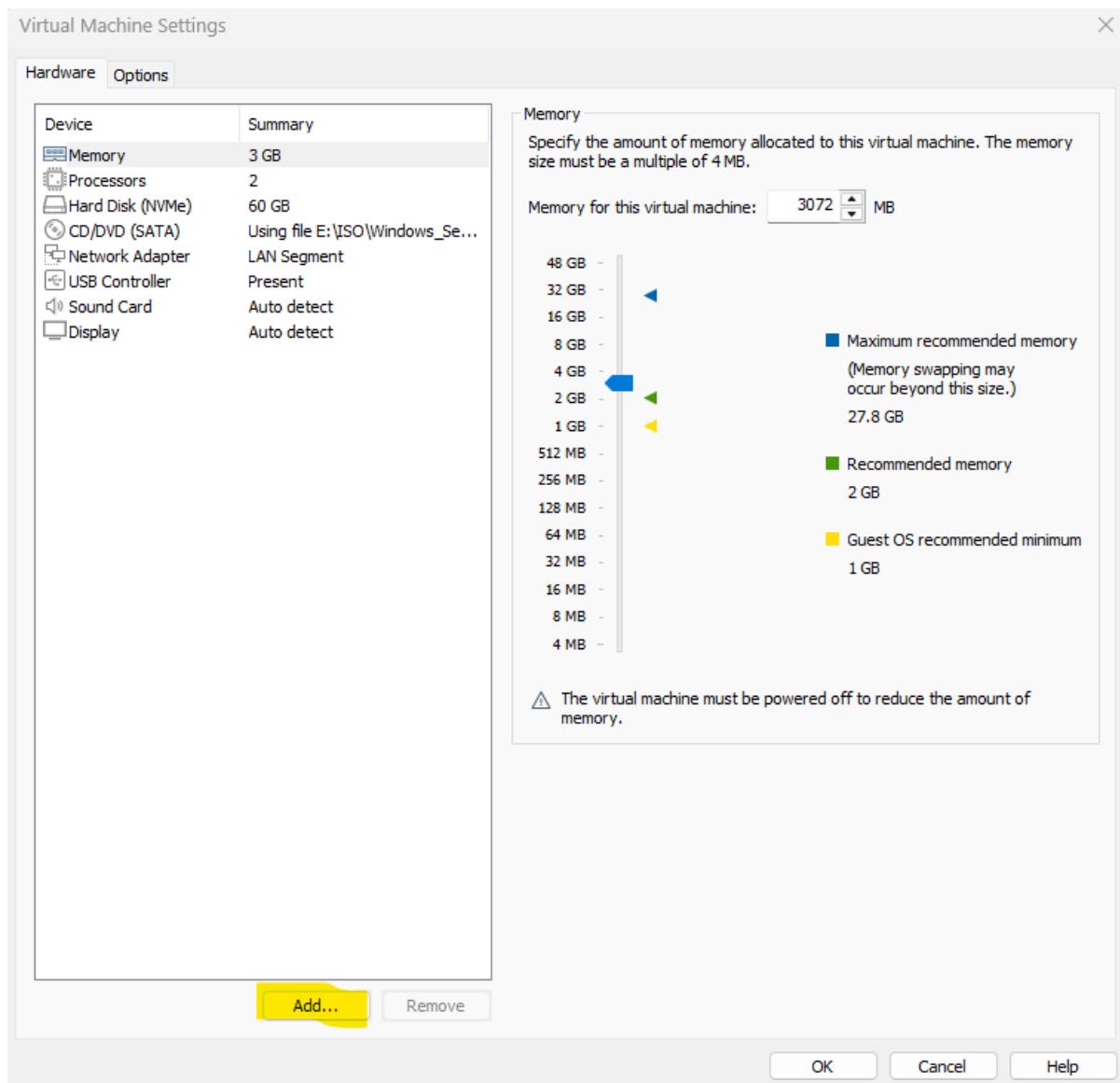
Click on "Launch Post-Installation tasks"



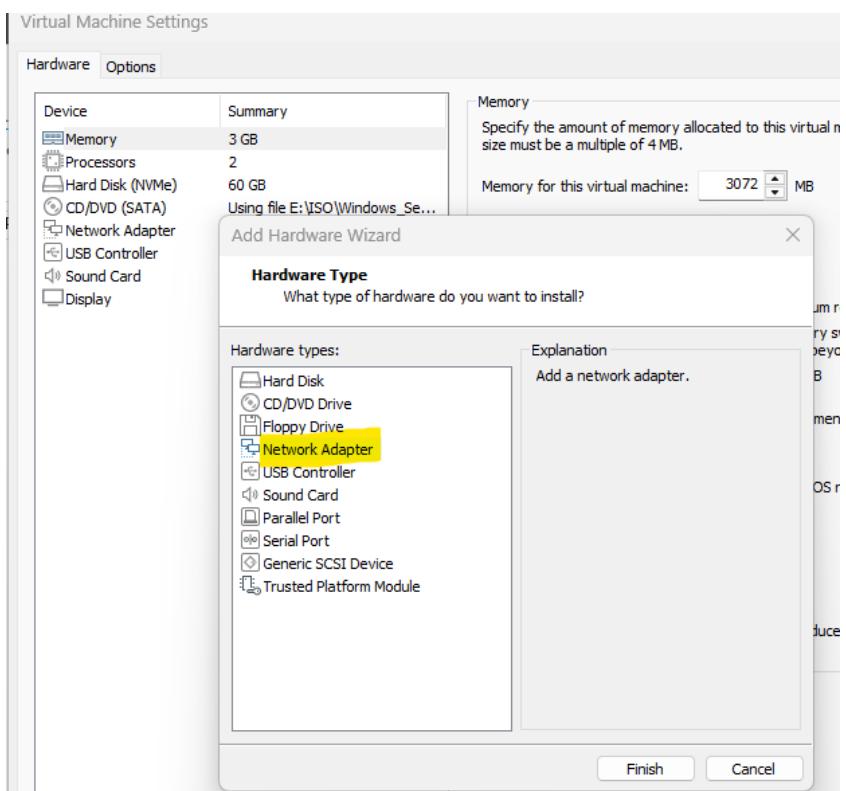
Add a new NIC card to node VM (Node01):



Click on "ADD":



Select “Network Adapter”:



Ensure that new network adapter is on NAT:

The screenshot shows the 'Server Manager' dashboard. In the center, there is a 'WELCOME TO SERVER MANAGER' panel with sections for 'QUICK START', 'WHAT'S NEW', and 'LEARN MORE'. On the left, there is a navigation menu with items like 'Storage Services'. A yellow circle with the number '1' is overlaid on the 'File' menu in the dashboard's top bar. To the right, there is a 'Virtual Machine Settings' dialog box. It shows a list of hardware components: Memory (3 GB), Processors (2), Hard Disk (NVMe) (60 GB), CD/DVD (SATA), Network Adapter, Network Adapter 2, USB Controller, Sound Card, and Display. 'Network Adapter 2' is highlighted with a yellow box. In the 'Device status' section, 'Connected' and 'Connect at power on' are checked. In the 'Network connection' section, 'NAT: Used to share the host's IP address' is selected. Other options include 'Bridged', 'Host-only', 'Custom', and 'LAN segment'. At the bottom right of the dialog is a 'LAN Command' button.

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

The screenshot shows a Windows Command Prompt window titled 'Administrator: C:\Windows\system32\cmd.exe'. The window displays the output of a 'ping google.com' command. The output shows four successful ping requests to the IP address 142.250.194.110, with round-trip times ranging from 48ms to 53ms and an average of 50ms. There is no loss of packets.

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

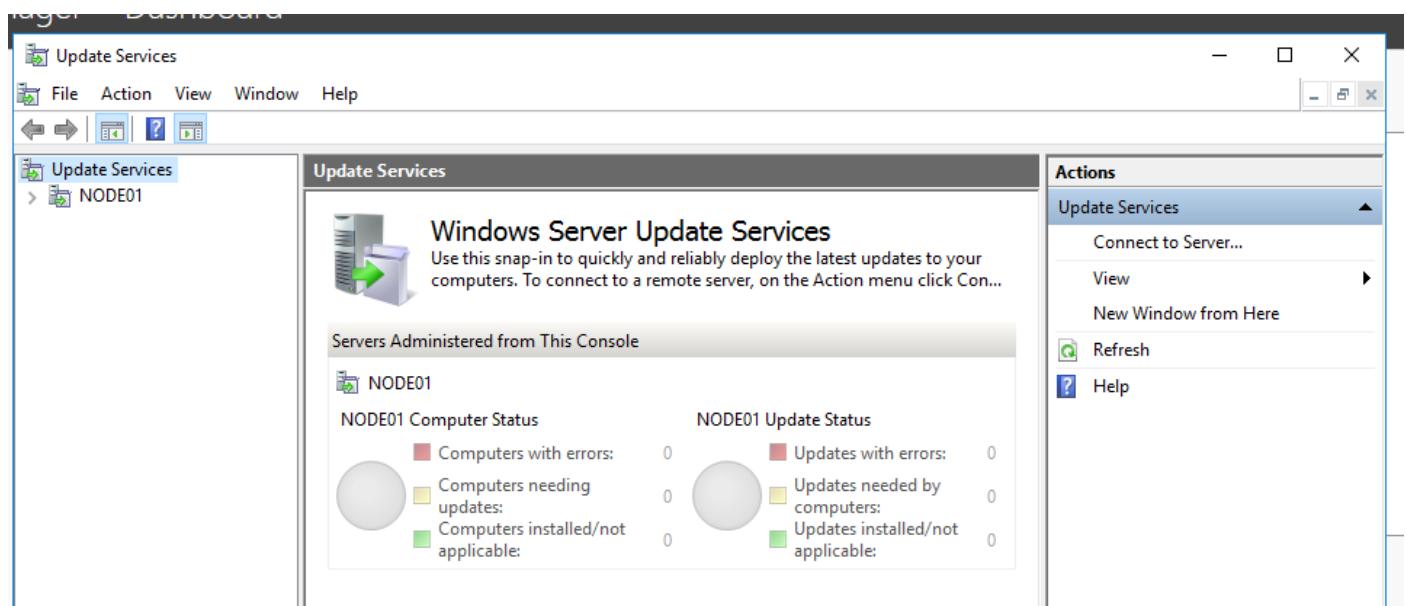
C:\Users\administrator.TRAINING>ping google.com

Pinging google.com [142.250.194.110] with 32 bytes of data:
Reply from 142.250.194.110: bytes=32 time=53ms TTL=128
Reply from 142.250.194.110: bytes=32 time=52ms TTL=128
Reply from 142.250.194.110: bytes=32 time=49ms TTL=128
Reply from 142.250.194.110: bytes=32 time=48ms TTL=128

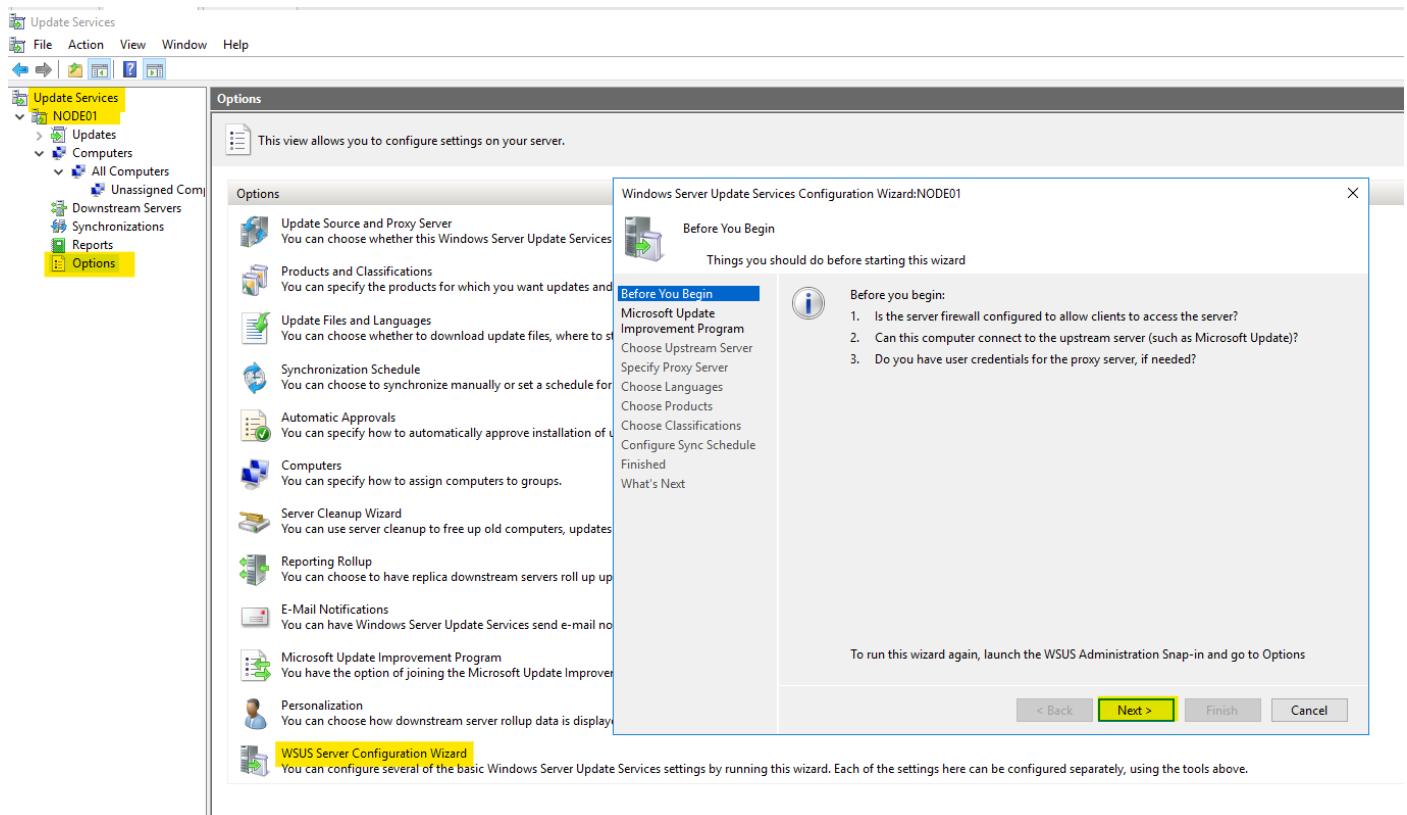
Ping statistics for 142.250.194.110:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 48ms, Maximum = 53ms, Average = 50ms
```

Configuring WSUS on Node01:

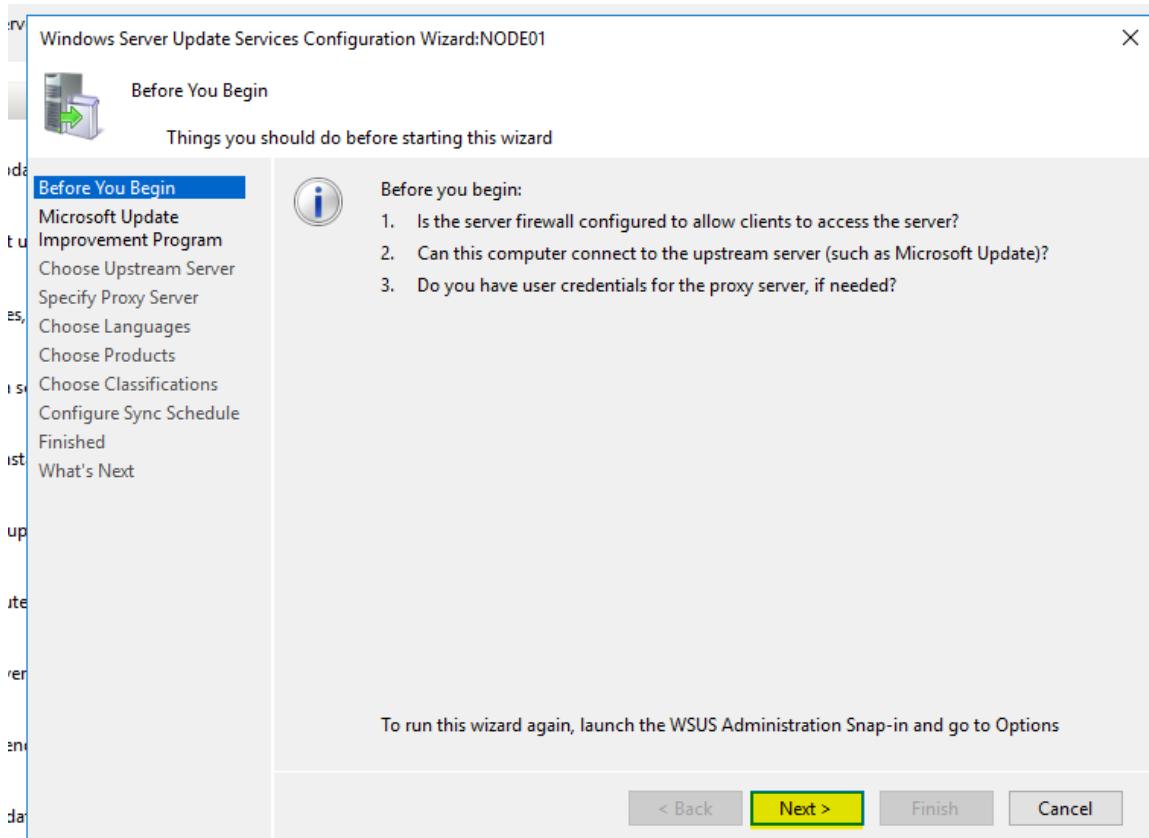
Server Manager Dashboard Page → Tools → Windows Server Update Service



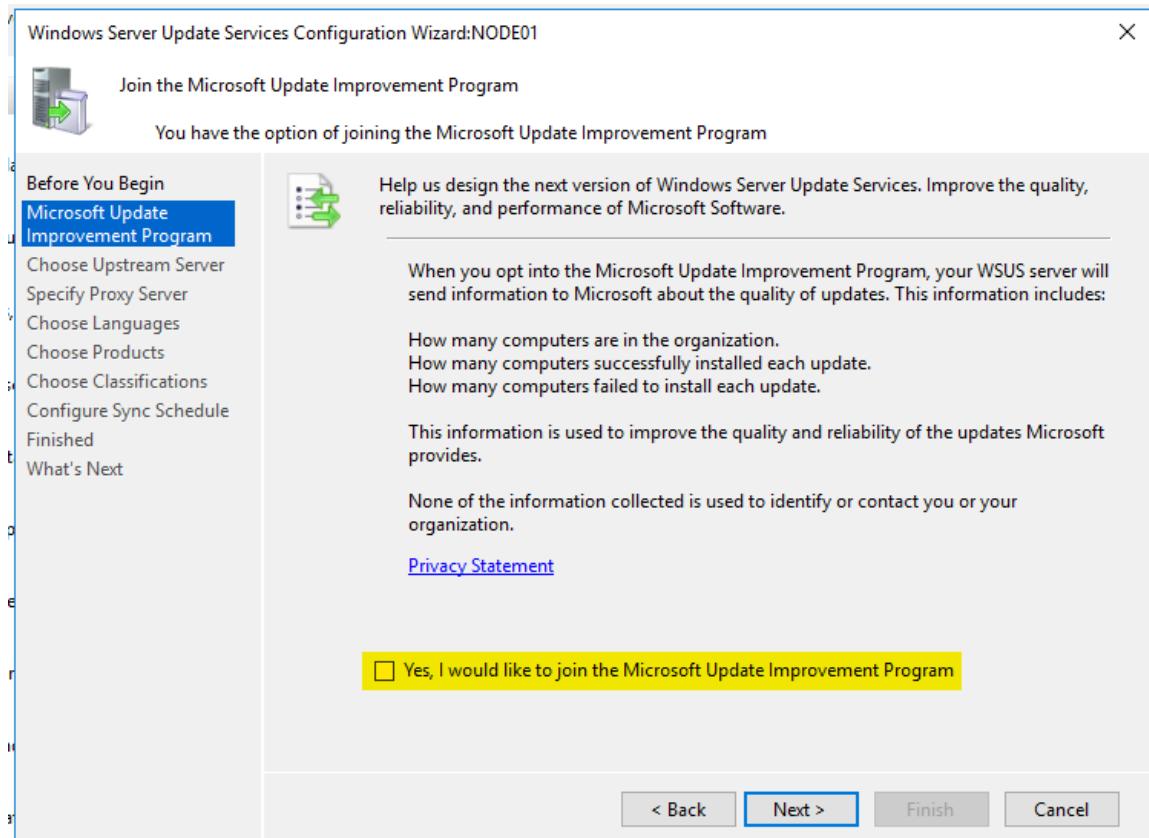
To configure WSUS configuration, Tools → Windows Server Update Service Console (select Options on left side):



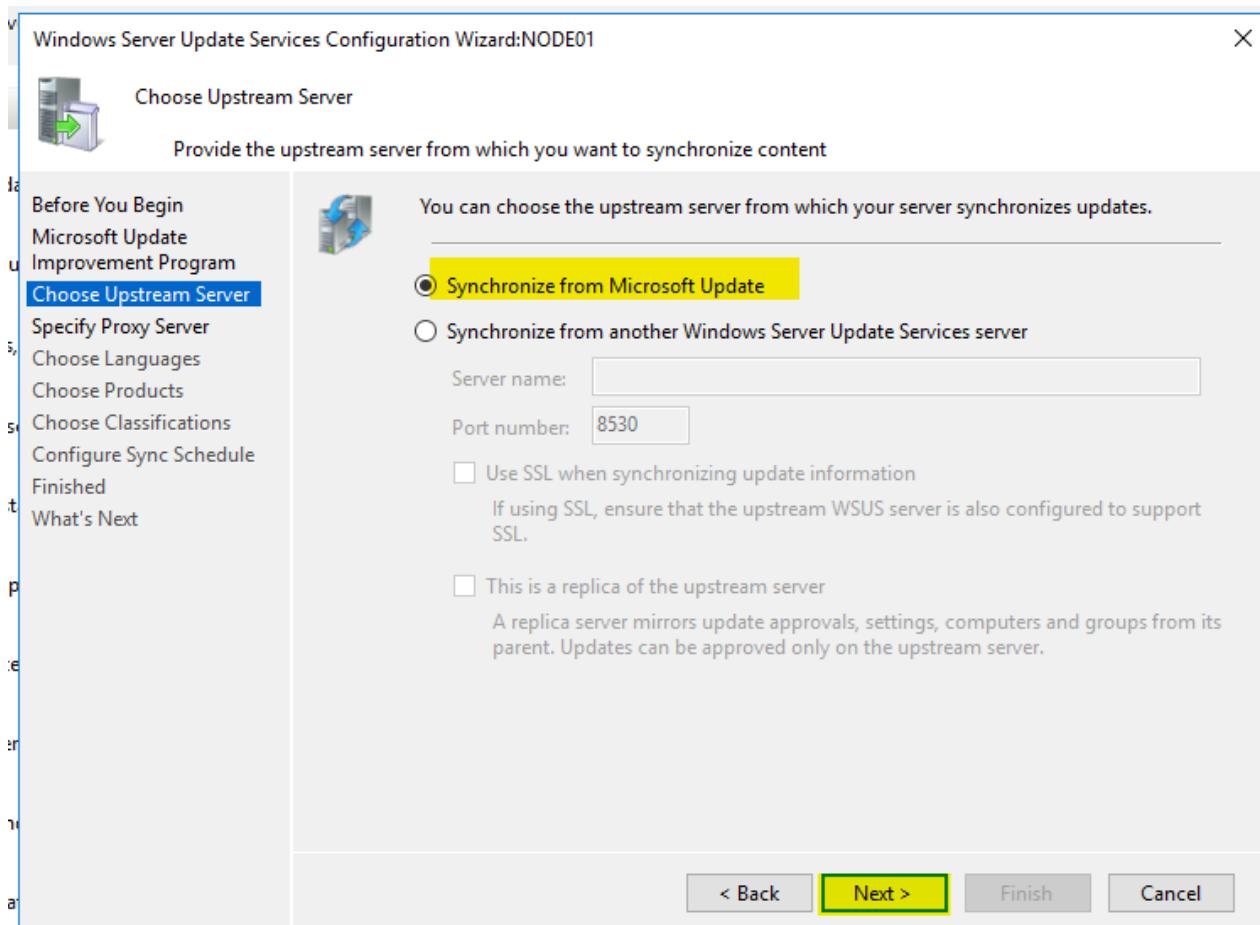
Click Next on “Before You Begin”:



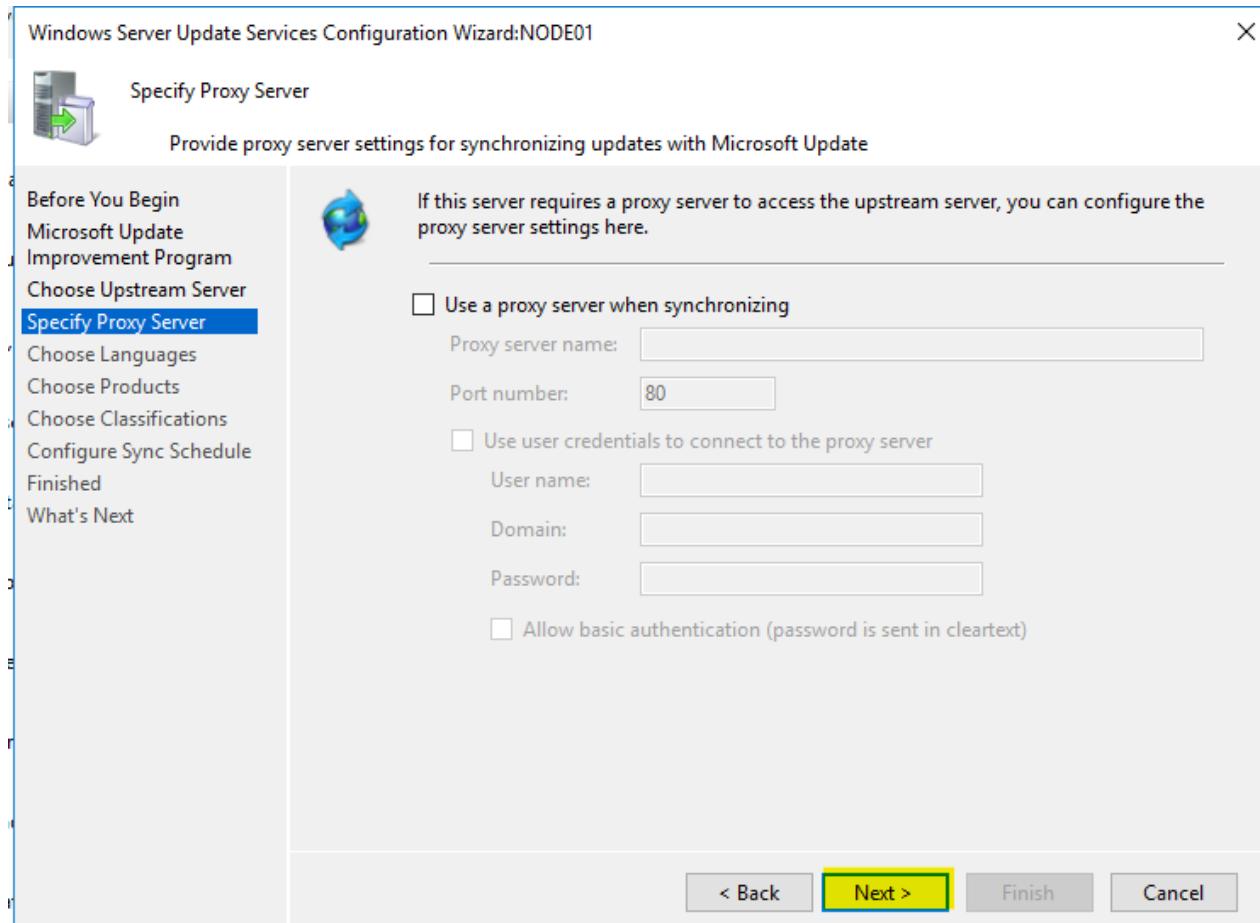
Untick “Yes, I would like to join Microsoft Update improvement program”



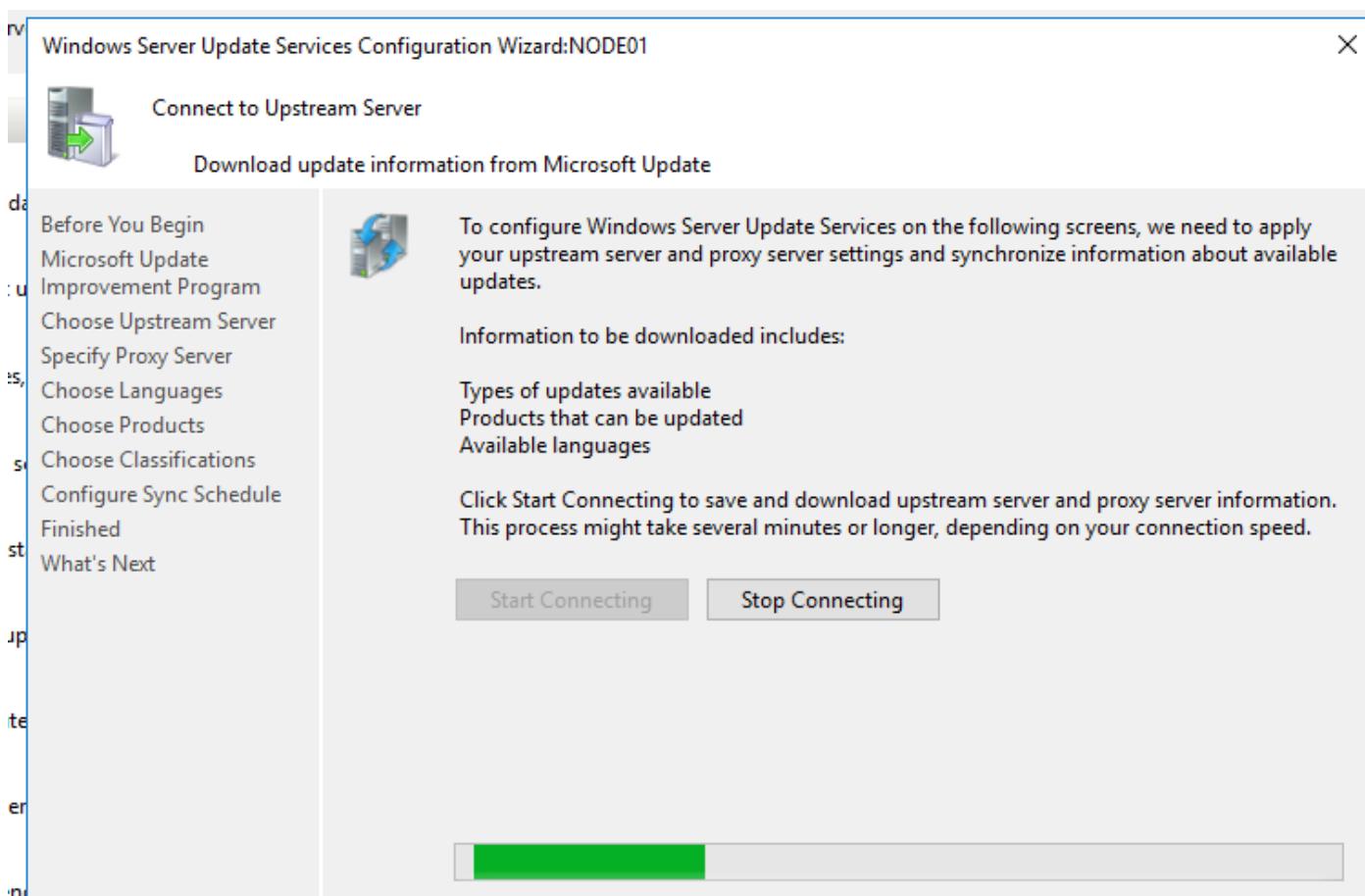
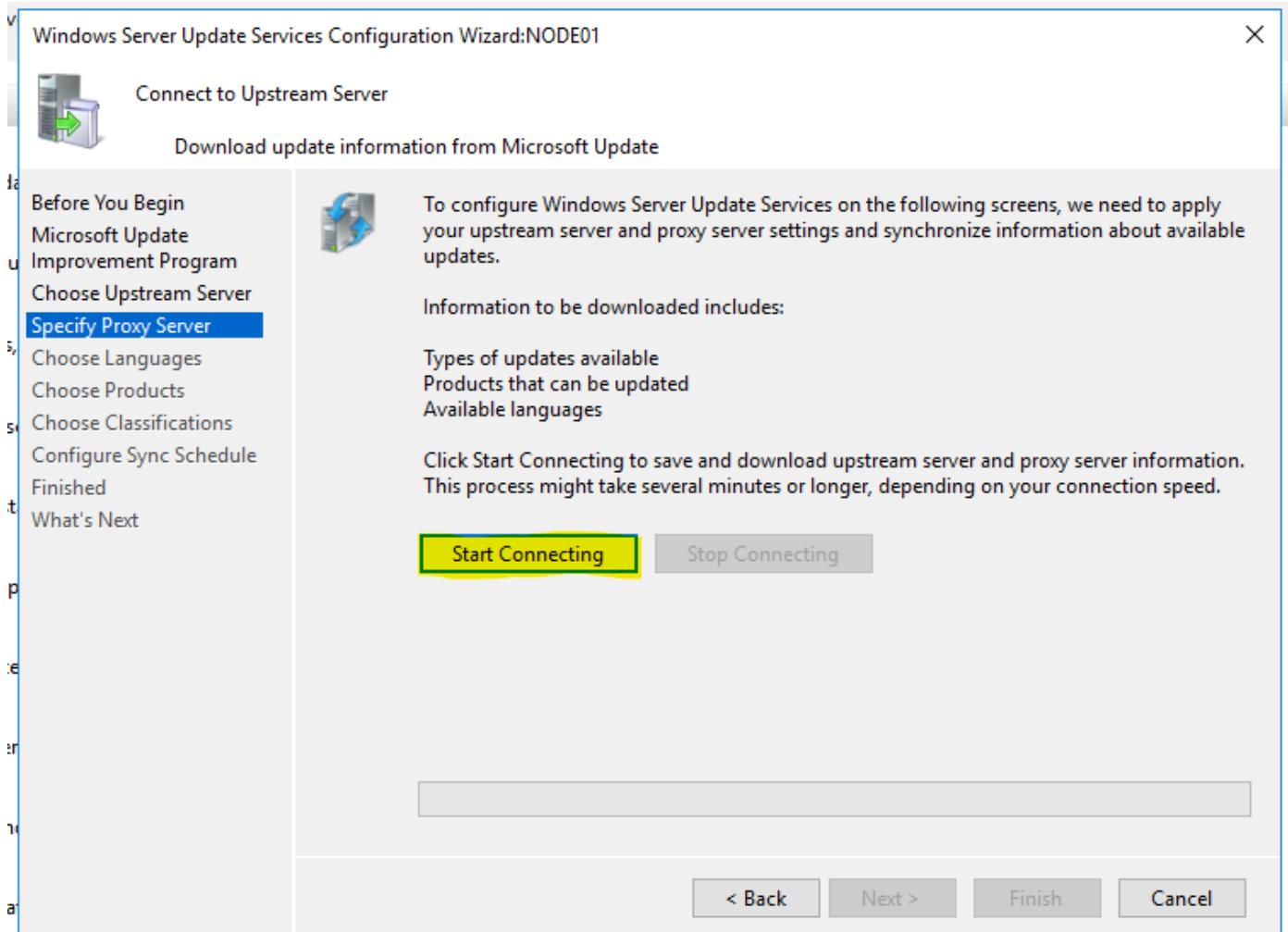
Select “Synchronize from Microsoft Update”, as we are connected to internet:



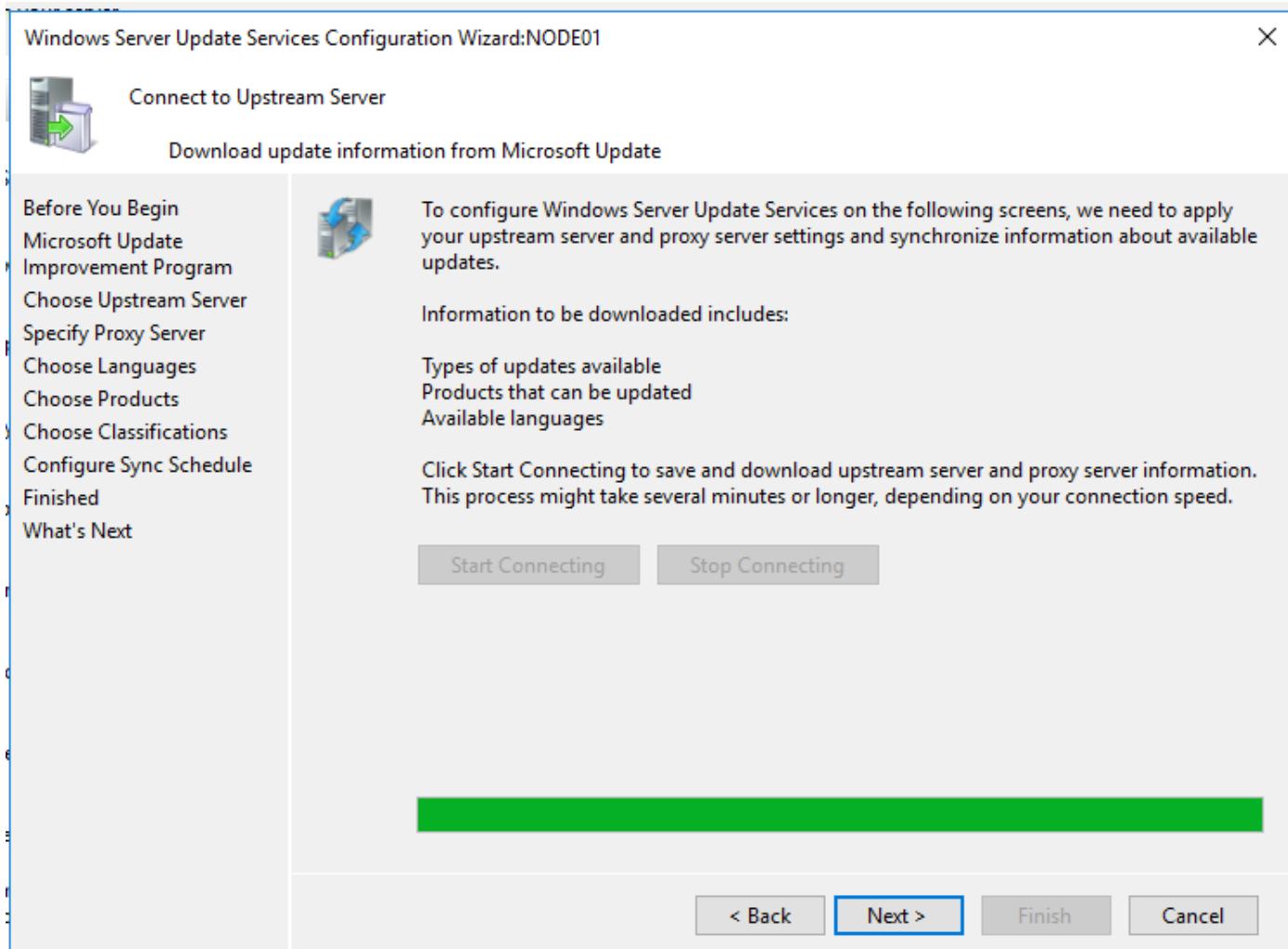
Leave the proxy server page and click Next:



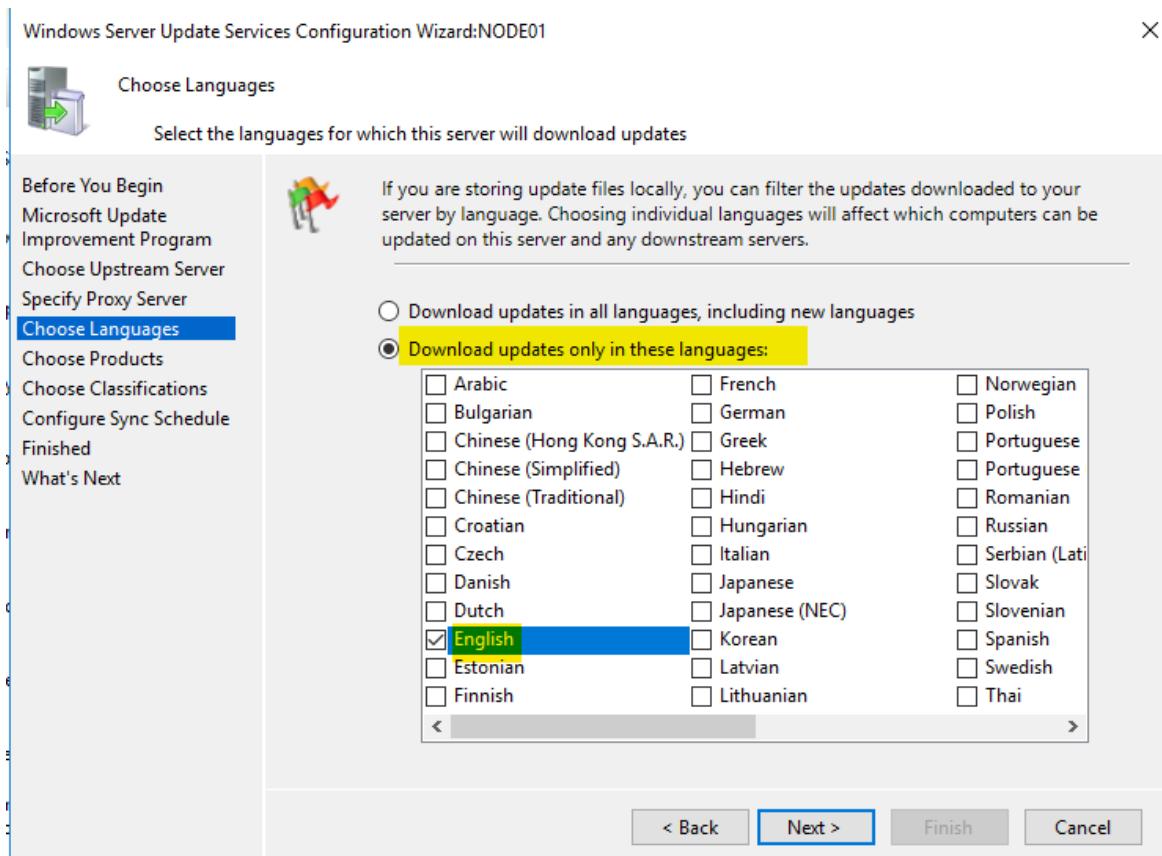
Click on "Start Connecting":



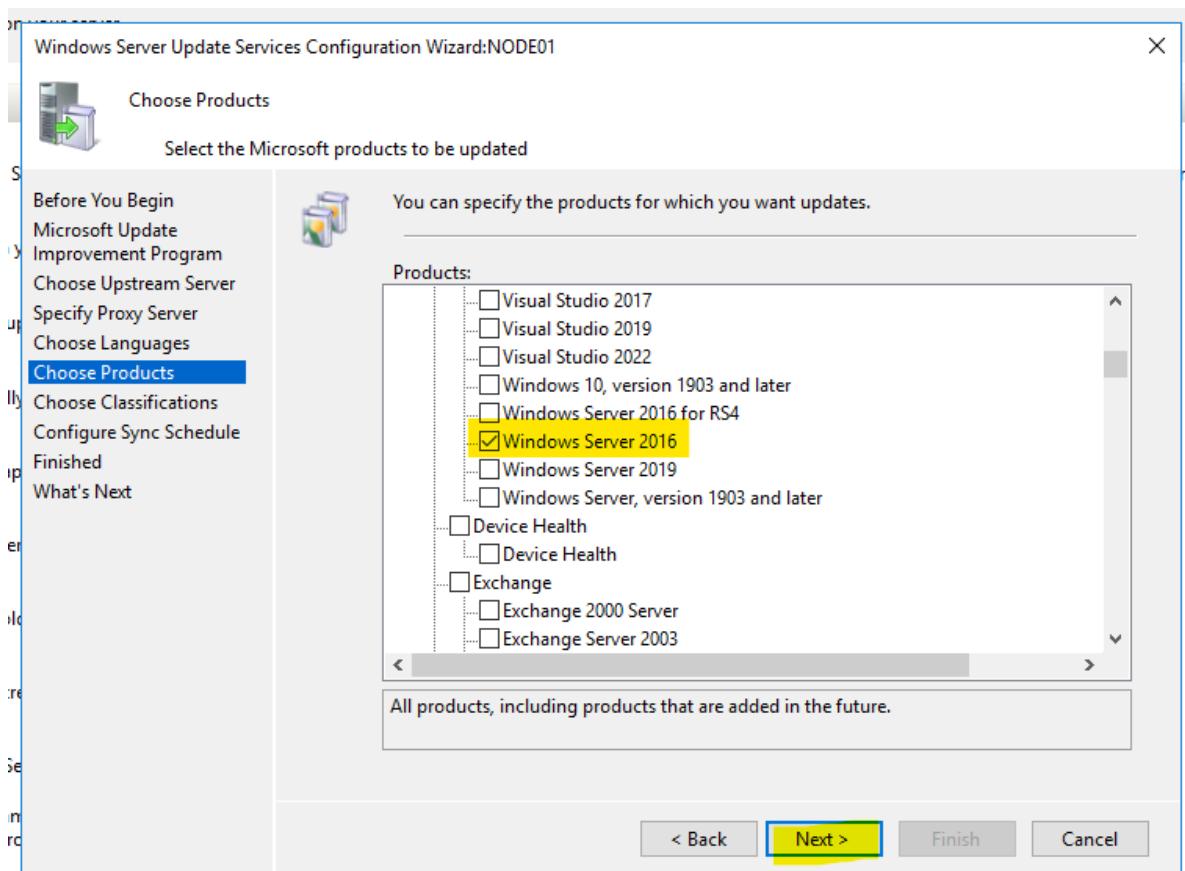
Approx. after 30mins the update was complete. Now click on Next:



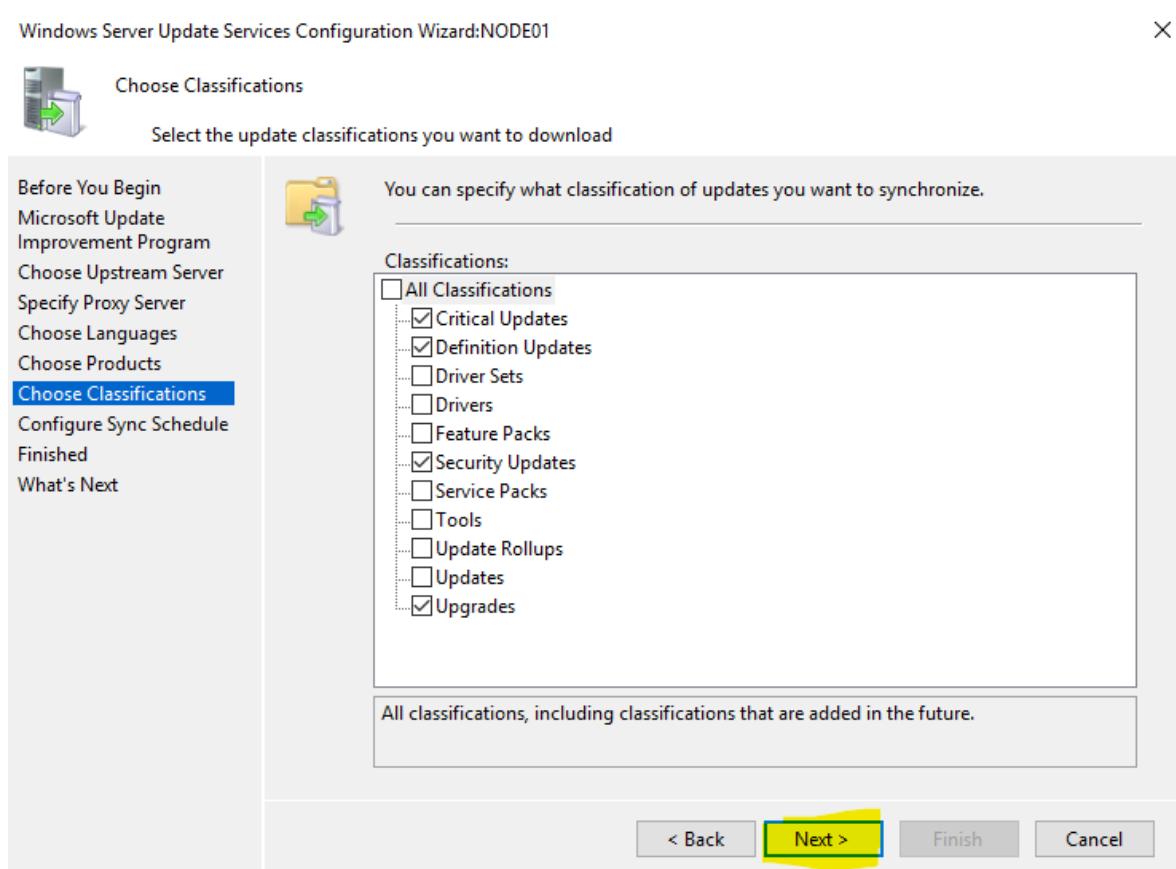
Select English language:



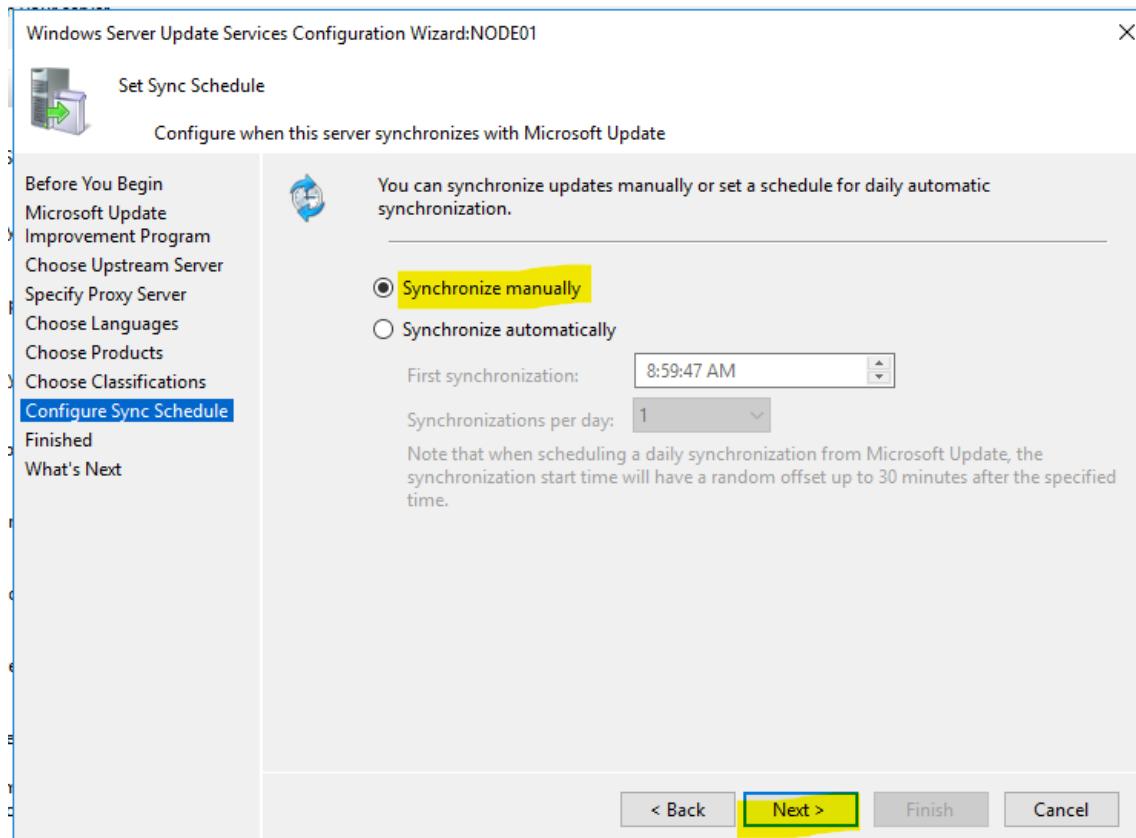
Select appropriate product (depending upon requirement):



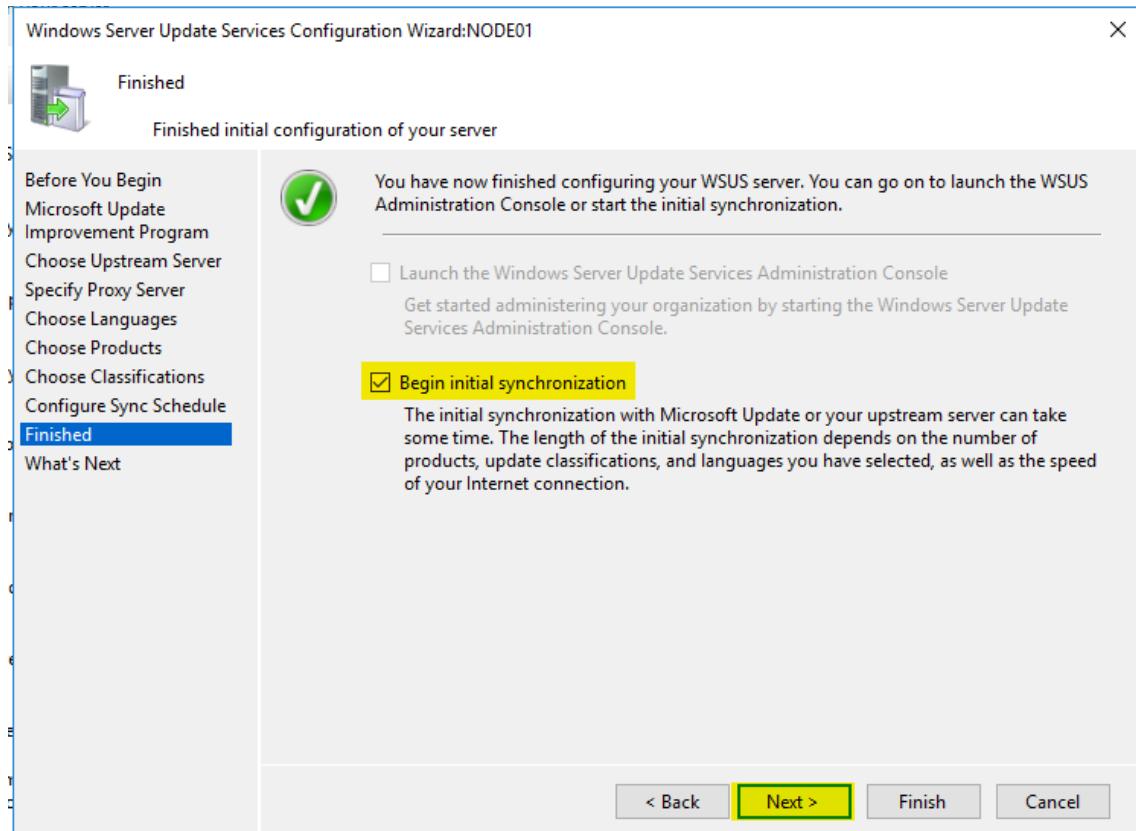
Select the required classification:



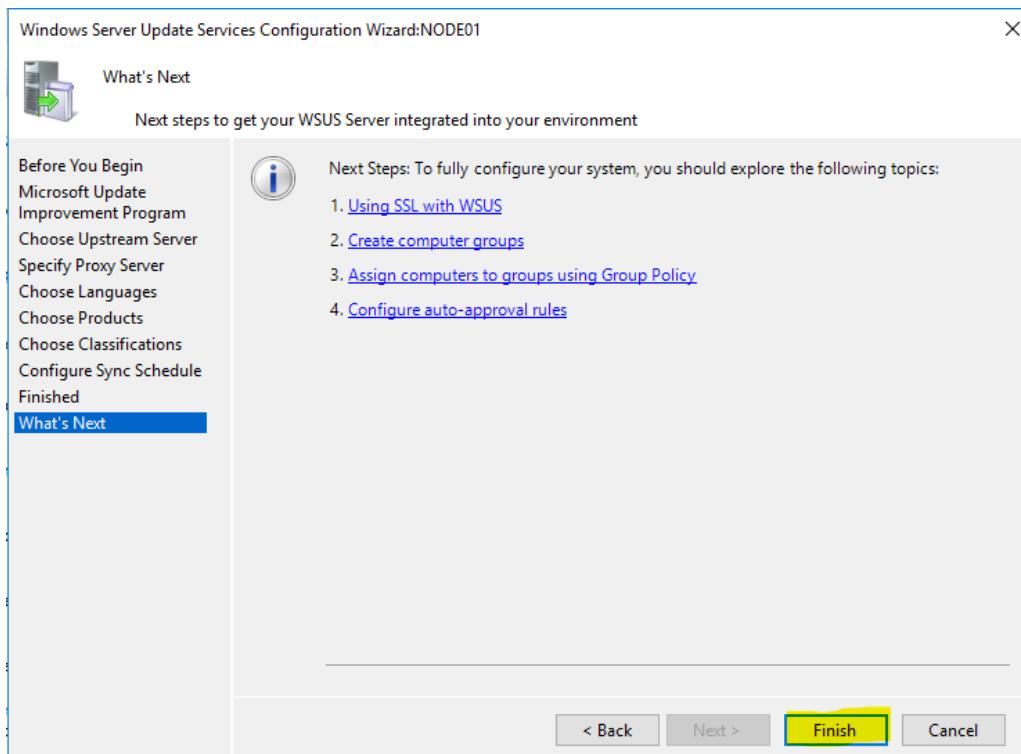
Select the sync time. We will select Manually as we will be using GPO for the updates:



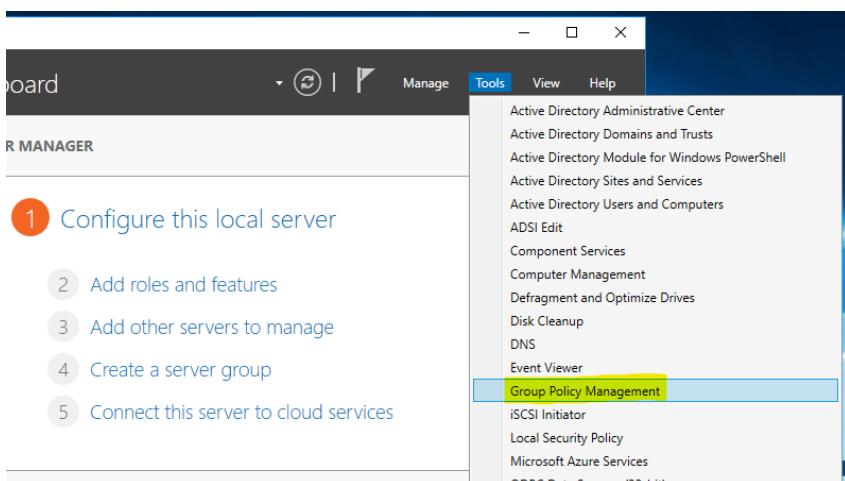
Check "Begin initial sync":



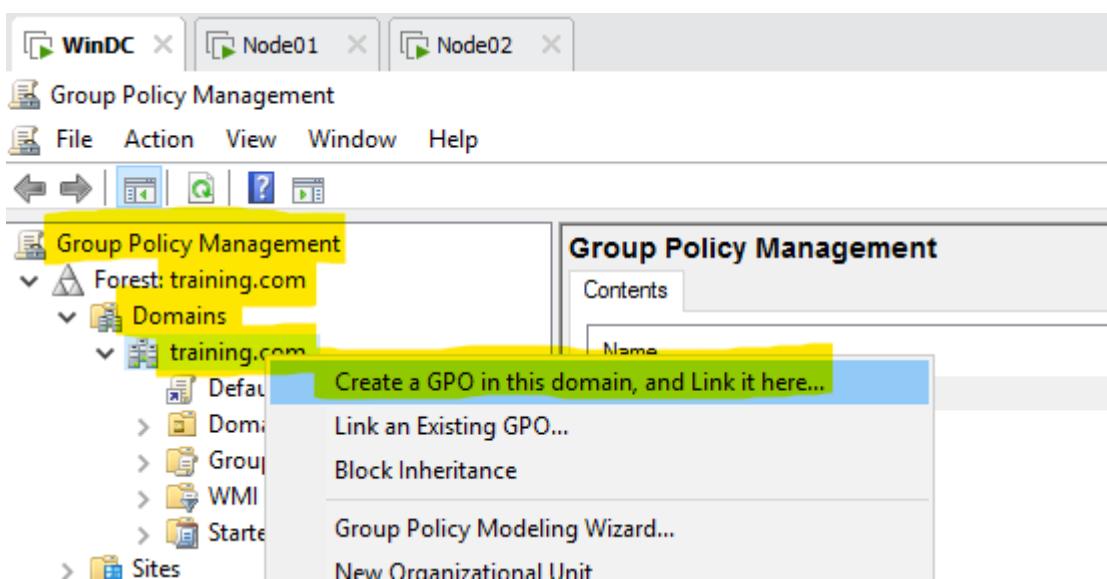
Finish the configuration:



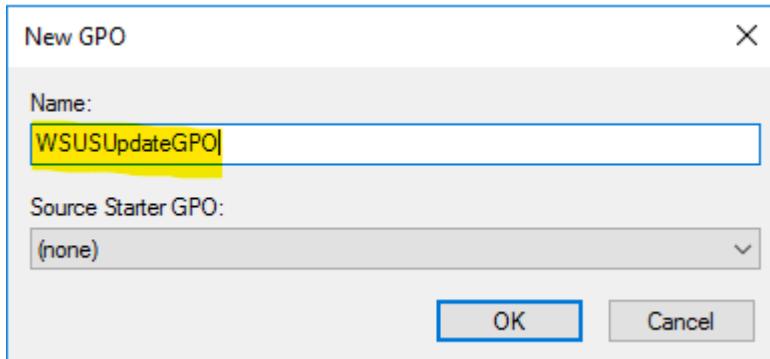
Configuring Group Policy for WSUS on DC machine:



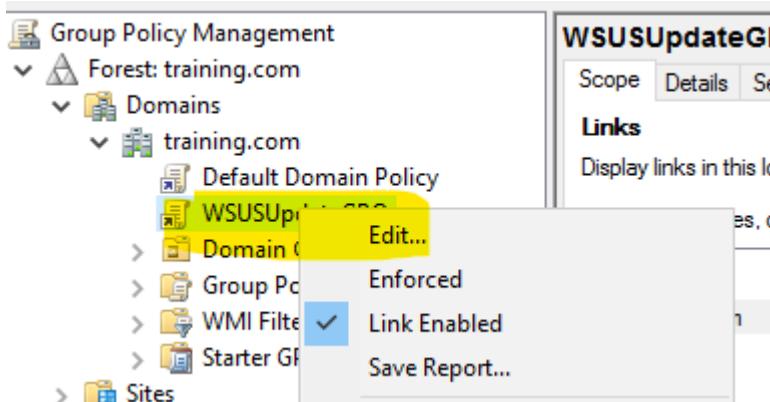
Create a new GPO:



Give any name to it.



Right click and edit it:



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

WinDC Node01 Node02

Group Policy Management Editor

File Action View Help

NetMeeting

OneDrive

Online Assistance

Portable Operating System

Presentation Settings

Remote Desktop Services

RSS Feeds

Search

Security Center

Shutdown Options

Smart Card

Software Protection Platform

Sound Recorder

Store

Sync your settings

Tablet PC

Task Scheduler

Windows Calendar

Windows Color System

Windows Customer Experience

Windows Defender

Windows Error Reporting

Windows Hello for Business

Windows Ink Workspace

Windows Installer

Windows Logon Options

Windows Mail

Windows Media Digital Rights M

Windows Media Player

Windows Messenger

Windows Mobility Center

Windows PowerShell

Windows Reliability Analysis

Windows Remote Management

Windows Remote Shell

Windows Update

All Settings

Configure Automatic Updates

Requirements: Windows XP Professional Service Pack 1 or at least Windows 2000 Service Pack 3

Description: Specifies whether this computer will receive security updates and other important downloads through the Windows automatic updating service.

Note: This policy does not apply to Windows RT.

This setting lets you specify whether automatic updates are enabled on this computer. If the service is enabled, you must select one of the four options in the Group Policy Setting:

2 = Notify before downloading and installing any updates.

When Windows finds updates that apply to this computer, users will be notified that updates are ready to be downloaded. After going to Windows Update, users can download and install any available updates.

3 = (Default setting) Download the updates automatically and notify when they are ready to be installed

Setting	State	Comment
Defer Windows Updates	Not configured	No
Allow Automatic Updates immediate installation	Not configured	No
Allow non-administrators to receive update notifications	Not configured	No
Allow signed updates from an intranet Microsoft update serv...	Not configured	No
Always automatically restart at the scheduled time	Not configured	No
Automatic Updates detection frequency	Not configured	No
Configure Automatic Updates	Not configured	No
Delay Restart for scheduled installations	Not configured	No
Do not adjust default option to 'Install Updates and Shut Do...	Not configured	No
Do not connect to any Windows Update Internet locations	Not configured	No
Do not display 'Install Updates and Shut Down' option in Sh...	Not configured	No
Do not include drivers with Windows Updates	Not configured	No
Enable client-side targeting	Not configured	No
Enabling Windows Update Power Management to automati...	Not configured	No
No auto-restart with logged on users for scheduled automat...	Not configured	No
Remove access to use all Windows Update features	Not configured	No
Re-prompt for restart with scheduled installations	Not configured	No
Reschedule Automatic Updates scheduled installations	Not configured	No
Specify deadline before auto-restart for update installat...	Not configured	No
Specify intranet Microsoft update service location	Not configured	No
Turn off auto-restart for updates during active hours	Not configured	No
Turn on recommended updates via Automatic Updates	Not configured	No
Turn on Software Notifications	Not configured	No

Double-click on the policy & fill details:

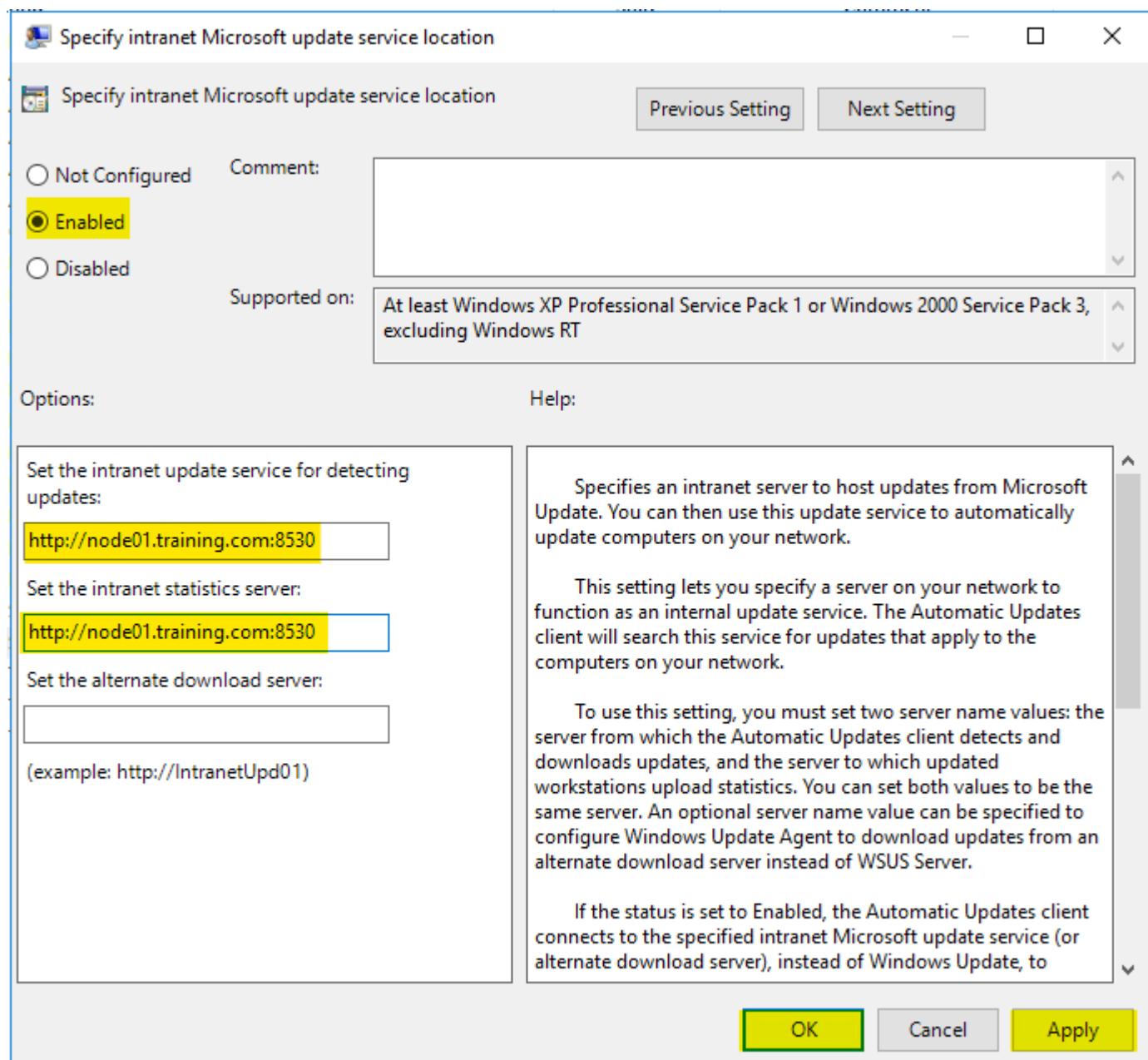
The screenshot shows the Windows Update GPO configuration interface. On the left, a navigation pane lists various settings like NetMeeting, OneDrive, and Windows Update. The 'Windows Update' folder is selected. In the main pane, the 'Configure Automatic Updates' policy is being edited. The 'Setting' tab is selected, showing the 'Defer Windows Updates' section. A dialog box titled 'Configure Automatic Updates' is open, displaying options for automatic updates. The 'Enabled' radio button is selected. Under 'Configure automatic updating:', the dropdown is set to '3 - Auto download and notify for install'. Other options include 'Install during automatic maintenance' (unchecked), 'Scheduled install day' (set to '7 - Every Saturday'), and 'Scheduled install time' (set to '17:00'). A note states: 'When Windows finds updates that apply to this computer, users will be notified that updates are ready to be downloaded. After going to Windows Update, users can download and install any available updates.' Below this, it says: '3 = (Default setting) Download the updates automatically and notify when they are ready to be installed'. A note also mentions: 'Windows finds updates that apply to the computer and'. At the bottom of the dialog are 'OK', 'Cancel', and 'Apply' buttons.

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

The screenshot shows the Windows Update GPO configuration interface. The 'Specify intranet Microsoft update service location' policy is being edited. The 'Setting' tab is selected, showing the 'Defer Windows Updates' section. A table lists various settings with their current state and comment status. The 'Specify intranet Microsoft update service location' row is highlighted with a blue background. Other rows include: 'Allow Automatic Updates immediate installation' (Not configured, No), 'Allow non-administrators to receive update notifications' (Not configured, No), 'Allow signed updates from an intranet Microsoft update service...' (Not configured, No), 'Always automatically restart at the scheduled time' (Not configured, No), 'Automatic Updates detection frequency' (Not configured, No), 'Configure Automatic Updates' (Enabled, No), 'Delay Restart for scheduled installations' (Not configured, No), 'Do not adjust default option to 'Install Updates and Shut Do...' (Not configured, No), 'Do not connect to any Windows Update Internet locations' (Not configured, No), 'Do not display 'Install Updates and Shut Down' option in Sh...' (Not configured, No), 'Do not include drivers with Windows Updates' (Not configured, No), 'Enable client-side targeting' (Not configured, No), 'Enabling Windows Update Power Management to automati...' (Not configured, No), 'No auto-restart with logged on users for scheduled automat...' (Not configured, No), 'Remove access to use all Windows Update features' (Not configured, No), 'Re-prompt for restart with scheduled installations' (Not configured, No), 'Reschedule Automatic Updates scheduled installations' (Not configured, No), 'Specify deadline before auto-restart for update installation' (Not configured, No), 'Turn off auto-restart for updates during active hours' (Not configured, No), 'Turn on recommended updates via Automatic Updates' (Not configured, No), and 'Turn on Software Notifications' (Not configured, No). At the bottom of the table are 'OK', 'Cancel', and 'Apply' buttons.

Setting	State	Comment
Allow Automatic Updates immediate installation	Not configured	No
Allow non-administrators to receive update notifications	Not configured	No
Allow signed updates from an intranet Microsoft update service...	Not configured	No
Always automatically restart at the scheduled time	Not configured	No
Automatic Updates detection frequency	Not configured	No
Configure Automatic Updates	Enabled	No
Delay Restart for scheduled installations	Not configured	No
Do not adjust default option to 'Install Updates and Shut Do...	Not configured	No
Do not connect to any Windows Update Internet locations	Not configured	No
Do not display 'Install Updates and Shut Down' option in Sh...	Not configured	No
Do not include drivers with Windows Updates	Not configured	No
Enable client-side targeting	Not configured	No
Enabling Windows Update Power Management to automati...	Not configured	No
No auto-restart with logged on users for scheduled automat...	Not configured	No
Remove access to use all Windows Update features	Not configured	No
Re-prompt for restart with scheduled installations	Not configured	No
Reschedule Automatic Updates scheduled installations	Not configured	No
Specify deadline before auto-restart for update installation	Not configured	No
Specify intranet Microsoft update service location	Not configured	No
Turn off auto-restart for updates during active hours	Not configured	No
Turn on recommended updates via Automatic Updates	Not configured	No
Turn on Software Notifications	Not configured	No

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



Now on clients, update the group policy:

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

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

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

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

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

```
C:\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.

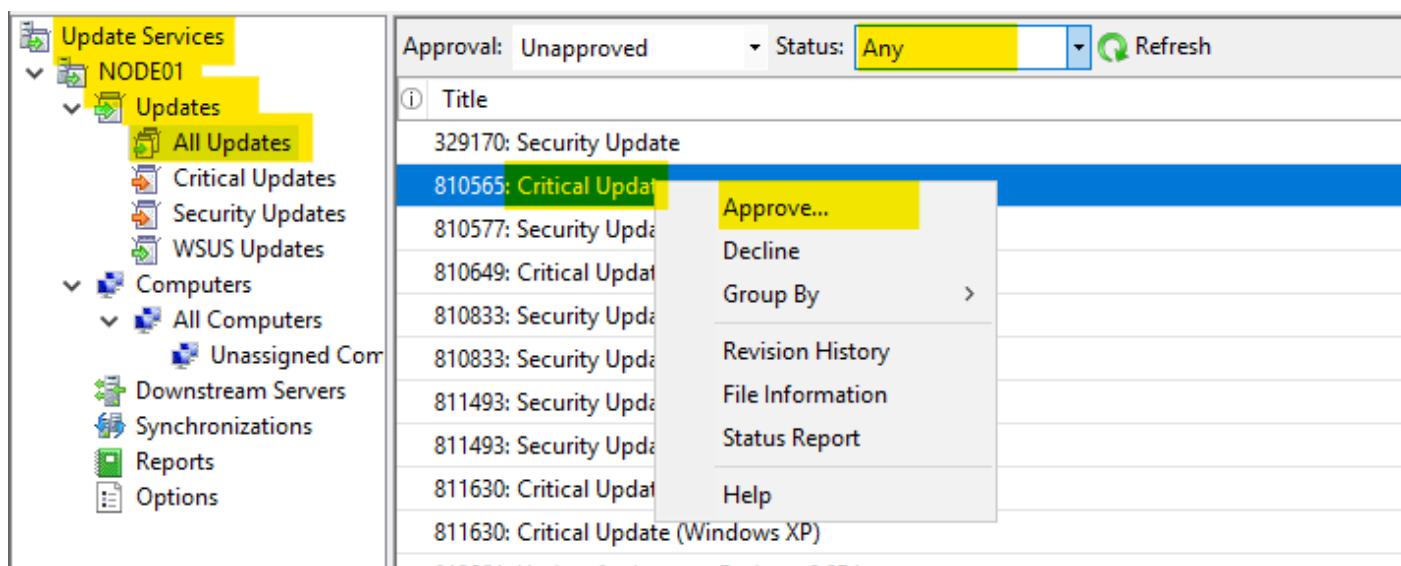
Created on 5/5/2025 at 4:57:06 AM

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:

The screenshot shows the Windows Update Services interface. On the left, a navigation tree includes 'Update Services', 'NODE01', 'Updates' (selected), 'All Updates', 'Critical Updates', 'Security Updates', and 'WSUS Updates'. Under 'Updates', there are 'Computers' (selected) and 'All Computers'. Other sections include 'Downstream Servers', 'Synchronizations', 'Reports', and 'Options'. The main pane displays a list of updates with columns for 'Title', 'Classification', 'Installed/Not Ap...', and 'Approval'. The 'Approval' column shows '0% Not approved' for most entries. A context menu is open over the list, with 'Approve...' highlighted in yellow. Other options in the menu include 'Decline', 'Group By', 'Status Report', and 'Help'. The status bar at the bottom indicates 'Windows Update Services - 1 item(s) found'.

Title	Classification	Installed/Not Ap...	Approval
329170: Security Update	Security Updates	0%	Not approved
810565: Critical Update	Critical Updates	0%	Not approved
810577: Security Update	Security Updates	0%	Not approved
810649: Critical Update	Critical Updates	0%	Not approved
810833: Security Update (Windows 2000)	Security Updates	0%	Not approved
810833: Security Update (Windows XP)	Security Updates	0%	Not approved
811493: Security Update (Windows 2000)	Security Updates	0%	Not approved
811493: Security Update (Windows XP)	Security Updates	0%	Not approved
811630: Critical Update (Windows 2000)	Critical Updates	0%	Not approved
811630: Critical Update (Windows XP)	Critical Updates	0%	Not approved
813951: Update for Internet Explorer 6 SP1	Critical Updates	0%	Not approved
814033: Critical Update	Critical Updates	0%	Not approved
814033: Critical Update	Critical Updates	0%	Not approved
814078: Security Update (Microsoft Jscript version 5.1, Windows 2000)	Security Updates	0%	Not approved
814078: Security Update (Microsoft Jscript version 5.5, Windows 2000)	Security Updates	0%	Not approved

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)

