MCSA Complete Labs

Version 22.05

Ahmed Abdelwahed
ahmed@abdelwahed.me
www.abdelwahed.me
LinkedIn

Contents

Active Directory

Primary Active Directory

Lab Objective

Active Directory Domain Services (AD DS) serves as the central database for storing data on all objects within your Active Directory Forest and processes authentication requests.

This lab explains the process to add and install active directory domain services on windows server 2016.

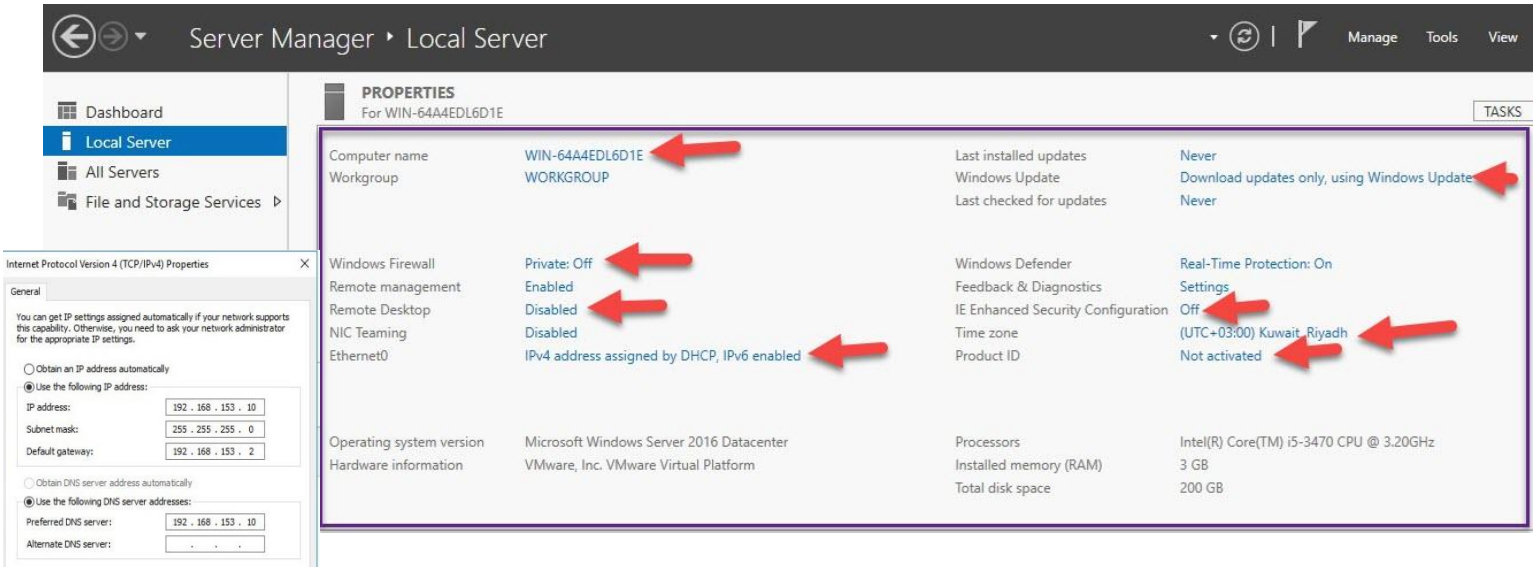
- Server Name: DC01
- IP Address: 192.168.153.10
- DNS: 192.168.153.10
- Domain Name: ITPROLABS.XYZ

Initial Configuration

Before you start active directory installation on windows server 2016, there are some changes its recommended to configure on server including the following:

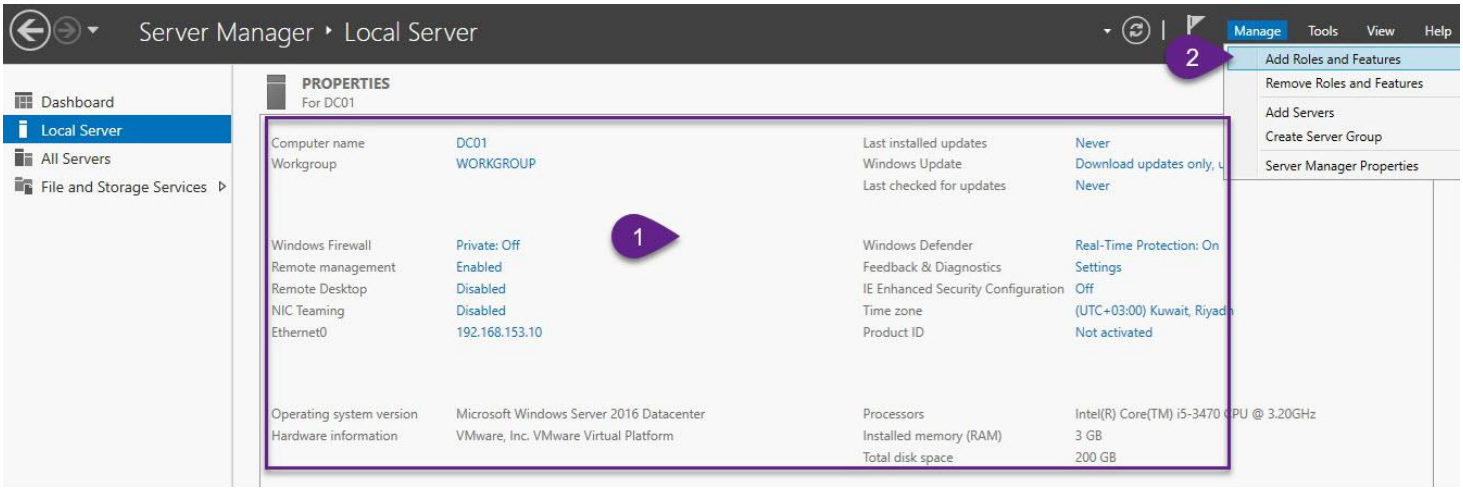
- Server fully update
- Configure static IP
- Create complex password for built-in administrator
- Rename server
- Configure time zone

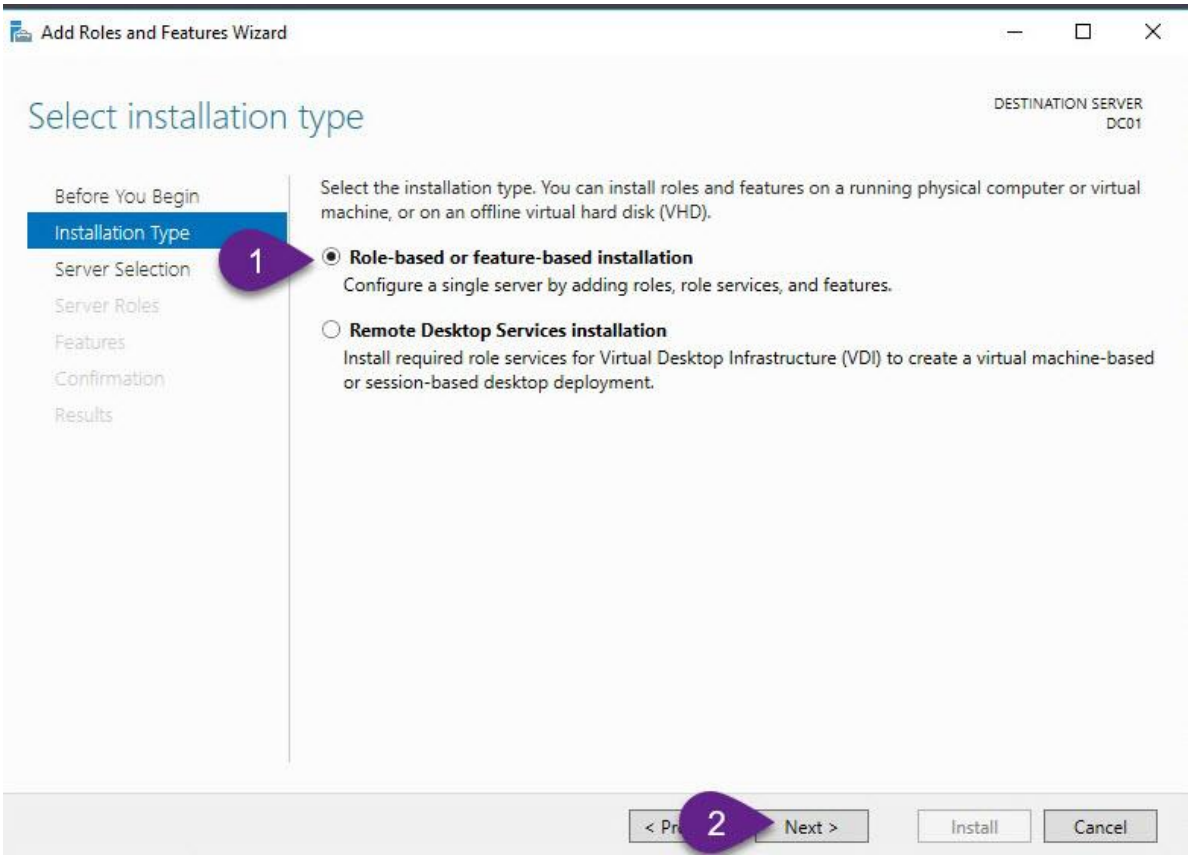
to change previous setting open server manager from start menu and follow the below

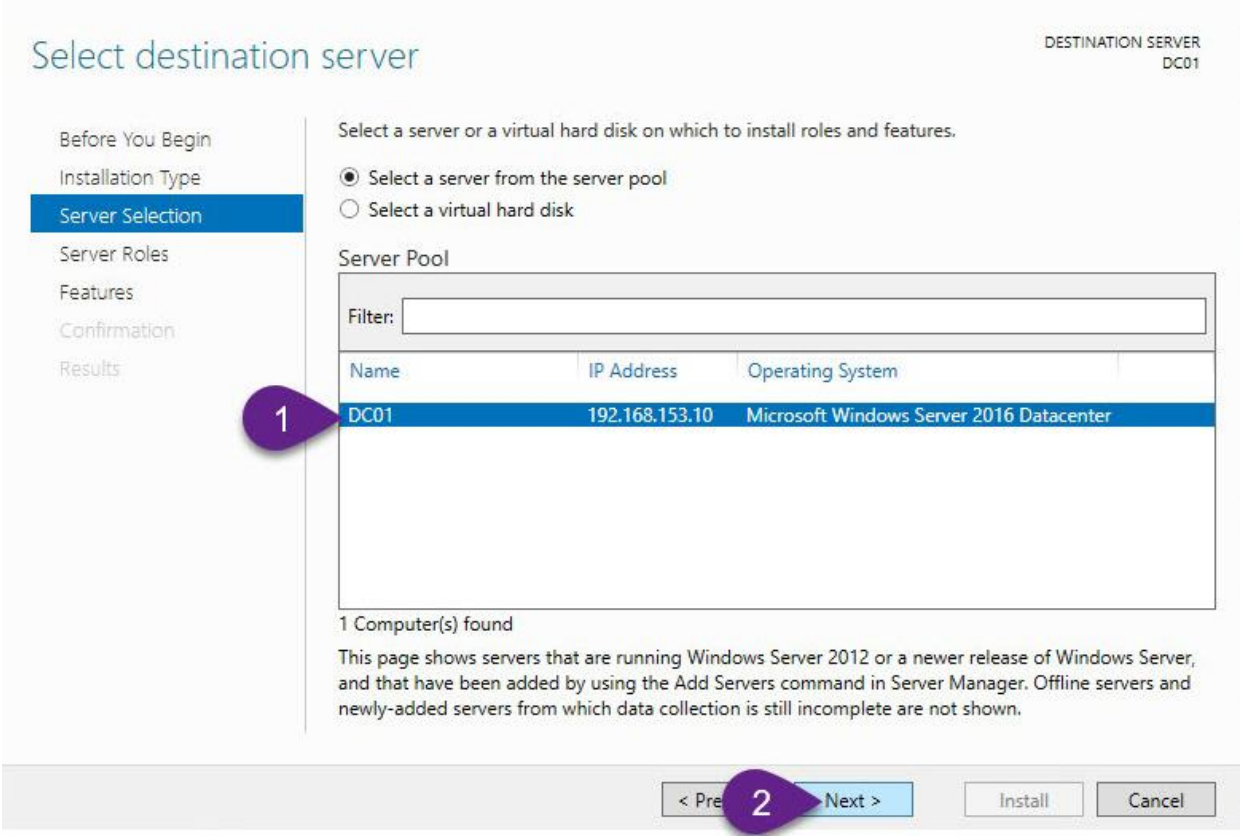


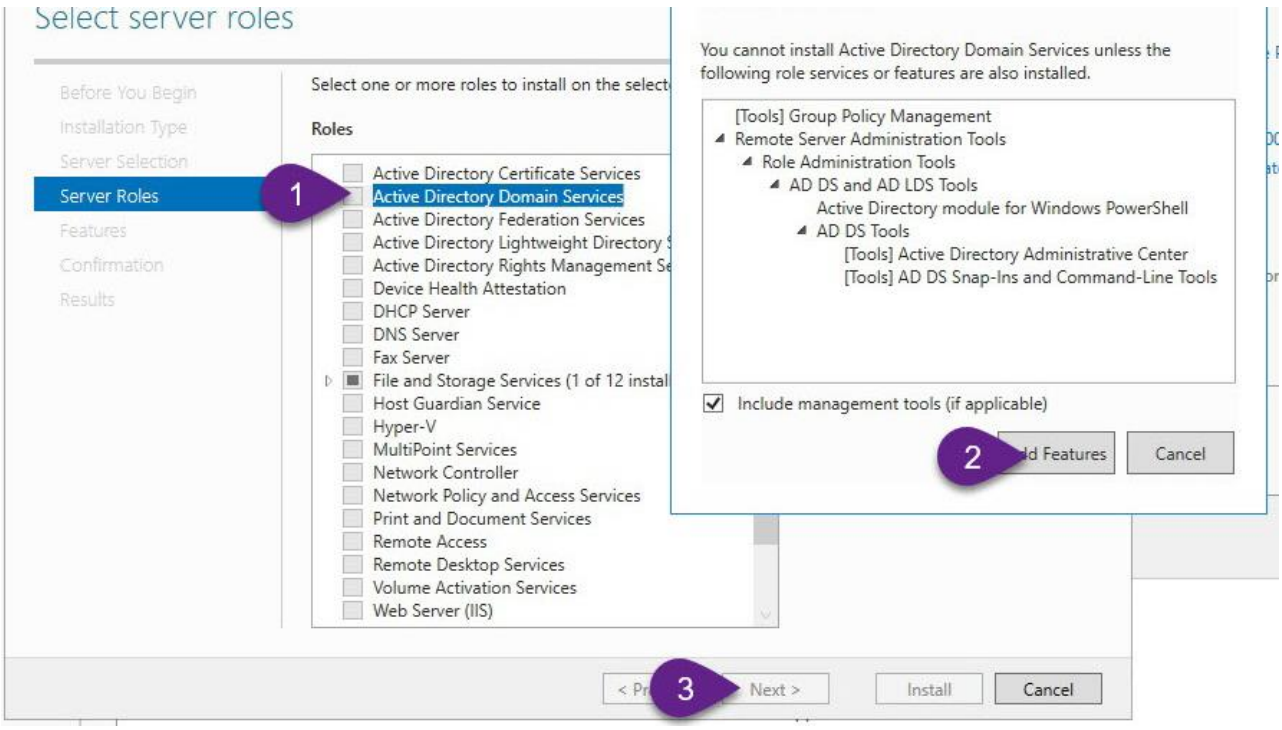
Install Active directory role

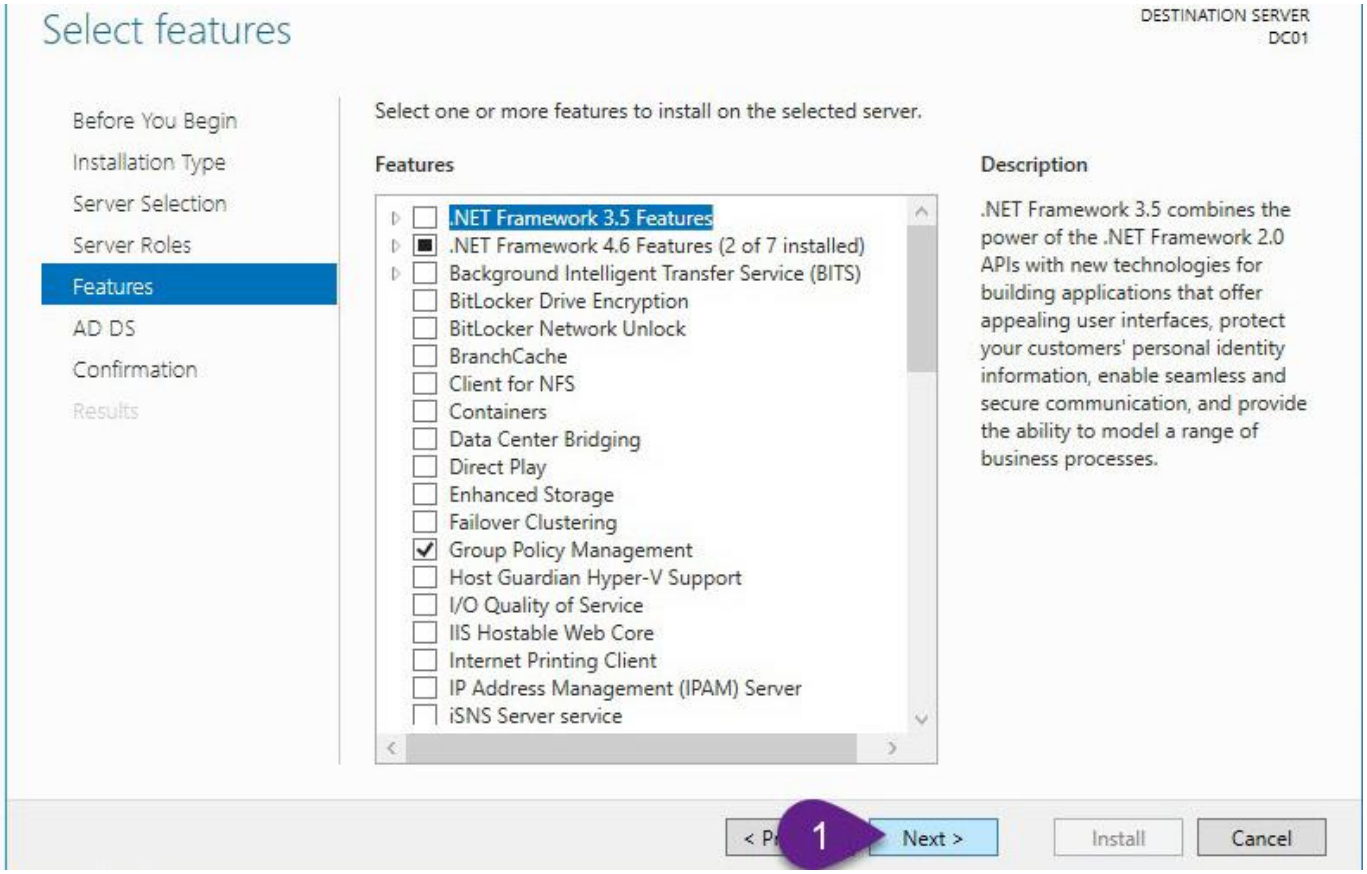
Our server is now prepared for the installation of Active Directory Domain Services, as depicted in the following figures.

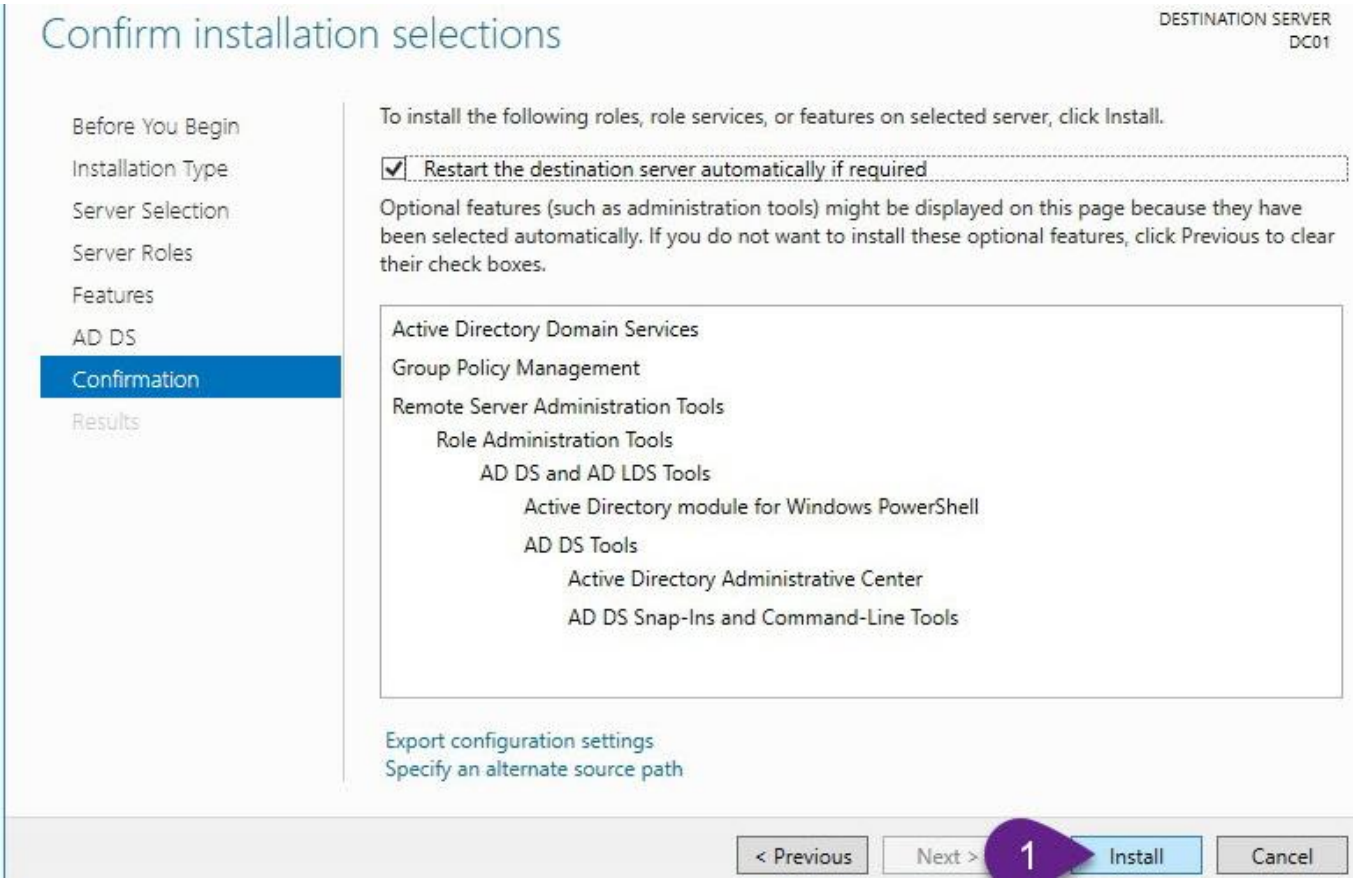





Select destination server
DESTINATION SERVER
DC01
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select a server or a virtual hard disk on which to install roles and features.
Select a server from the server pool
Select a virtual hard disk
Server Pool
Filter:
Name
IP Address
Operating System
1
DC01
192.168.153.10
Microsoft Windows Server 2016 Datacenter
1 Computer(s) found
This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.
< Pre
2
Next >
Install
Cancel


Select server roles
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select one or more roles to install on the select
Roles
1
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Federation Services
Active Directory Lightweight Directory
Active Directory Rights Management Se
Device Health Attestation
DHCP Server
DNS Server
Fax Server
File and Storage Services (1 of 12 instal
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)
You cannot install Active Directory Domain Services unless the following role services or features are also installed.
[Tools] Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
[Tools] Active Directory Administrative Center
[Tools] AD DS Snap-Ins and Command-Line Tools
Include management tools (if applicable)
2
d Features
Cancel
< Pr
3
Next >
Install
Cancel


Select features
DESTINATION SERVER
DC01
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results
Select one or more features to install on the selected server.
Features
.NET Framework 3.5 Features
.NET Framework 4.6 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
Group Policy Management
Host Guardian Hyper-V Support
I/O Quality of Service
IIS Hostable Web Core
Internet Printing Client
IP Address Management (IPAM) Server
iSNS Server service
Description
.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.
1
Next >
Install
Cancel

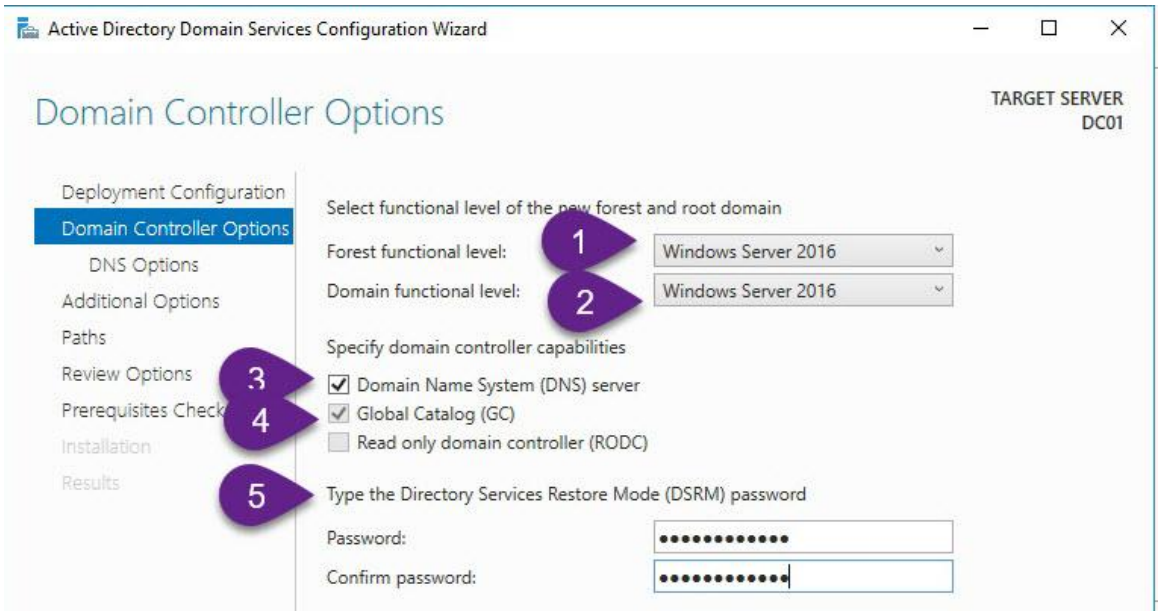

Confirm installation selections
DESTINATION SERVER
DC01
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results
To install the following roles, role services, or features on selected server, click Install.
Restart the destination server automatically if required
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.
Active Directory Domain Services
Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
Active Directory Administrative Center
AD DS Snap-Ins and Command-Line Tools
Export configuration settings
Specify an alternate source path
< Previous
Next >
1
Install
Cancel

Promoting to Domain Controllers

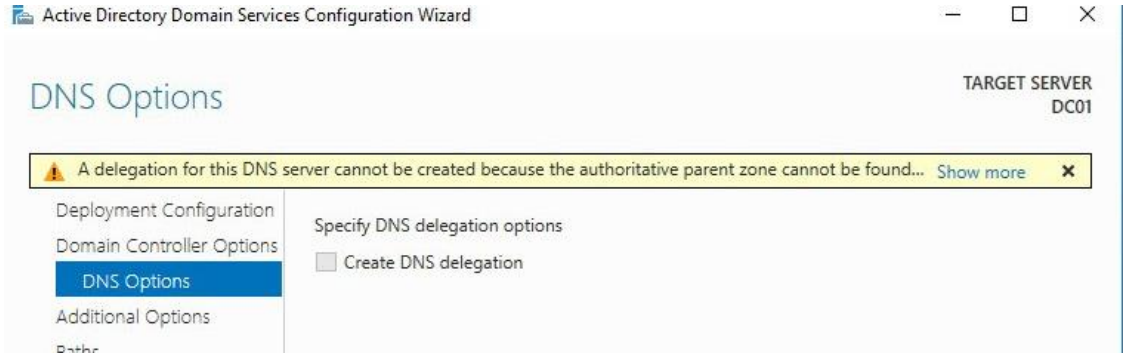
We can now upgrade the server to an active directory by following the steps illustrated below in the server manager.

- There are three permissible actions when elevating your server to active directory status:
  Make your server an additional domain controller in an existing domain,
  Transform your server into a child domain within an existing forest,
  Designate your server as the root of a new forest (as chosen for our scenario).

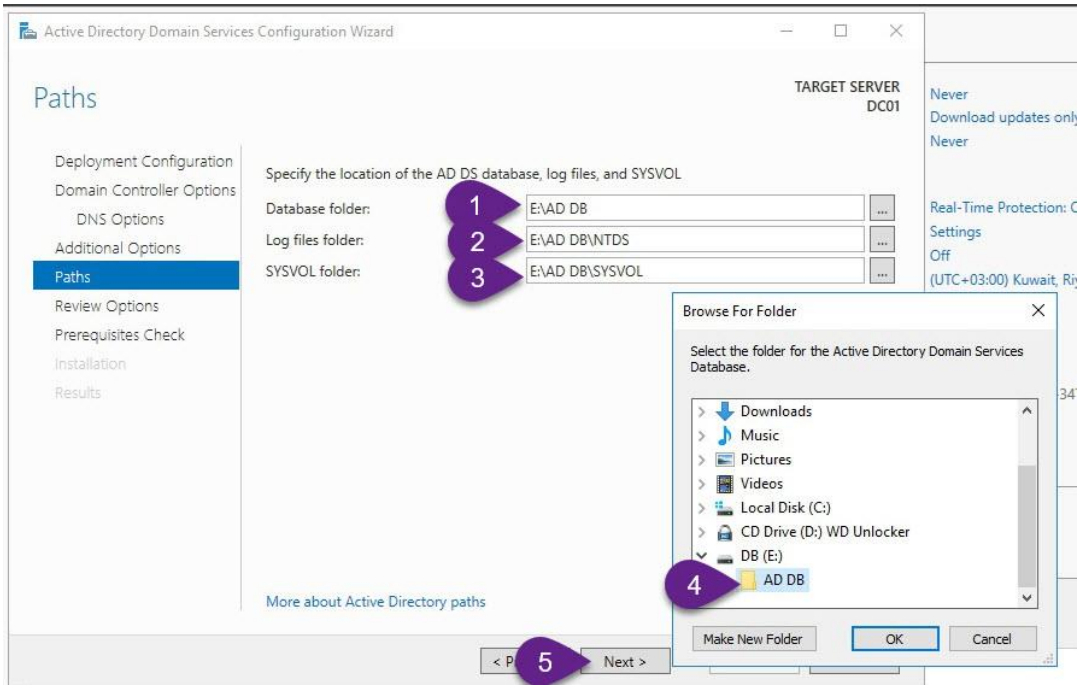
Choose the forest and domain functional level to activate extra features in Active Directory. For this scenario, opt for Windows Server 2016. Our domain will also serve as DNS and hold the global catalog. Lastly, set up a password for AD restore mode.

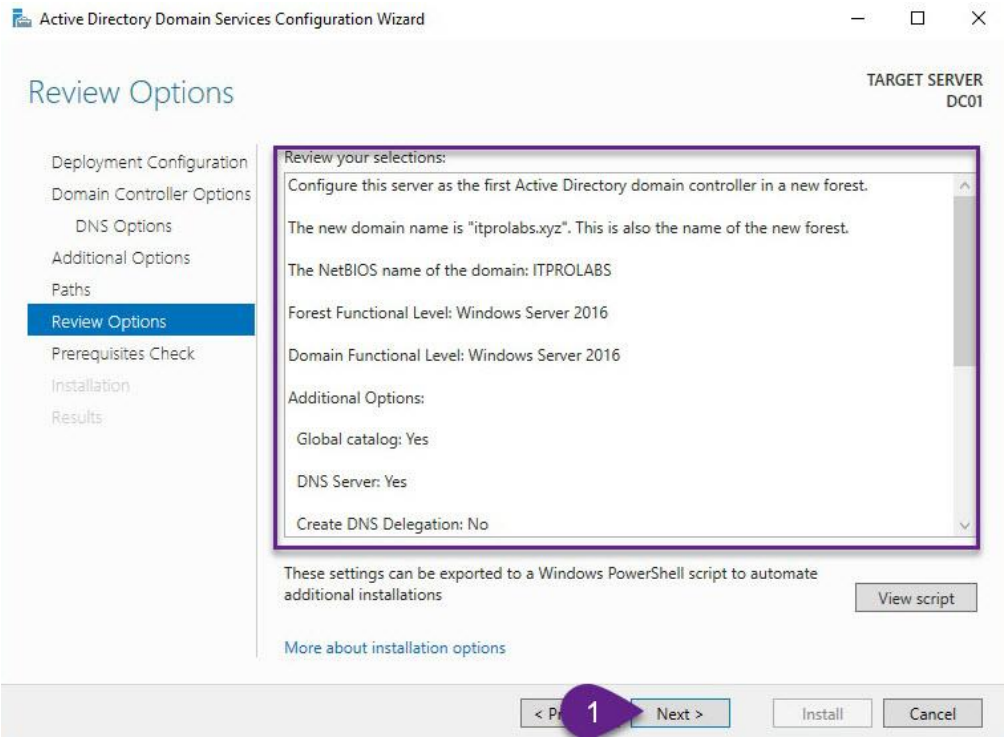

Active Directory Domain Services Configuration Wizard
Domain Controller Options
TARGET SERVER
DC01
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Select functional level of the new forest and root domain
Forest functional level:
Windows Server 2016
Domain functional level:
Windows Server 2016
Specify domain controller capabilities
Domain Name System (DNS) server
Global Catalog (GC)
Read only domain controller (RODC)
Type the Directory Services Restore Mode (DSRM) password
Password:
Confirm password:
1
2
3
4
5

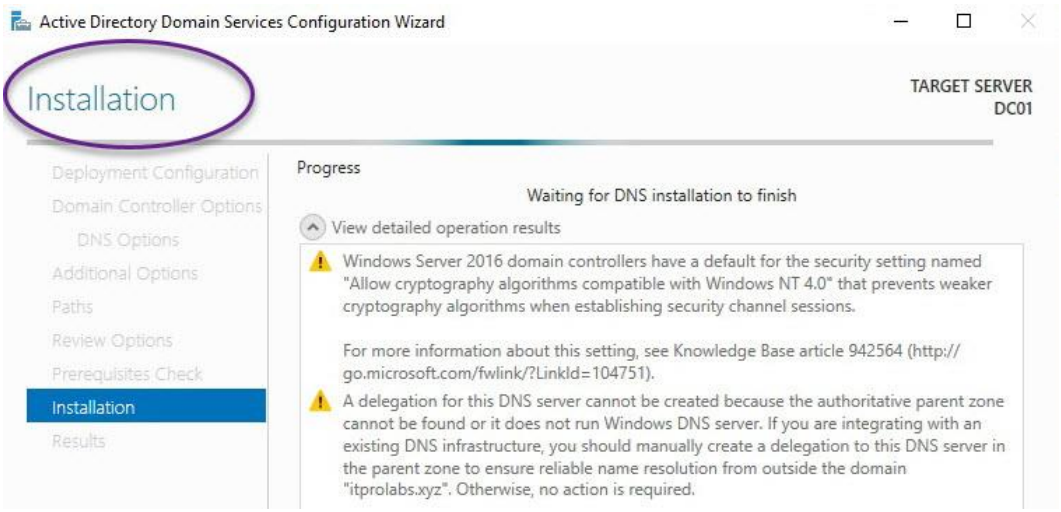

Active Directory Domain Services Configuration Wizard
Additional Options
TARGET SERVER
DC01
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Verify the NetBIOS name assigned to the domain and change it if necessary
The NetBIOS domain name:
ITPROLABS

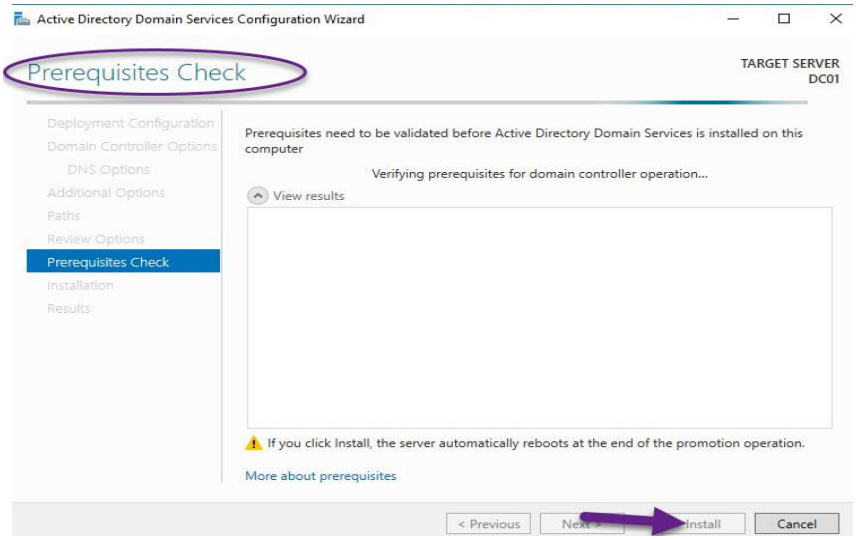

Active Directory Domain Services Configuration Wizard
DNS Options
TARGET SERVER
DC01
A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found...
Show more
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Specify DNS delegation options
Create DNS delegation

It is advisable to relocate the Active Directory database and log file locations away from the operating system partition.

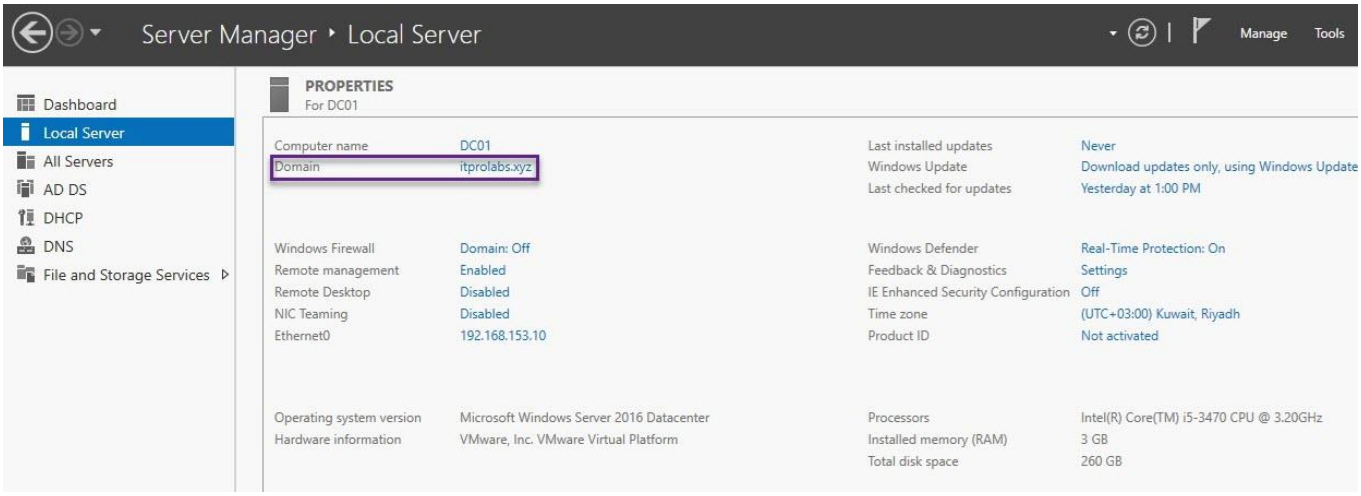


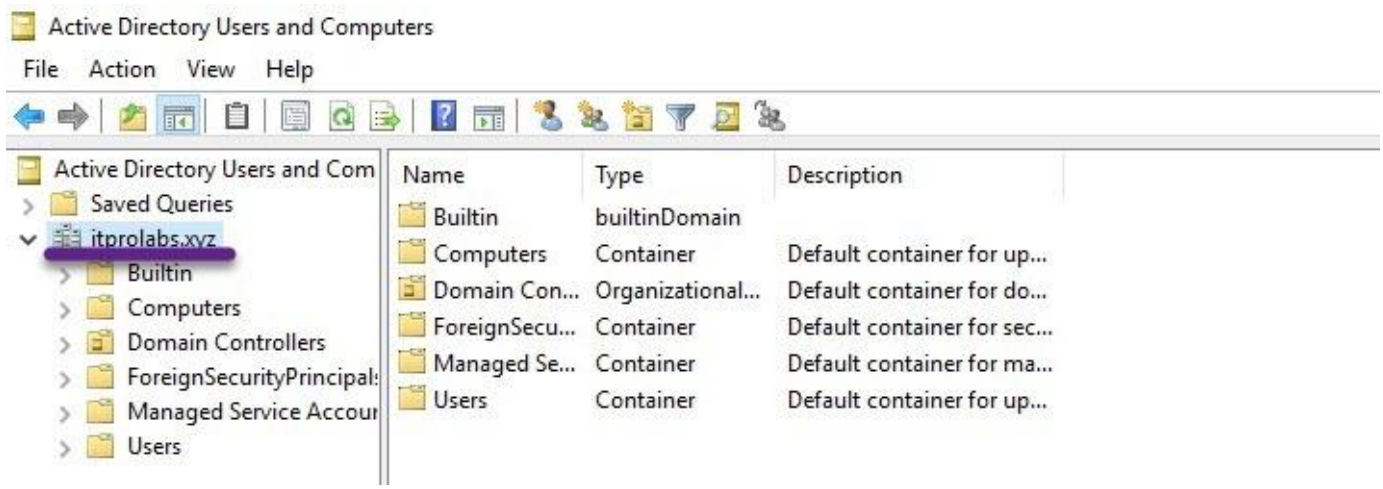



Active Directory Domain Services Configuration Wizard
Installation
TARGET SERVER
DC01
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Progress
Waiting for DNS installation to finish
View detailed operation results
Windows Server 2016 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.
For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).
A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "itprolabs.xyz". Otherwise, no action is required.


Active Directory Domain Services Configuration Wizard
Prerequisites Check
TARGET SERVER
DC01
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Prerequisites need to be validated before Active Directory Domain Services is installed on this computer
Verifying prerequisites for domain controller operation...
View results
If you click Install, the server automatically reboots at the end of the promotion operation.
More about prerequisites
< Previous
Next >
Install
Cancel

Our server has been successfully promoted to an active directory domain controller.





Secondary Active Directory Domain Controller

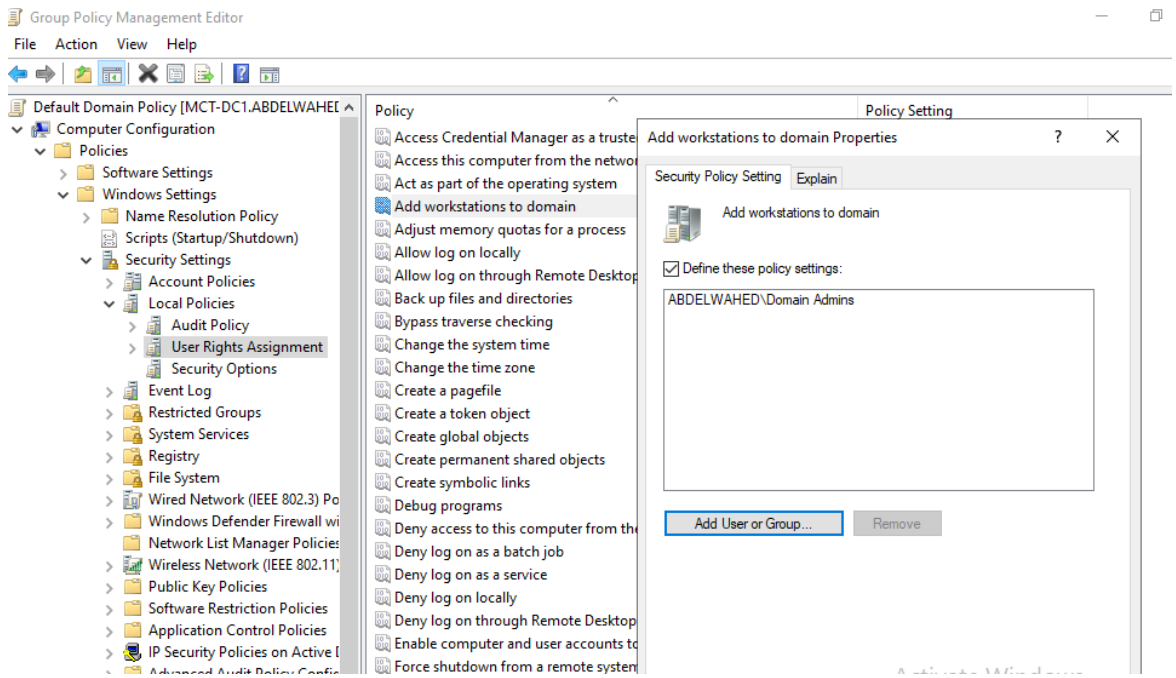
To enhance the high availability and reliability of our primary Domain Controller (DC) for **abdelwahed.me**, we are going to create a secondary Active Directory Domain Controller. This secondary DC will serve multiple purposes, including:

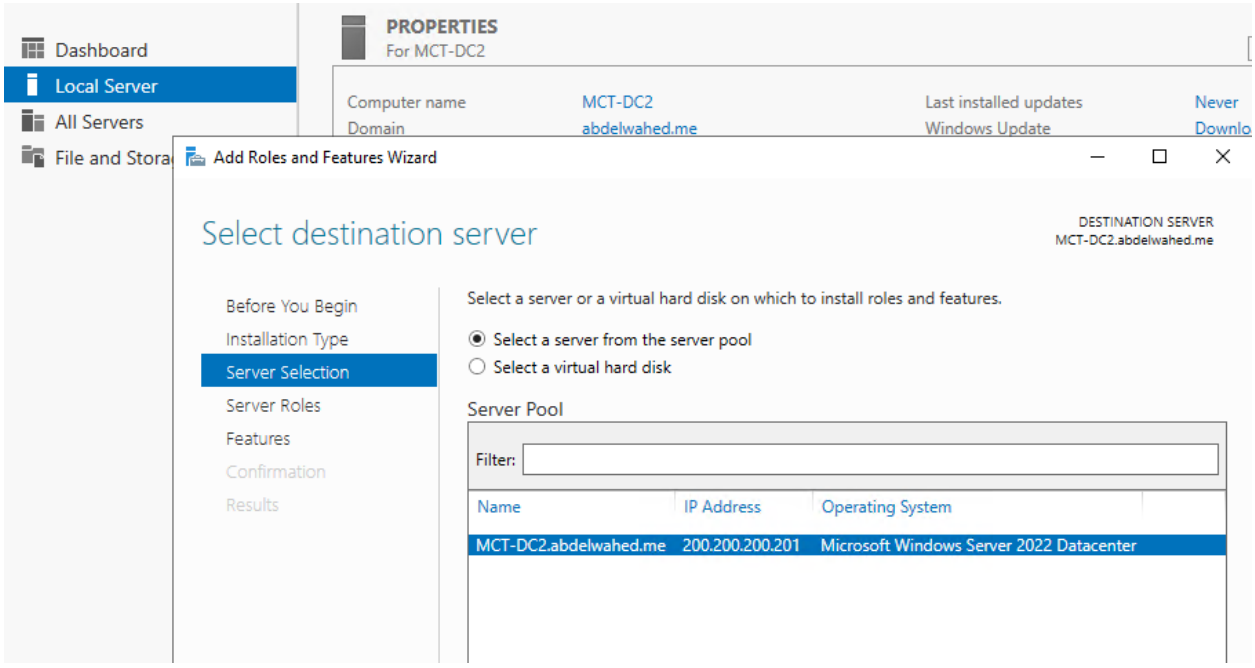
1. **High Availability:**
    - The secondary DC ensures that our Active Directory services remain available in case the primary DC experiences downtime or failure. This setup helps to maintain uninterrupted access to resources and authentication services.
2. **Upgrade Path:**
    - Operating System Upgrades: When upgrading from an older Windows Server version to a new one, the secondary DC can facilitate a smooth transition. By promoting a secondary DC with the new OS, we can gradually transfer roles and services, ensuring minimal disruption.
    - Hardware Upgrades: When the primary DC requires a hardware upgrade, the secondary DC can take over its responsibilities temporarily. This allows for seamless hardware updates without affecting domain services.
3. **Redundancy:**
    - The secondary DC acts as a backup for the Active Directory database. This redundancy protects against data loss and ensures that changes to the directory are replicated and preserved.
4. **Load Balancing:**
    - With a secondary DC, authentication and directory lookup requests can be distributed across multiple servers. This load balancing improves performance and responsiveness for users and applications.

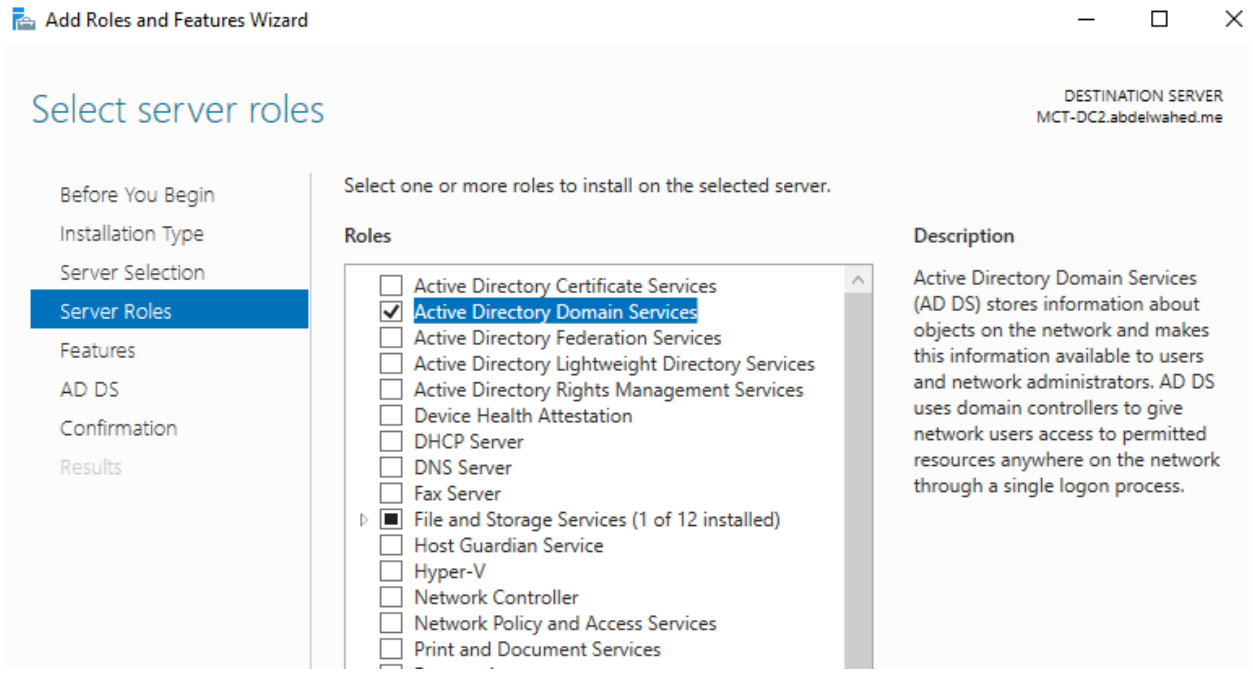
Steps to Create a Secondary Active Directory Domain Controller:

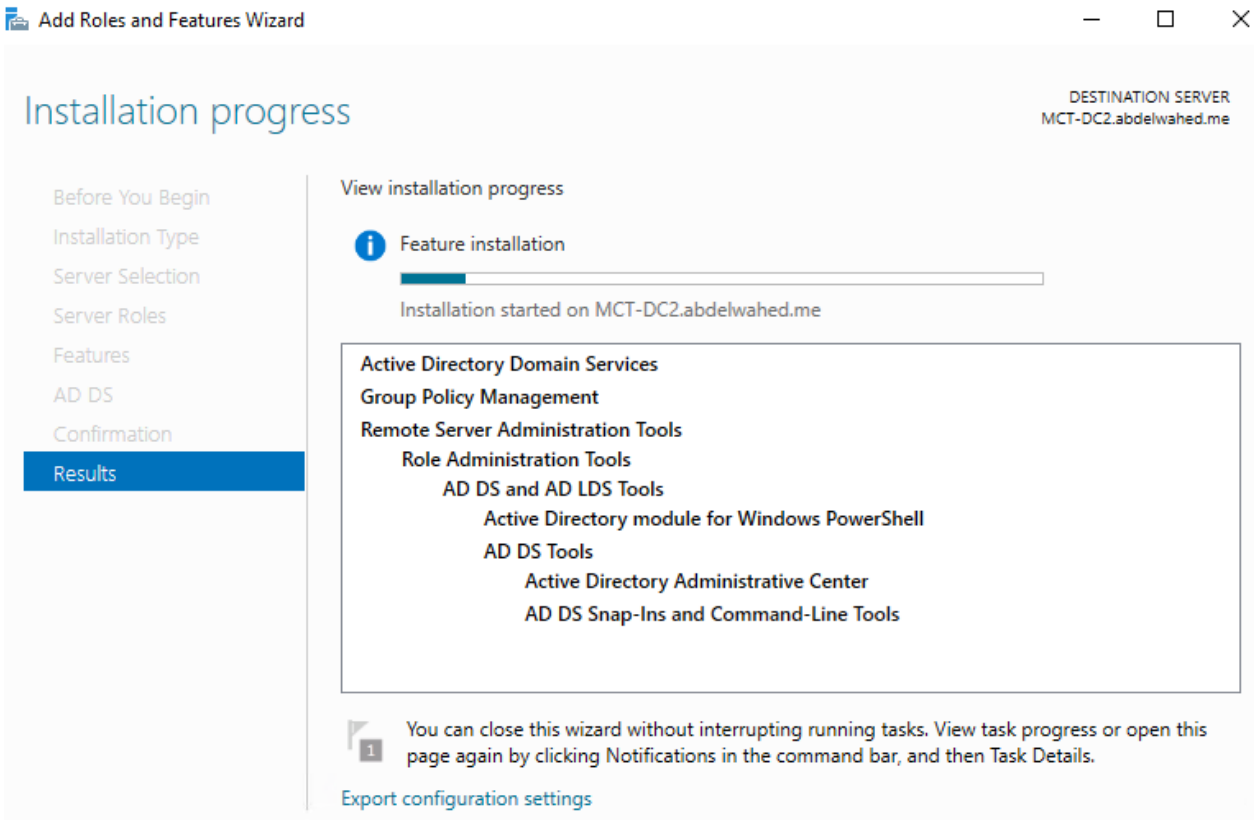
1. **Prepare the Secondary Server:**
    - Ensure that the secondary server meets the system requirements and is properly configured with a static IP address and DNS settings.
2. **Join the Secondary Server to the Domain:**
    - Add the secondary server to the existing domain abdelwahed.me.
3. **Install Active Directory Domain Services (AD DS):**
    - Use the Server Manager to install the AD DS role on the secondary server.
4. **Promote the Server to a Domain Controller:**
    - Promote the secondary server to a Domain Controller using the Active Directory Domain Services Configuration Wizard. Ensure it is configured to replicate from the primary DC.
5. **Verify Replication:**
    - Ensure that replication between the primary and secondary DCs is functioning correctly. Use tools like repadmin and Active Directory Sites and Services to monitor replication status.
6. **Transfer FSMO Roles (if necessary):**
    - Consider transferring Flexible Single Master Operations (FSMO) roles to the secondary DC if needed for load balancing or during the upgrade process.

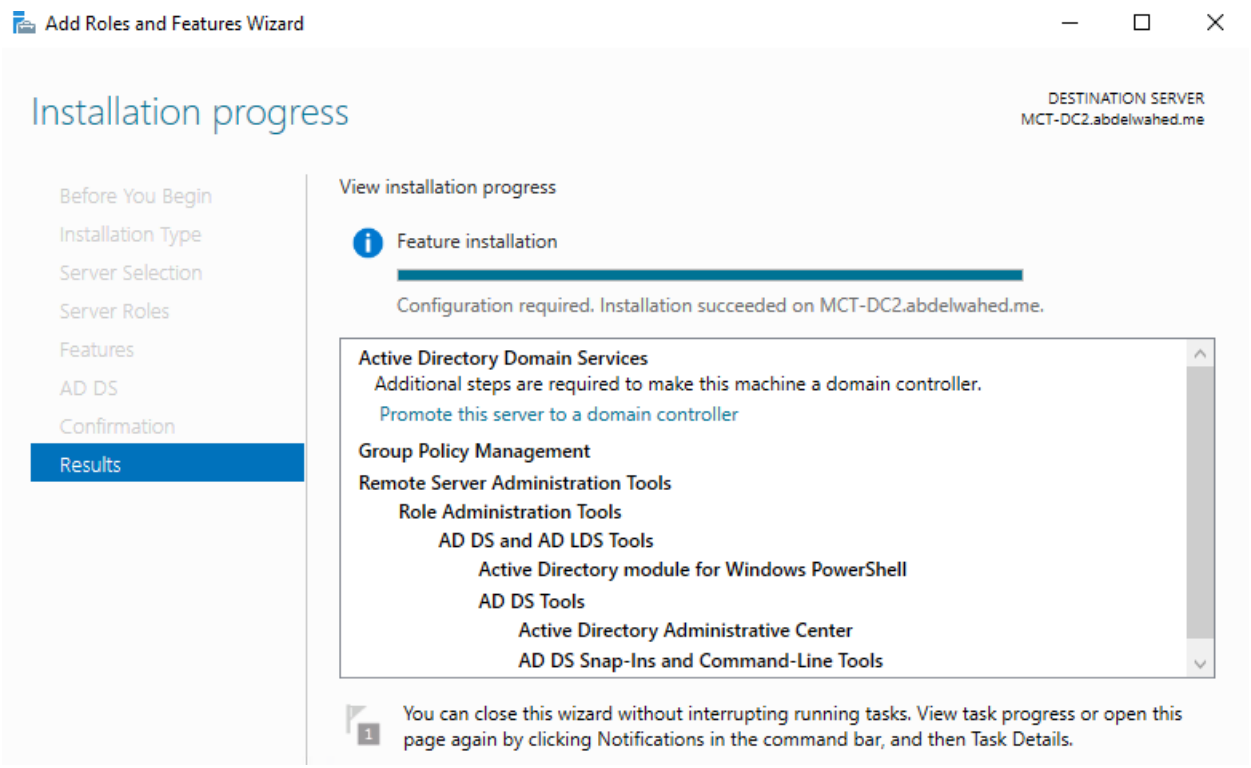
All steps explained above are illustrated in the photos below:

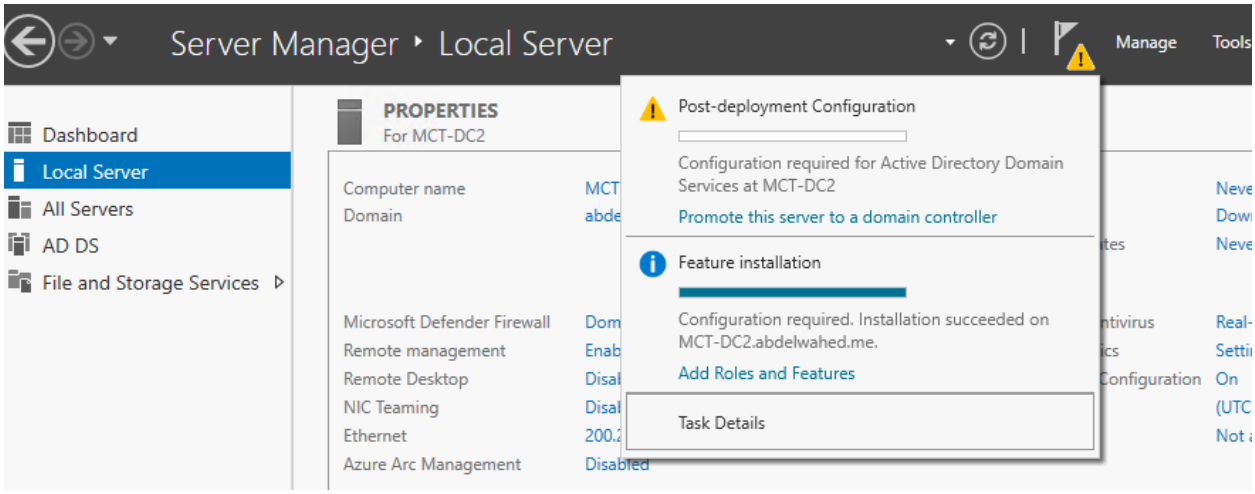

Group Policy Management Editor
File Action View Help
Default Domain Policy [MCT-DC1.ABDELWAHED
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Po
Windows Defender Firewall wi
Network List Manager Policies
Wireless Network (IEEE 802.11)
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active
Policy
Policy Setting
Access Credential Manager as a truste
Access this computer from the networ
Act as part of the operating system
Add workstations to domain
Adjust memory quotas for a process
Allow log on locally
Allow log on through Remote Desktop
Back up files and directories
Bypass traverse checking
Change the system time
Change the time zone
Create a pagefile
Create a token object
Create global objects
Create permanent shared objects
Create symbolic links
Debug programs
Deny access to this computer from th
Deny log on as a batch job
Deny log on as a service
Deny log on locally
Deny log on through Remote Desktop
Enable computer and user accounts to
Force shutdown from a remote system
Add workstations to domain Properties
Security Policy Setting
Explain
Add workstations to domain
Define these policy settings:
ABDELWAHED\Domain Admins
Add User or Group...
Remove

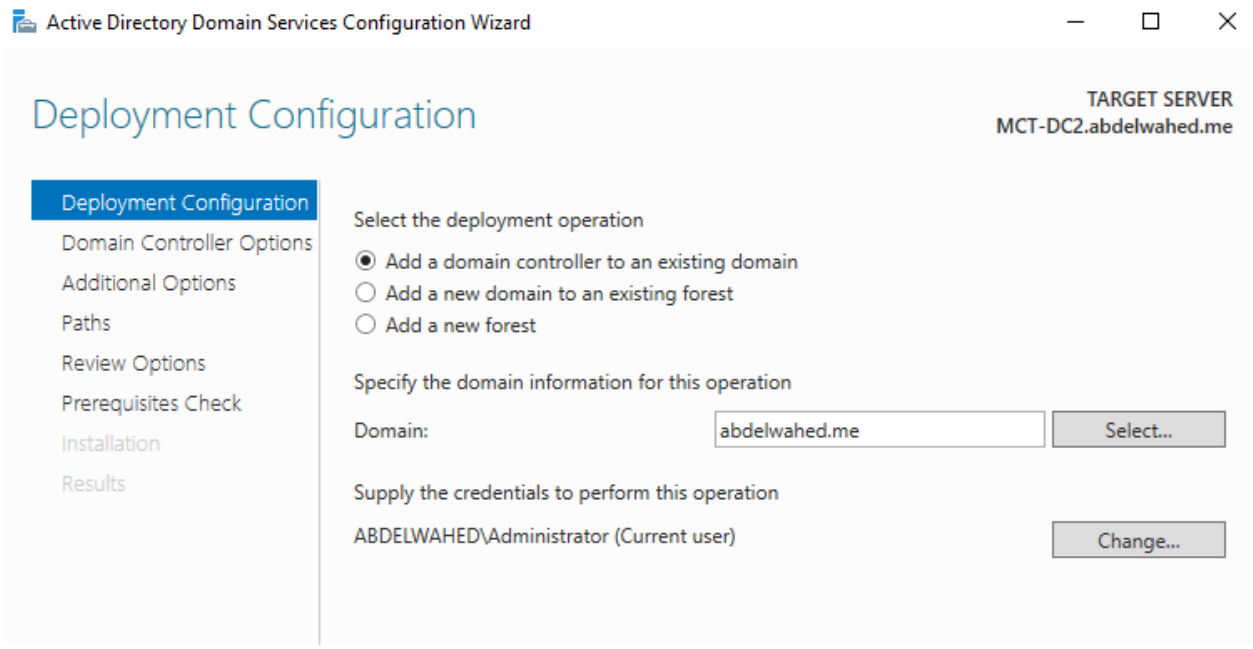

Dashboard
Local Server
All Servers
File and Stora
PROPERTIES
For MCT-DC2
Computer name
MCT-DC2
Domain
abdelwahed.me
Last installed updates
Never
Windows Update
Downlo
Add Roles and Features Wizard
Select destination server
DESTINATION SERVER
MCT-DC2.abdelwahed.me
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
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
MCT-DC2.abdelwahed.me
200.200.200.201
Microsoft Windows Server 2022 Datacenter

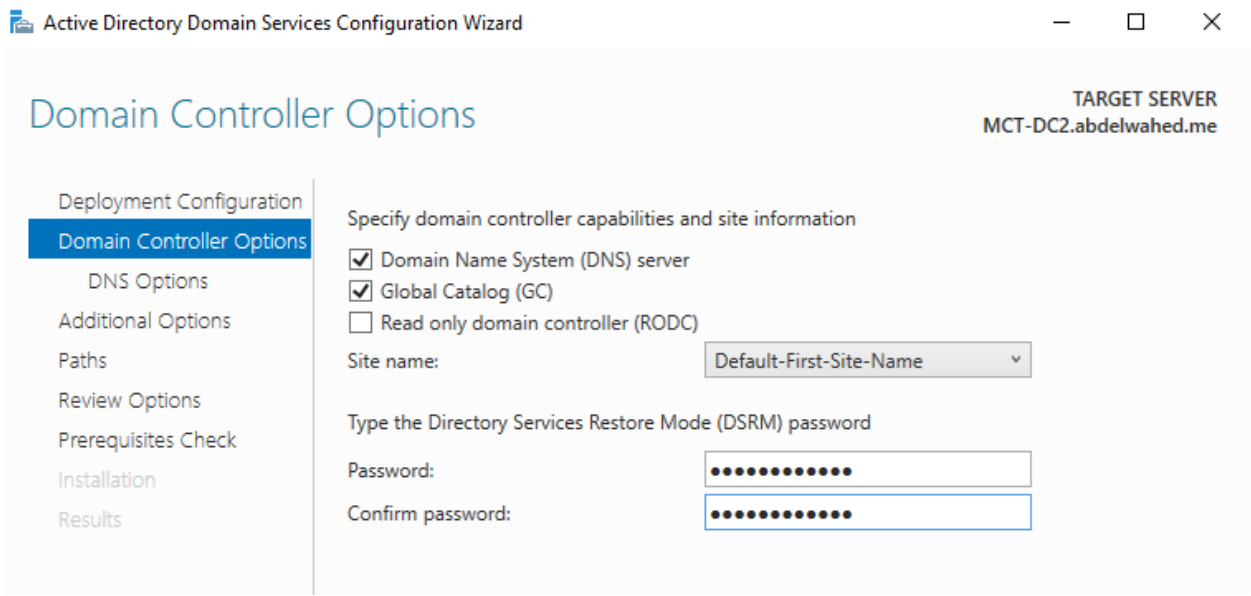

Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
MCT-DC2.abdelwahed.me
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Federation Services
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
Network Controller
Network Policy and Access Services
Print and Document Services
Description
Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.

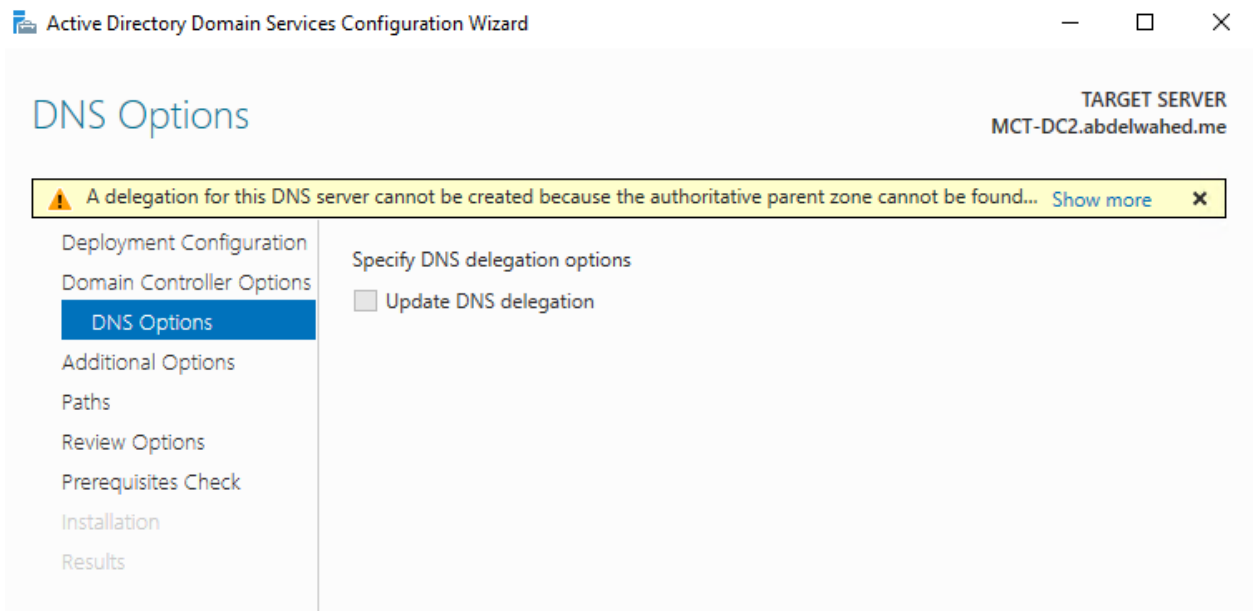

Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
MCT-DC2.abdelwahed.me
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results
View installation progress
Feature installation
Installation started on MCT-DC2.abdelwahed.me
Active Directory Domain Services
Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
Active Directory Administrative Center
AD DS Snap-Ins and Command-Line Tools
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

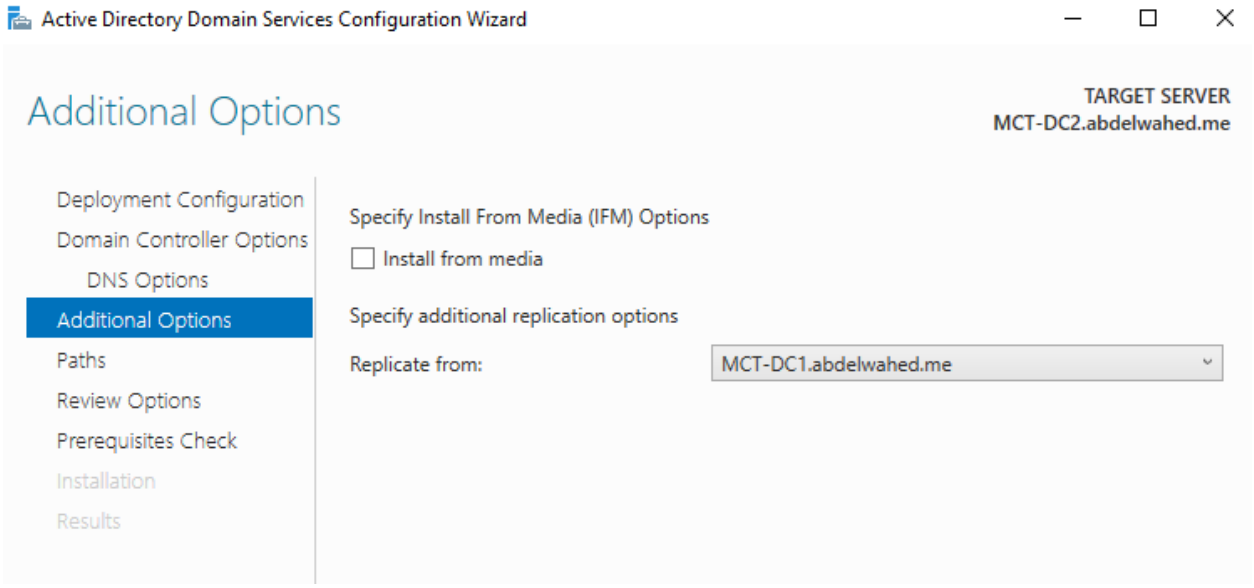

Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
MCT-DC2.abdelwahed.me
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results
View installation progress
Feature installation
Configuration required. Installation succeeded on MCT-DC2.abdelwahed.me.
Active Directory Domain Services
Additional steps are required to make this machine a domain controller.
Promote this server to a domain controller
Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
Active Directory Administrative Center
AD DS Snap-Ins and Command-Line Tools
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.

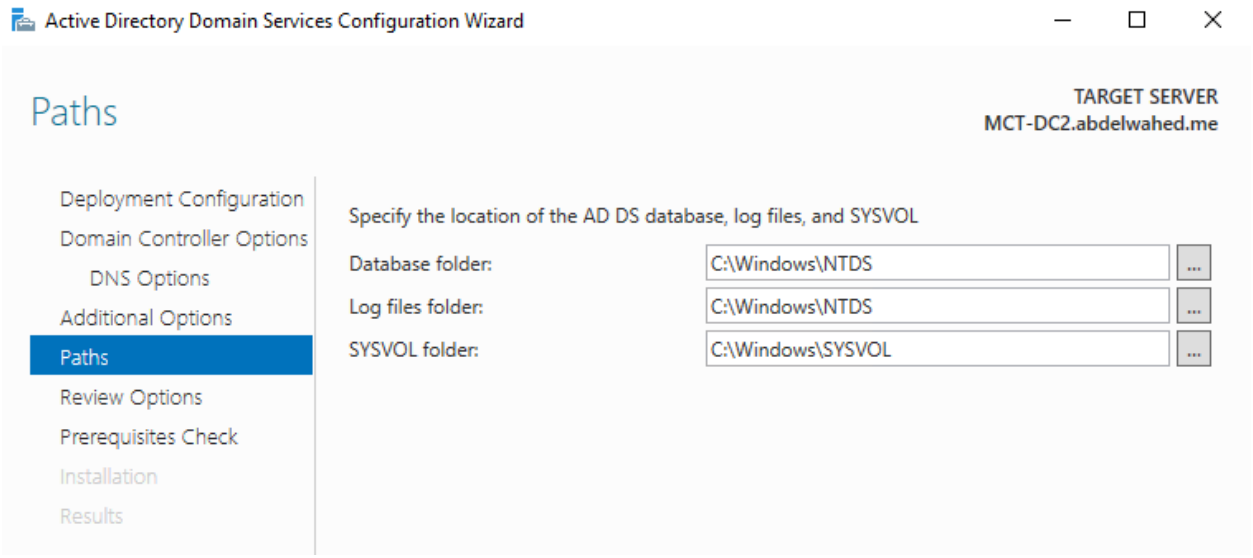

Server Manager ‣ Local Server
Manage
Tools
Dashboard
Local Server
All Servers
AD DS
File and Storage Services
PROPERTIES
For MCT-DC2
Computer name
Domain
Microsoft Defender Firewall
Remote management
Remote Desktop
NIC Teaming
Ethernet
Azure Arc Management
Disabled
Post-deployment Configuration
Configuration required for Active Directory Domain Services at MCT-DC2
Promote this server to a domain controller
Feature installation
Configuration required. Installation succeeded on MCT-DC2.abdelwahed.me.
Add Roles and Features
Task Details

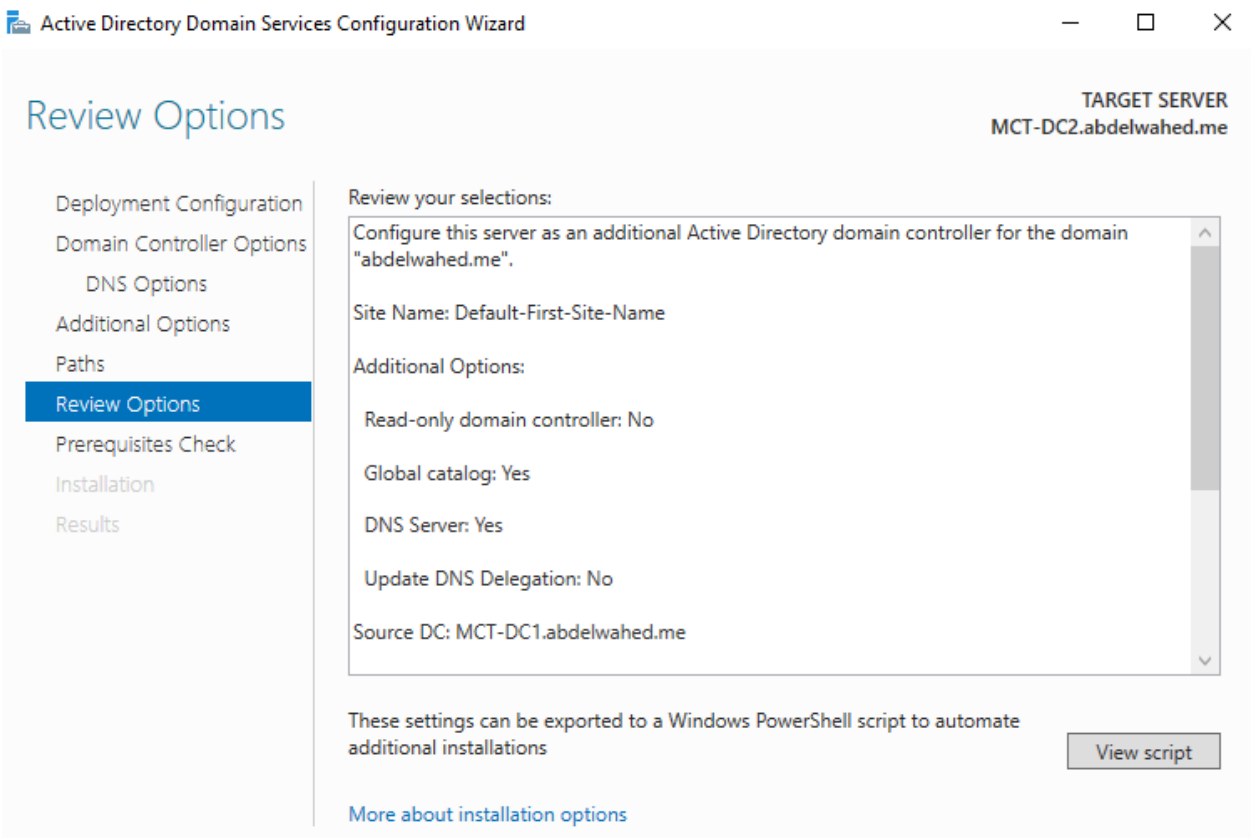

Active Directory Domain Services Configuration Wizard
Deployment Configuration
TARGET SERVER
MCT-DC2.abdelwahed.me
Deployment Configuration
Domain Controller Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Select the deployment operation
Add a domain controller to an existing domain
Add a new domain to an existing forest
Add a new forest
Specify the domain information for this operation
Domain:
abdelwahed.me
Select...
Supply the credentials to perform this operation
ABDELWAHED\Administrator (Current user)
Change...

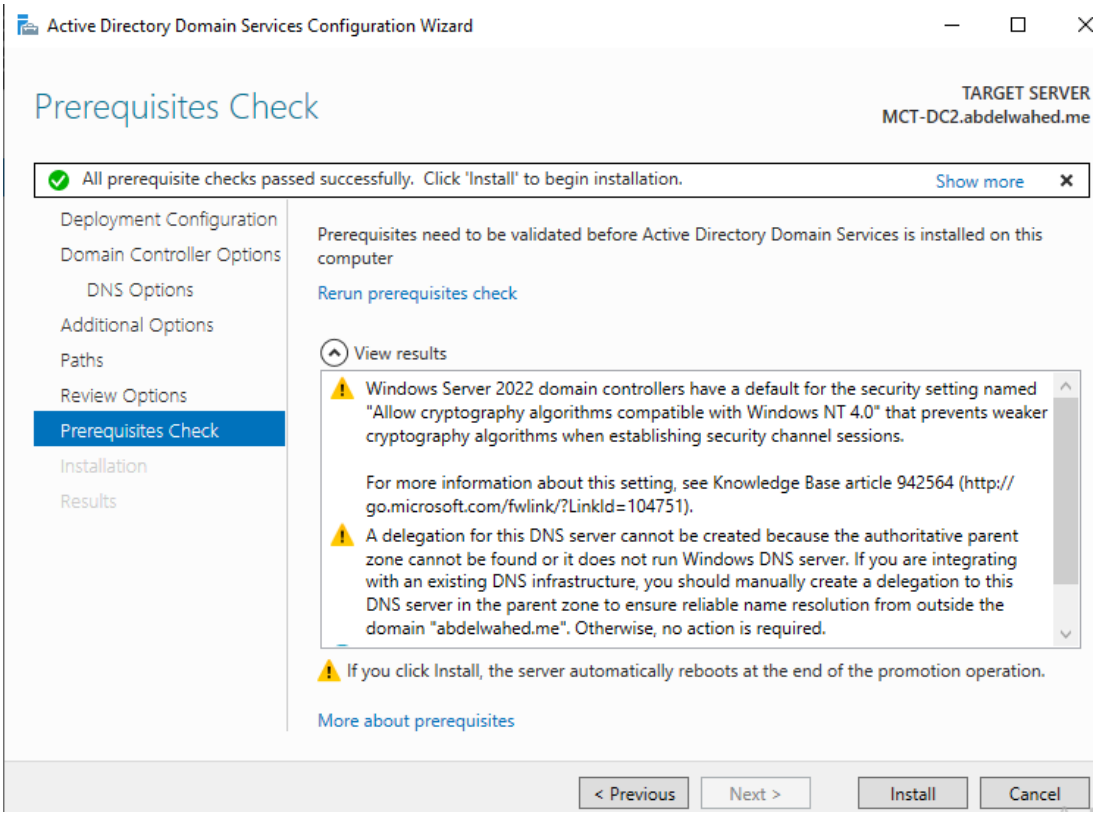

Active Directory Domain Services Configuration Wizard
Domain Controller Options
TARGET SERVER
MCT-DC2.abdelwahed.me
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Specify domain controller capabilities and site information
Domain Name System (DNS) server
Global Catalog (GC)
Read only domain controller (RODC)
Site name:
Default-First-Site-Name
Type the Directory Services Restore Mode (DSRM) password
Password:
Confirm password:

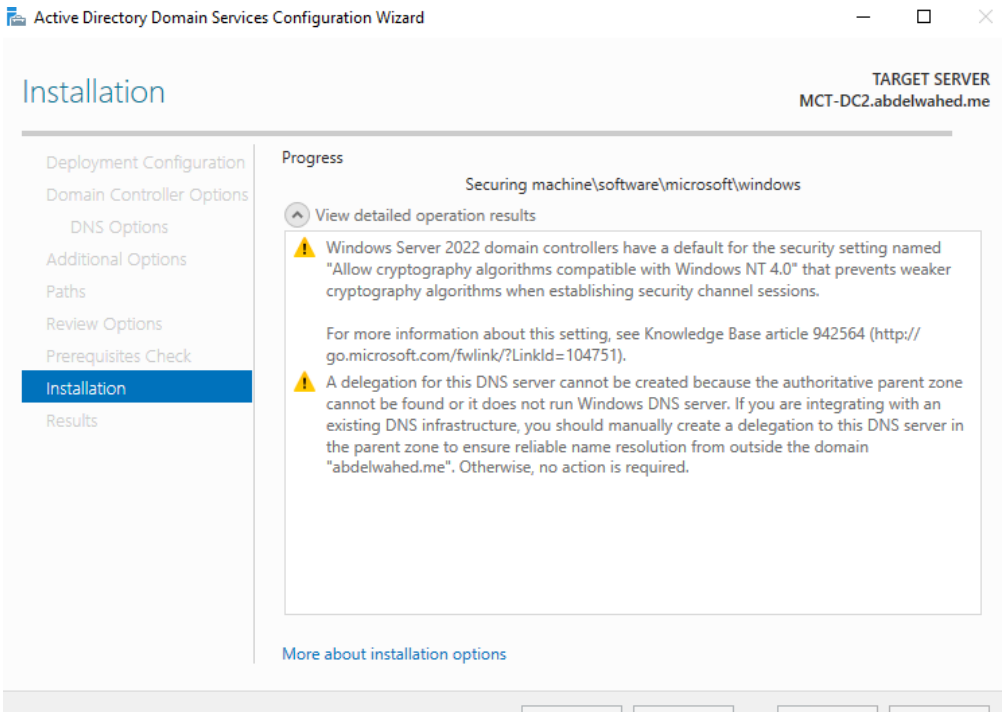

Active Directory Domain Services Configuration Wizard
DNS Options
TARGET SERVER
MCT-DC2.abdelwahed.me
A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found...
Show more
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Specify DNS delegation options
Update DNS delegation

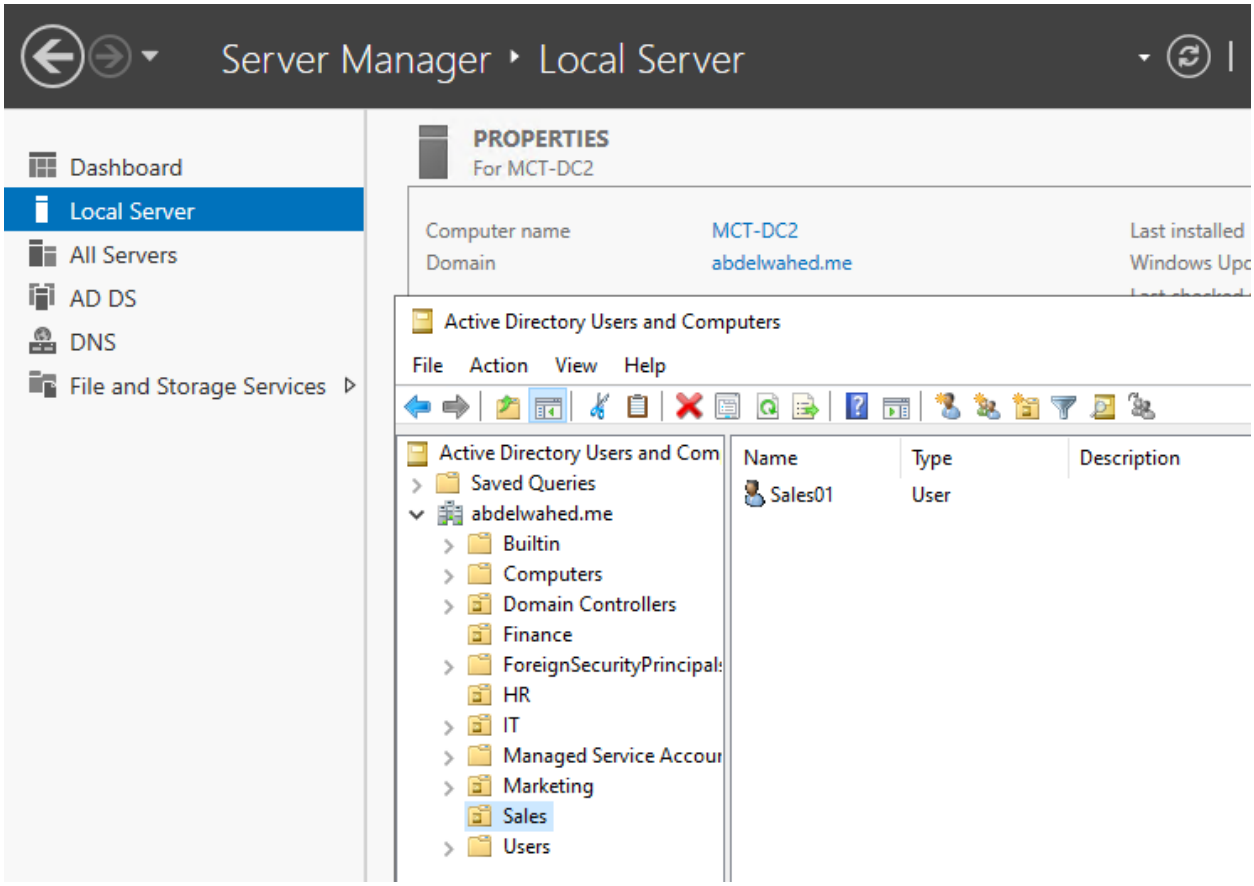

Active Directory Domain Services Configuration Wizard
Additional Options
TARGET SERVER
MCT-DC2.abdelwahed.me
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Specify Install From Media (IFM) Options
Install from media
Specify additional replication options
Replicate from:
MCT-DC1.abdelwahed.me


Active Directory Domain Services Configuration Wizard
Paths
TARGET SERVER
MCT-DC2.abdelwahed.me
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Specify the location of the AD DS database, log files, and SYSVOL
Database folder:
C:\Windows\NTDS
Log files folder:
C:\Windows\NTDS
SYSVOL folder:
C:\Windows\SYSVOL


Active Directory Domain Services Configuration Wizard
Review Options
TARGET SERVER
MCT-DC2.abdelwahed.me
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Review your selections:
Configure this server as an additional Active Directory domain controller for the domain "abdelwahed.me".
Site Name: Default-First-Site-Name
Additional Options:
Read-only domain controller: No
Global catalog: Yes
DNS Server: Yes
Update DNS Delegation: No
Source DC: MCT-DC1.abdelwahed.me
These settings can be exported to a Windows PowerShell script to automate additional installations
View script
More about installation options


Active Directory Domain Services Configuration Wizard
Prerequisites Check
TARGET SERVER
MCT-DC2.abdelwahed.me
All prerequisite checks passed successfully. Click 'Install' to begin installation.
Show more
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Prerequisites need to be validated before Active Directory Domain Services is installed on this computer
Rerun prerequisites check
View results
Windows Server 2022 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.
For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).
A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "abdelwahed.me". Otherwise, no action is required.
If you click Install, the server automatically reboots at the end of the promotion operation.
More about prerequisites
< Previous
Next >
Install
Cancel


Active Directory Domain Services Configuration Wizard
Installation
TARGET SERVER
MCT-DC2.abdelwahed.me
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Progress
Securing machine\software\microsoft\windows
View detailed operation results
Windows Server 2022 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.
For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).
A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "abdelwahed.me". Otherwise, no action is required.
More about installation options


Server Manager ‣ Local Server
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
PROPERTIES
For MCT-DC2
Computer name
MCT-DC2
Domain
abdelwahed.me
Last installed
Windows Upc
Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
abdelwahed.me
Builtin
Computers
Domain Controllers
Finance
ForeignSecurityPrincipal:
HR
IT
Managed Service Accour
Marketing
Sales
Users
Name
Type
Description
Sales01
User

DHCP

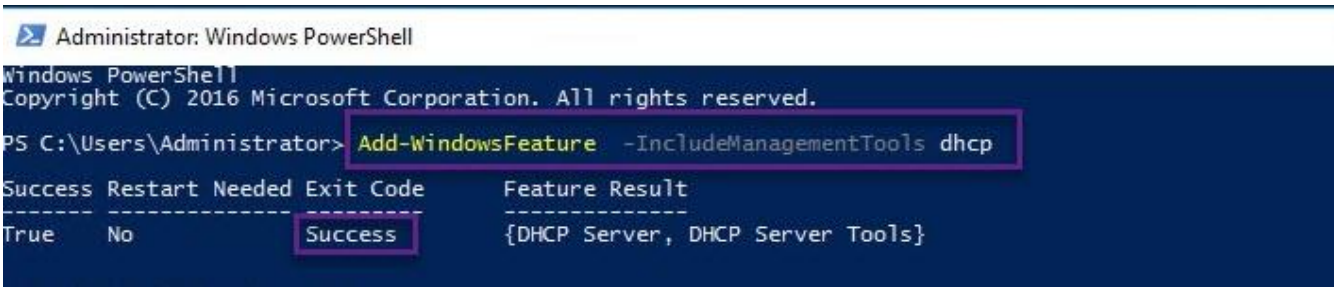
Lab Goal

The Dynamic Host Configuration Protocol (DHCP) automatically assigns TCP/IP configuration such as IP address, subnet mask, default gateway, DNS server, and various other parameters. This laboratory session is designed to impart the necessary skills for installing and administering a DHCP Server.

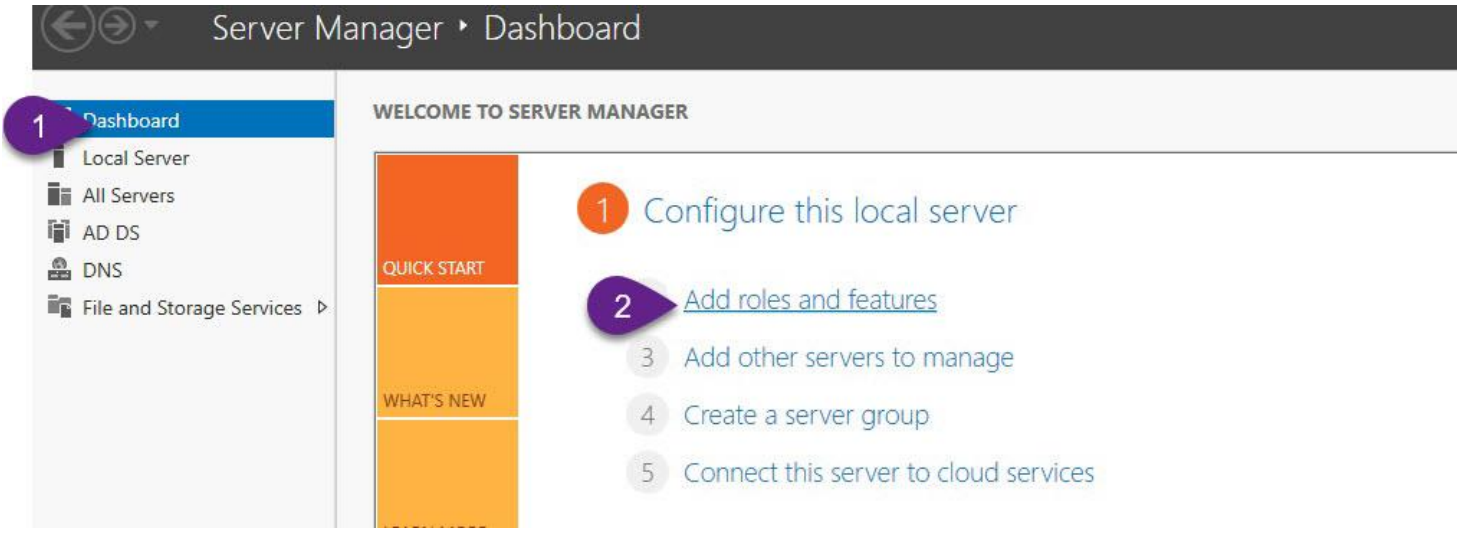
Install DHCP role

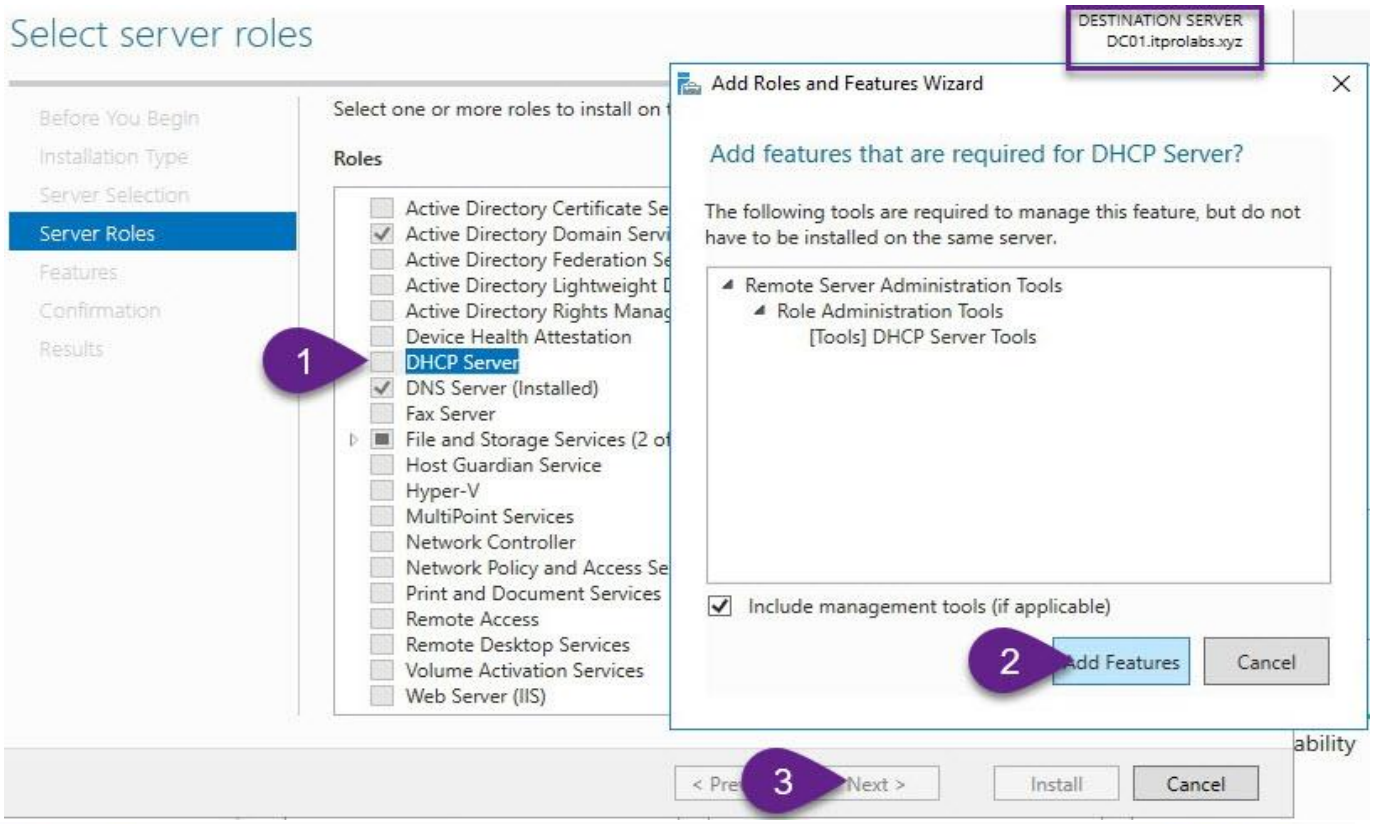
The DHCP server role can be added using the server manager by selecting 'Add Roles,' or through PowerShell, as depicted in the instructions below:

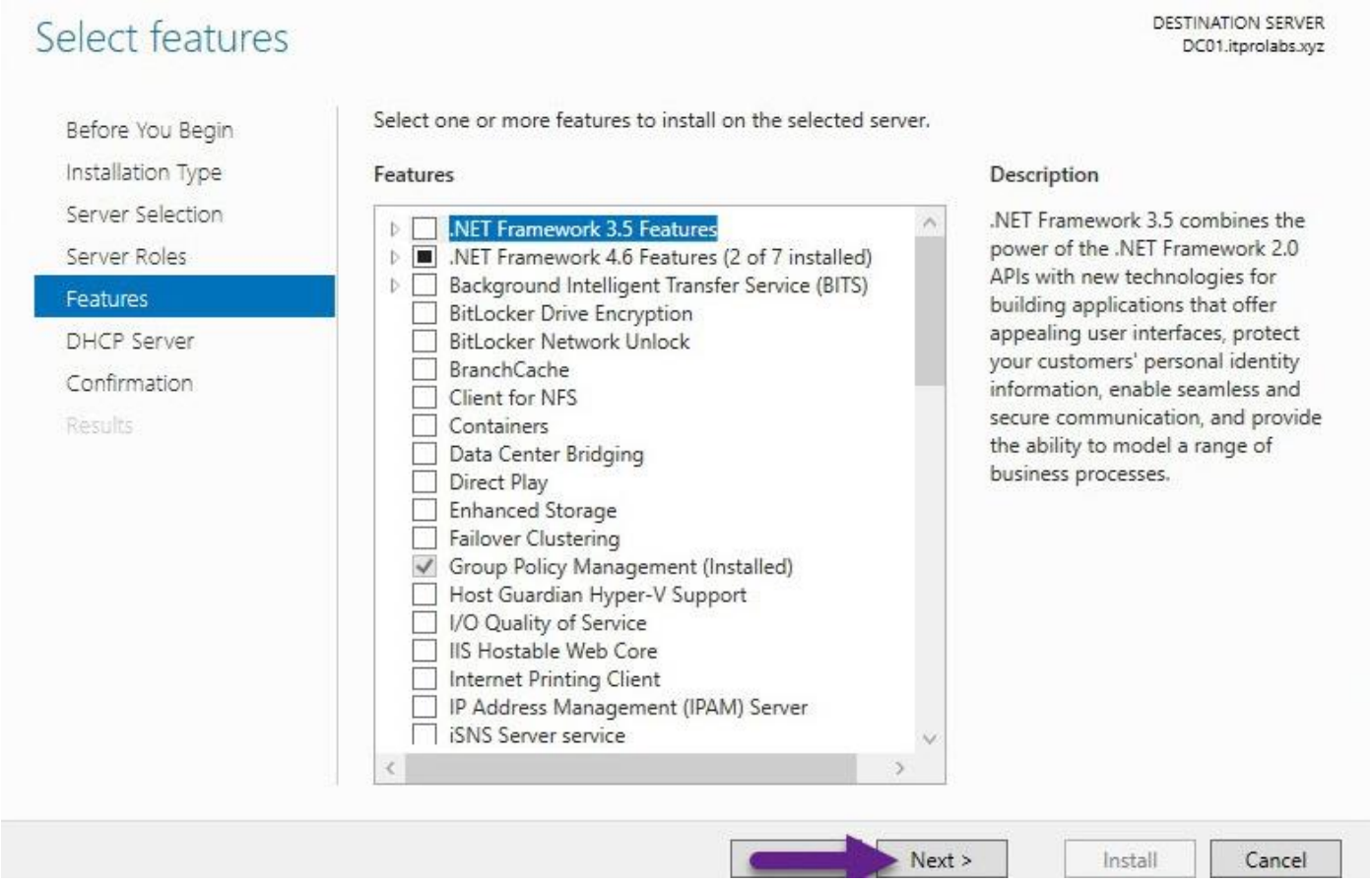
- Using PowerShell

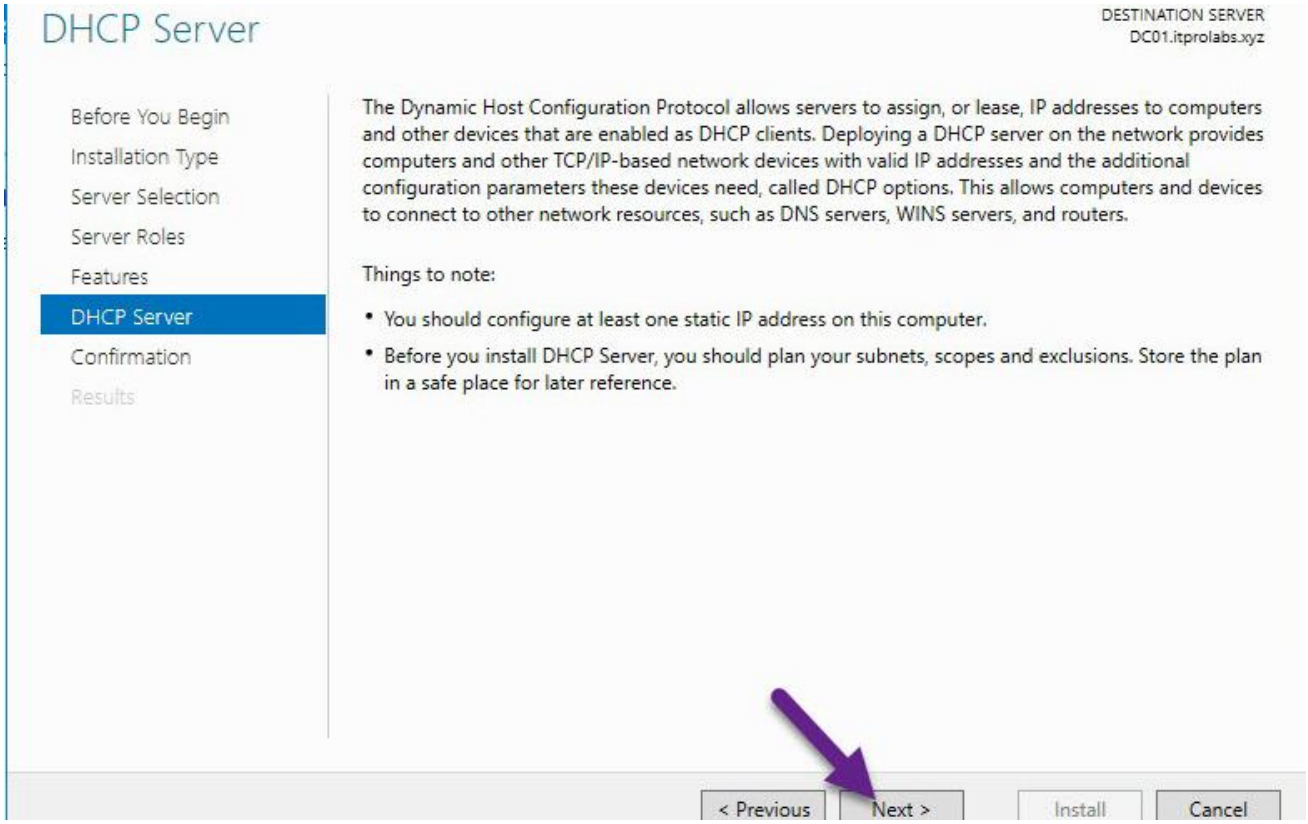


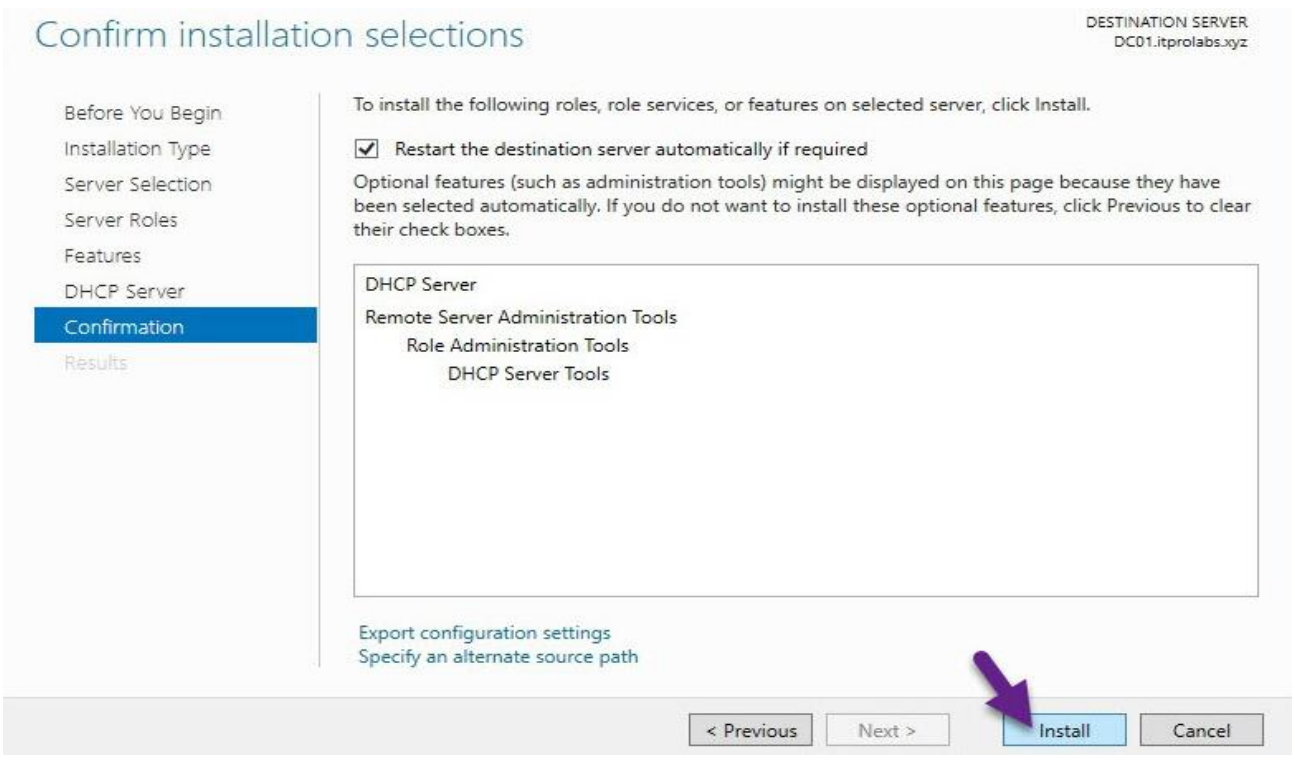
- Using Server Manager

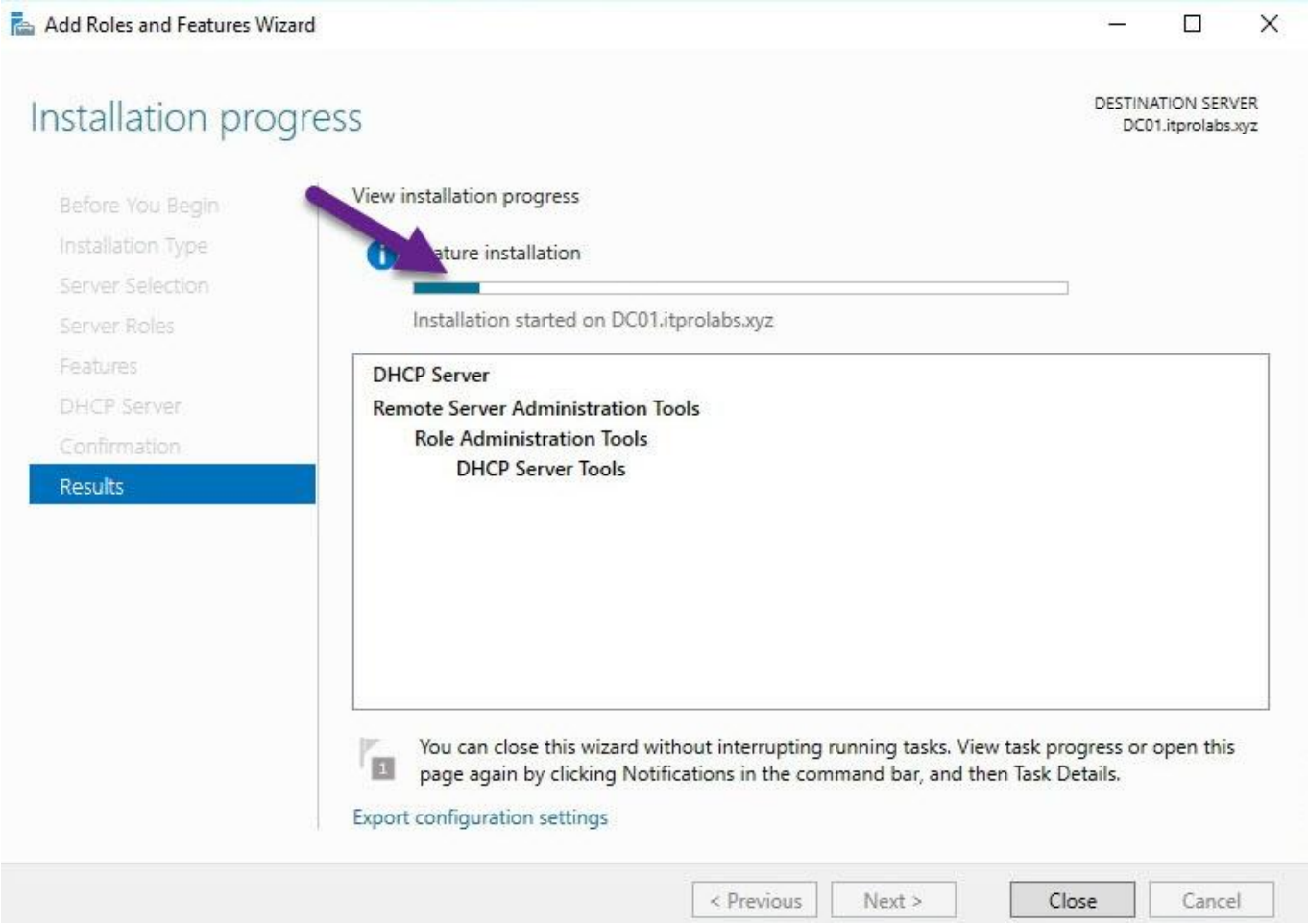



Select server roles
DESTINATION SERVER
DC01.itprolabs.xyz
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select one or more roles to install on
Roles
Active Directory Certificate Se
Active Directory Domain Servi
Active Directory Federation Se
Active Directory Lightweight D
Active Directory Rights Manag
Device Health Attestation
DHCP Server
DNS Server (Installed)
Fax Server
File and Storage Services (2 of
Host Guardian Service
Hyper-V
MultiPoint Services
Network Controller
Network Policy and Access Se
Print and Document Services
Remote Access
Remote Desktop Services
Volume Activation Services
Web Server (IIS)
1
Add Roles and Features Wizard
Add features that are required for DHCP Server?
The following tools are required to manage this feature, but do not have to be installed on the same server.
Remote Server Administration Tools
Role Administration Tools
[Tools] DHCP Server Tools
Include management tools (if applicable)
2
Add Features
Cancel
ability
< Pre
3
Next >
Install
Cancel

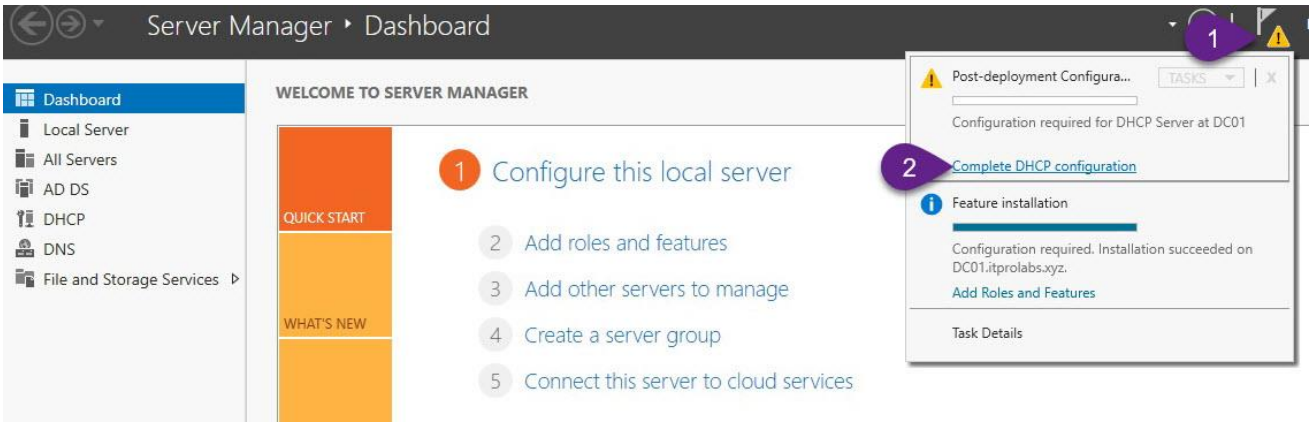

Select features
DESTINATION SERVER
DC01.itprolabs.xyz
Before You Begin
Installation Type
Server Selection
Server Roles
Features
DHCP Server
Confirmation
Results
Select one or more features to install on the selected server.
Features
.NET Framework 3.5 Features
.NET Framework 4.6 Features (2 of 7 installed)
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
Group Policy Management (Installed)
Host Guardian Hyper-V Support
I/O Quality of Service
IIS Hostable Web Core
Internet Printing Client
IP Address Management (IPAM) Server
iSNS Server service
Description
.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.
Next >
Install
Cancel


DHCP Server
DESTINATION SERVER
DC01.itprolabs.xyz
Before You Begin
Installation Type
Server Selection
Server Roles
Features
DHCP Server
Confirmation
Results
The Dynamic Host Configuration Protocol allows servers to assign, or lease, IP addresses to computers and other devices that are enabled as DHCP clients. Deploying a DHCP server on the network provides computers and other TCP/IP-based network devices with valid IP addresses and the additional configuration parameters these devices need, called DHCP options. This allows computers and devices to connect to other network resources, such as DNS servers, WINS servers, and routers.
Things to note:
• You should configure at least one static IP address on this computer.
• Before you install DHCP Server, you should plan your subnets, scopes and exclusions. Store the plan in a safe place for later reference.
< Previous
Next >
Install
Cancel


Confirm installation selections
DESTINATION SERVER
DC01.itprolabs.xyz
Before You Begin
Installation Type
Server Selection
Server Roles
Features
DHCP Server
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.
DHCP Server
Remote Server Administration Tools
Role Administration Tools
DHCP Server Tools
Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel

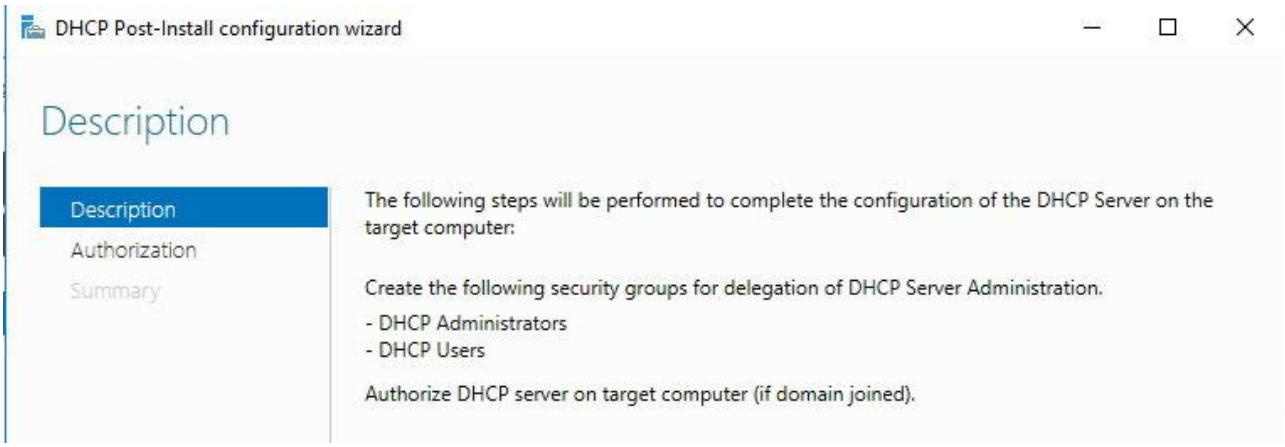


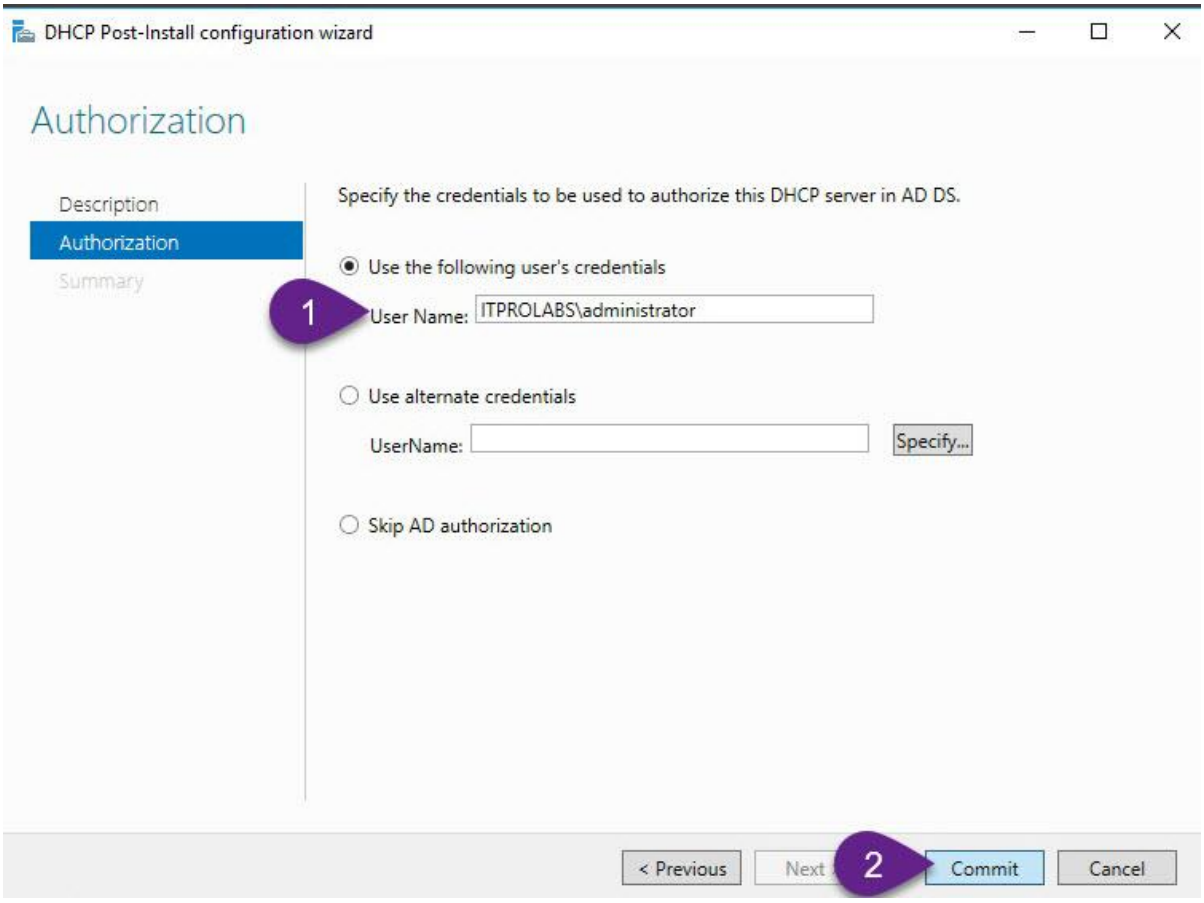
DHCP Post Installation Configuration



DHCP Authorization

In Active Directory, DHCP requires authorization to allocate IP addresses to DHCP clients, and this is carried out using a domain administrator account.

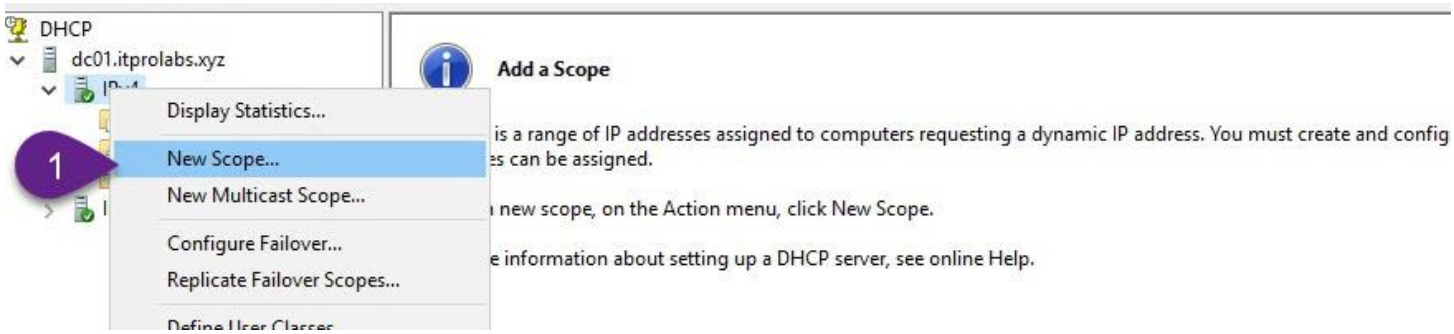


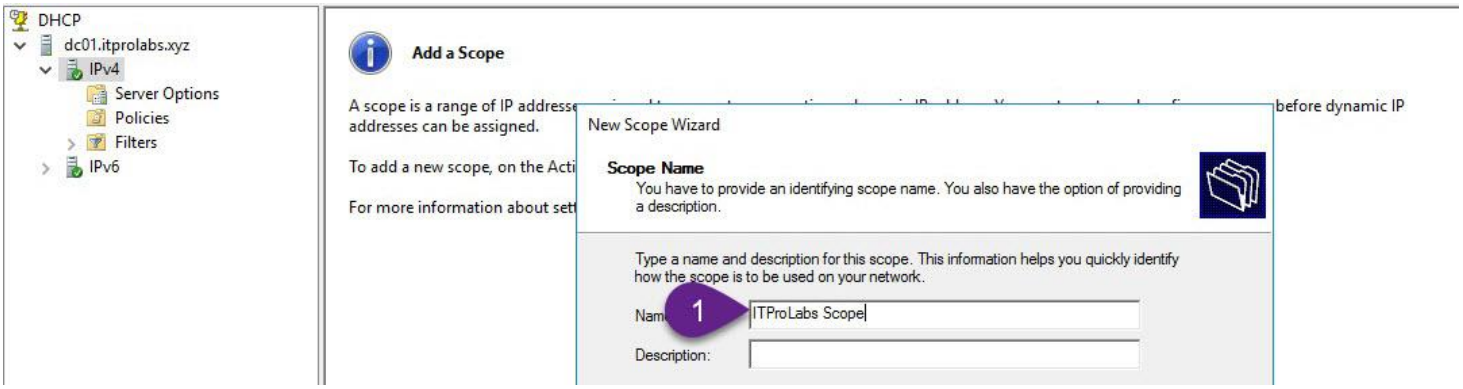


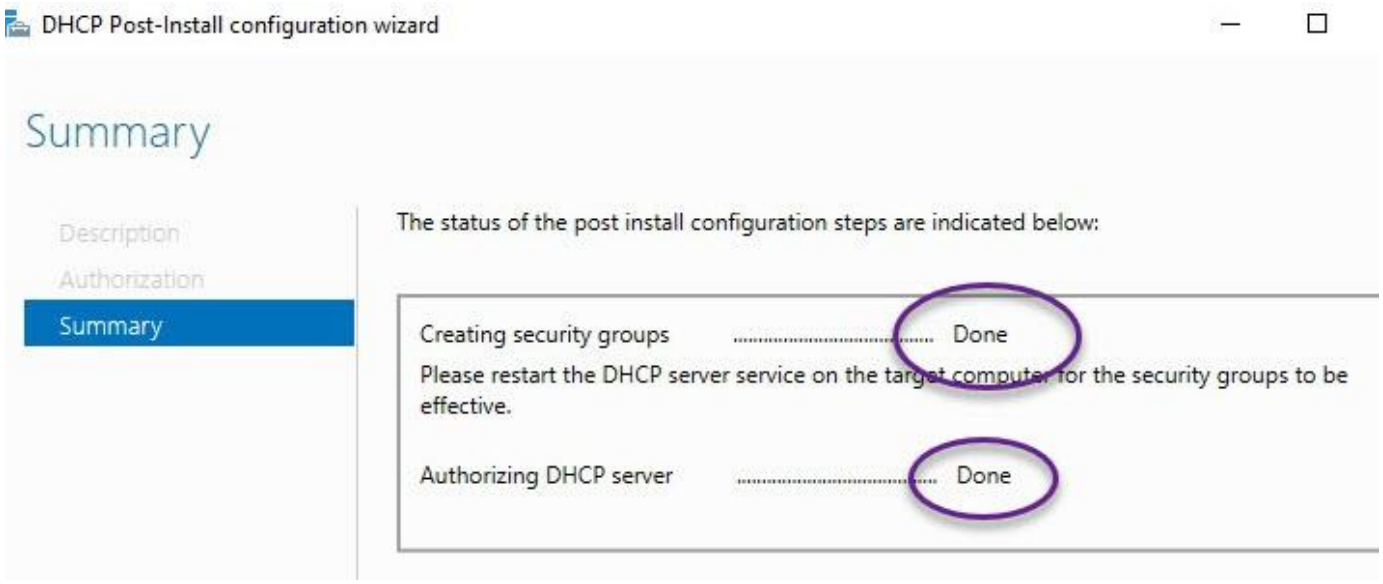
Configuring DHCP

Create and configure new scope

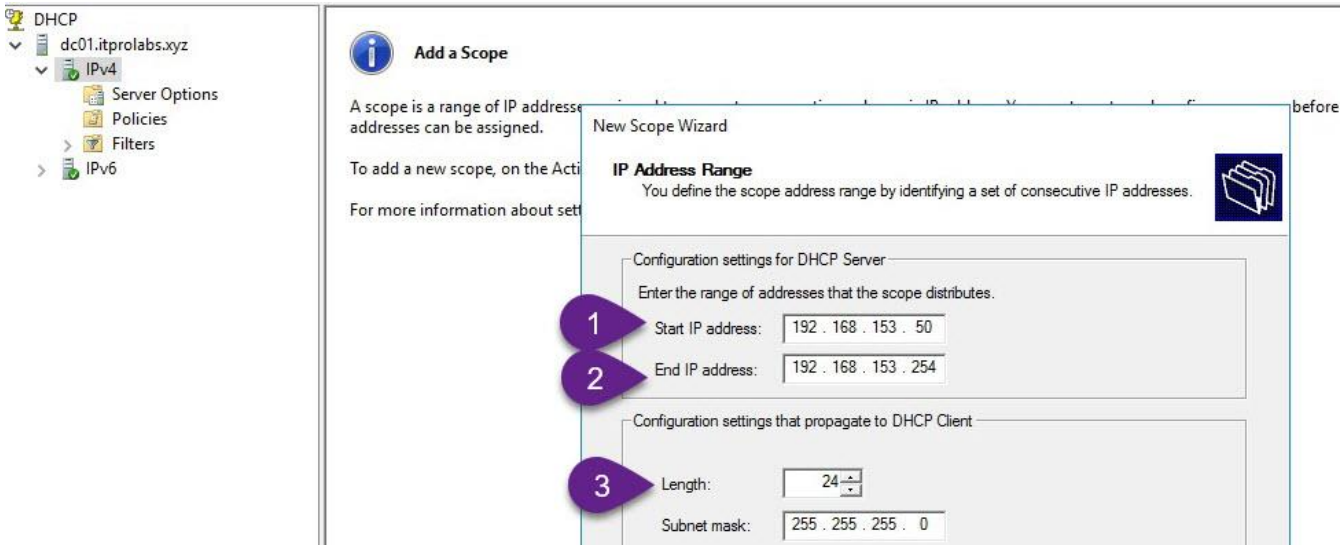
A DHCP scope represents a range of IP addresses that a DHCP server can assign to clients. To add and configure scope options, proceed as detailed in the following figures. Execute dhcpmgmt.msc to launch the DHCP management wizard.



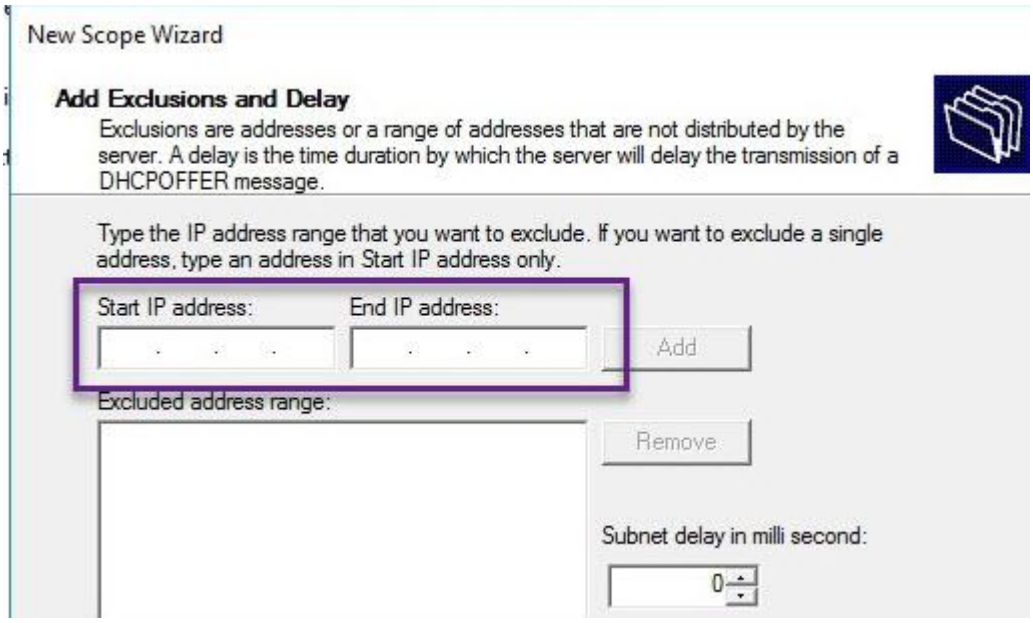




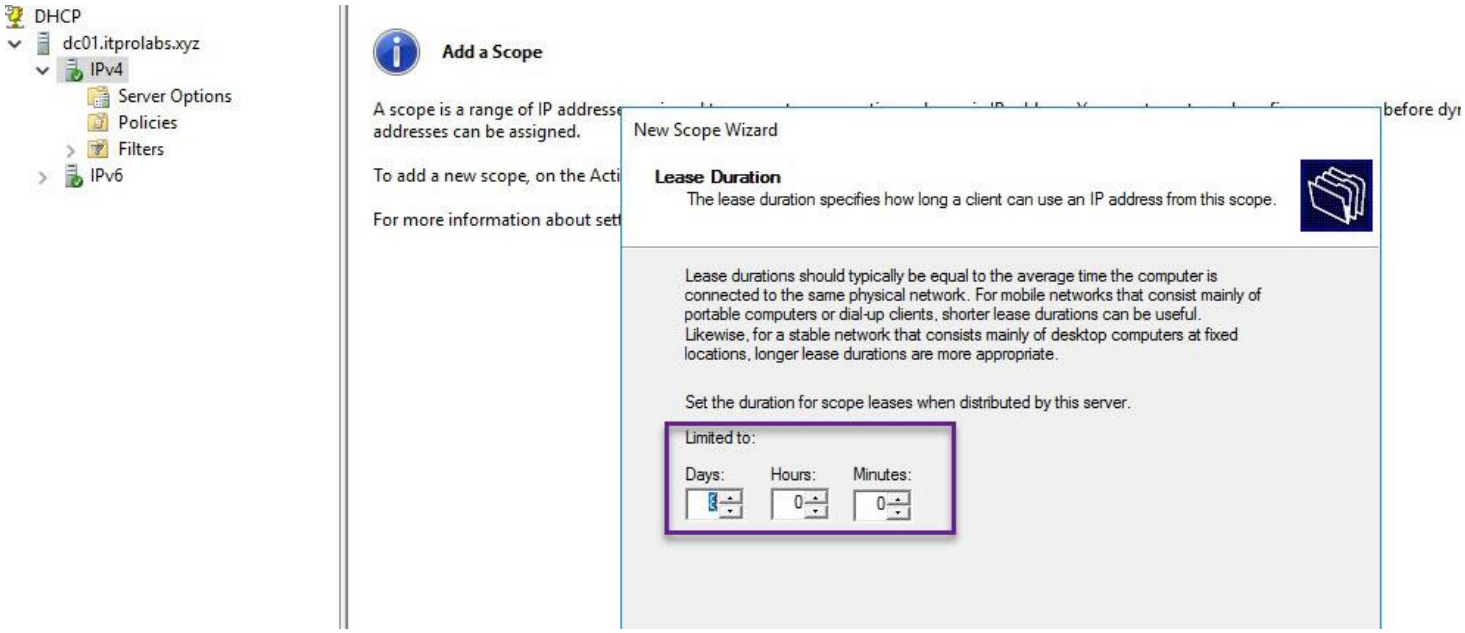
Please keep in mind that the range of IP addresses can be altered after creating the scope, but the subnet mask is not changeable.



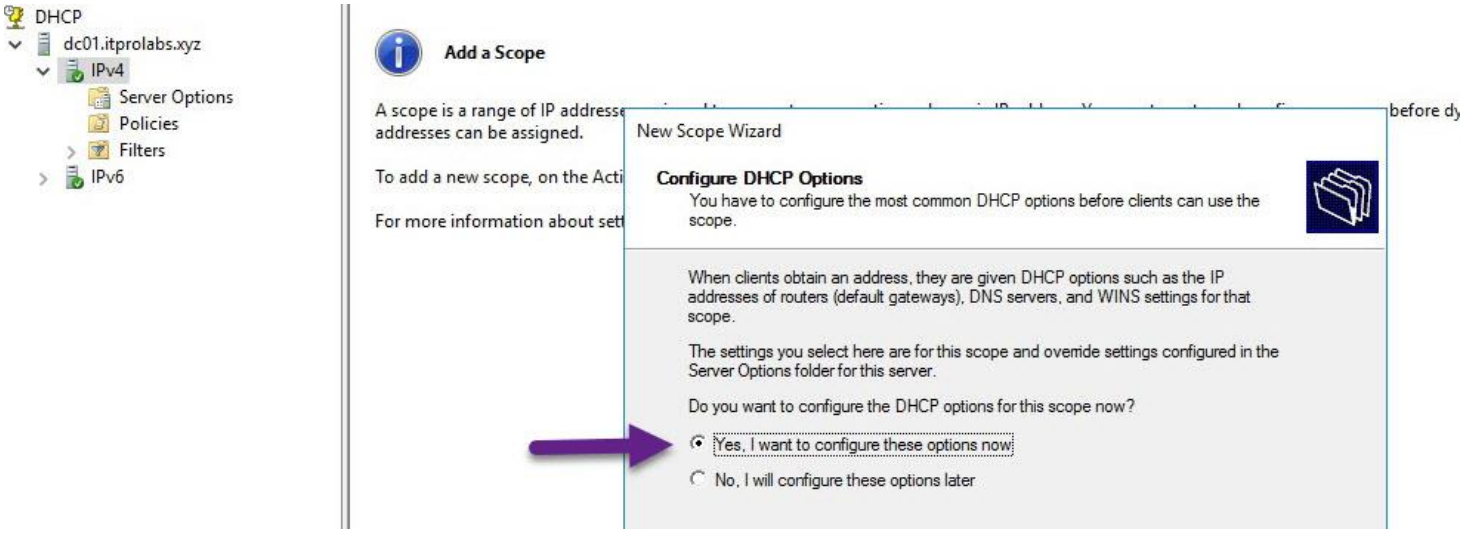
You have the option to exclude an IP address or a set of IP addresses from those available for DHCP allocation, allowing for manual assignment as static IPs.

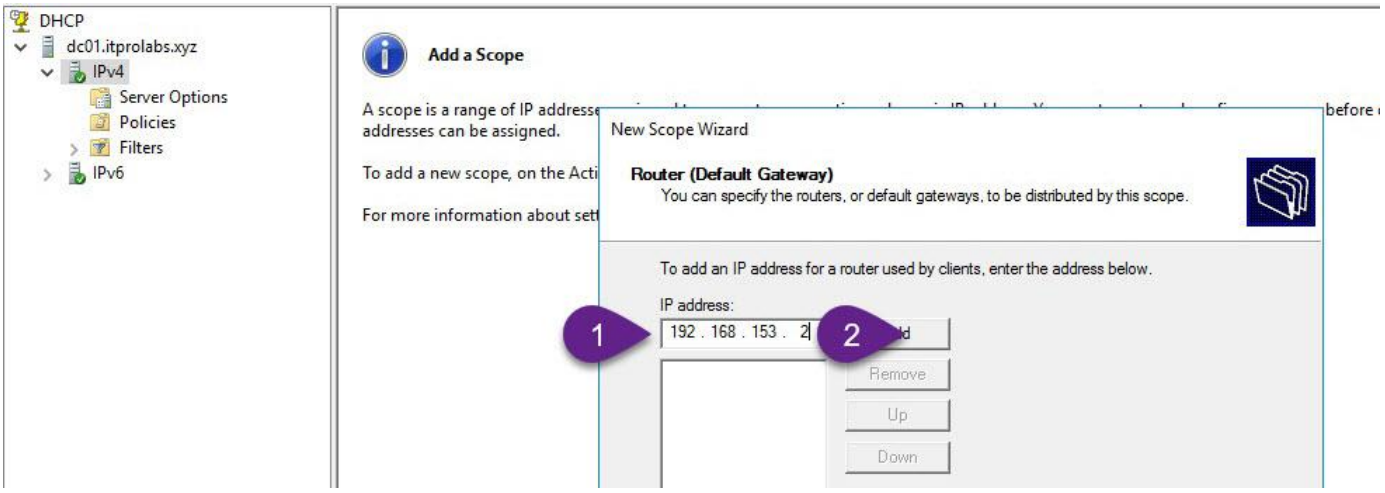


The standard setting for DHCP leases is 8 days, but you can adjust the duration to meet your needs.

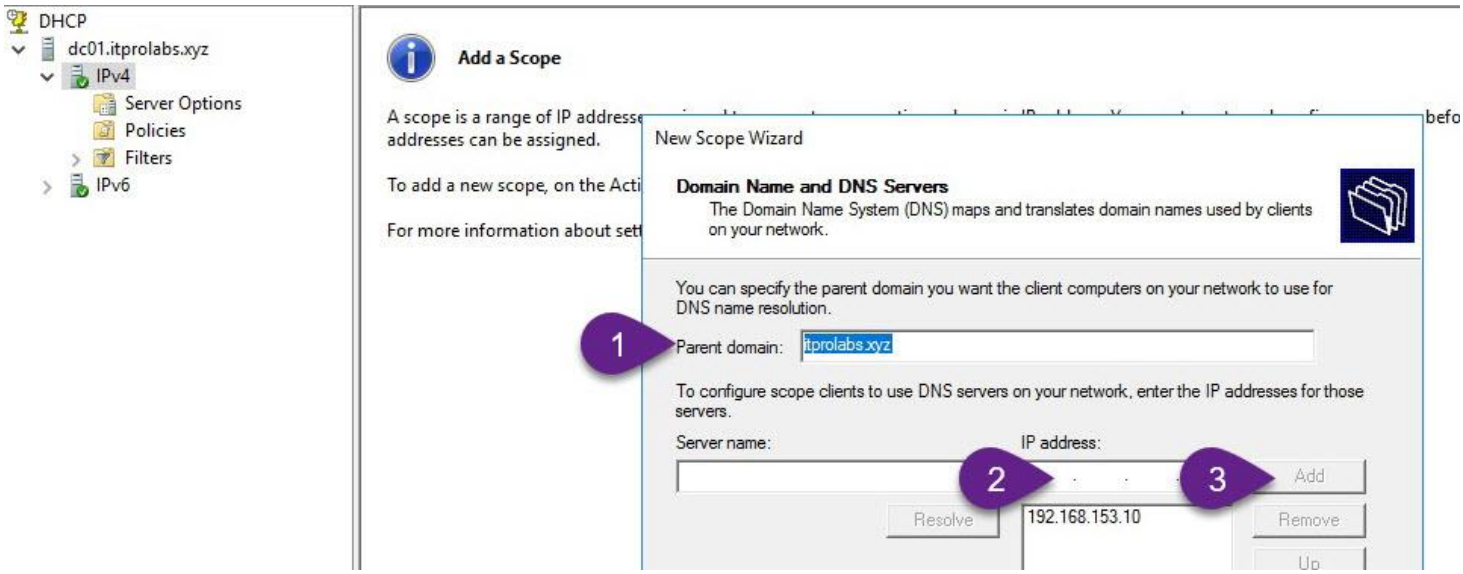


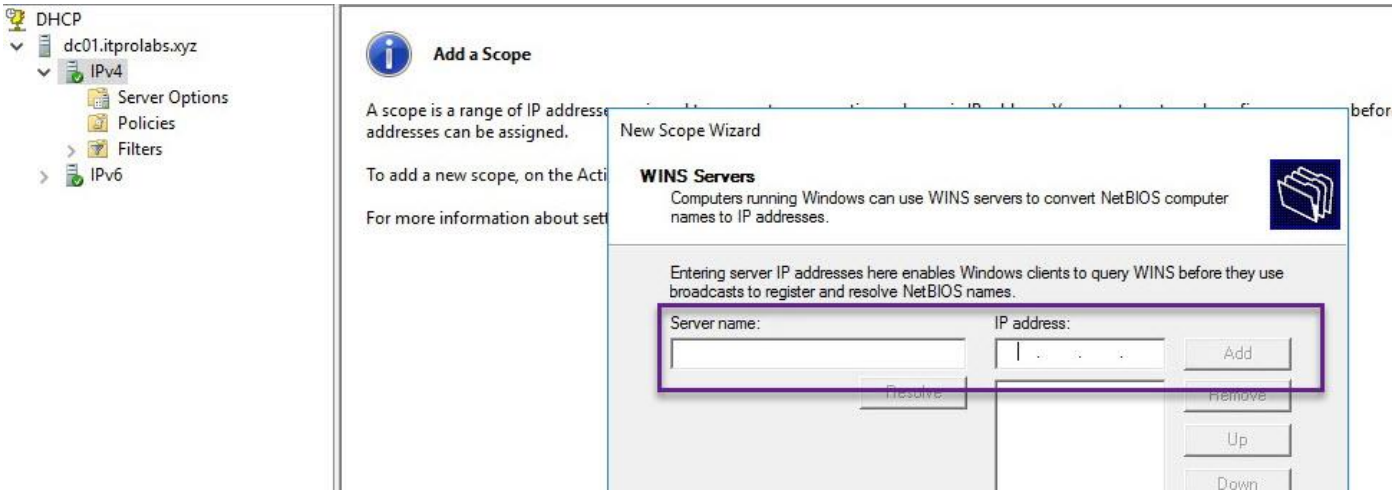
Set up the standard DHCP options now, or you have the option to configure them later.



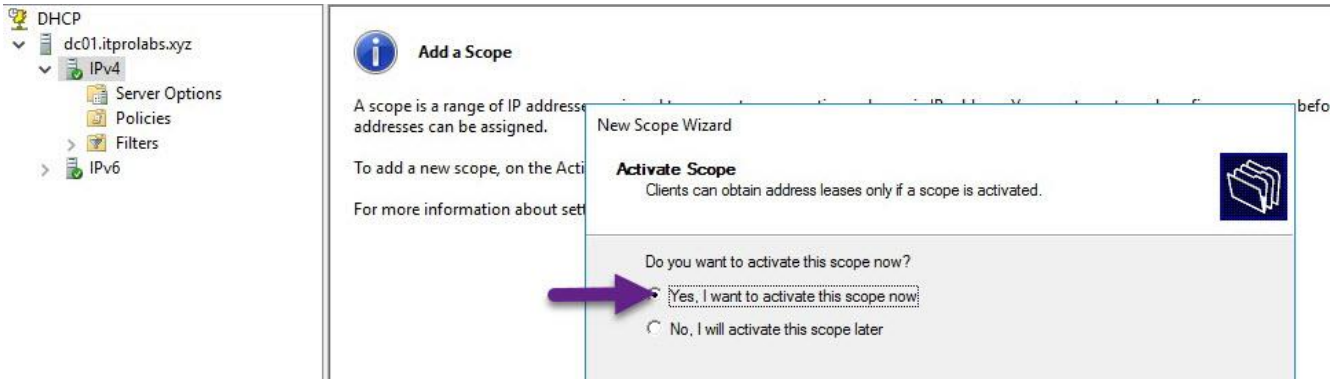


Choose a DNS server acquired via DHCP; for instance, in our setup, we have a domain (DNS Server) titled itprolabs.xyz with two DNS servers assigned the IP addresses 192.168.153.10 and 192.168.153.9.

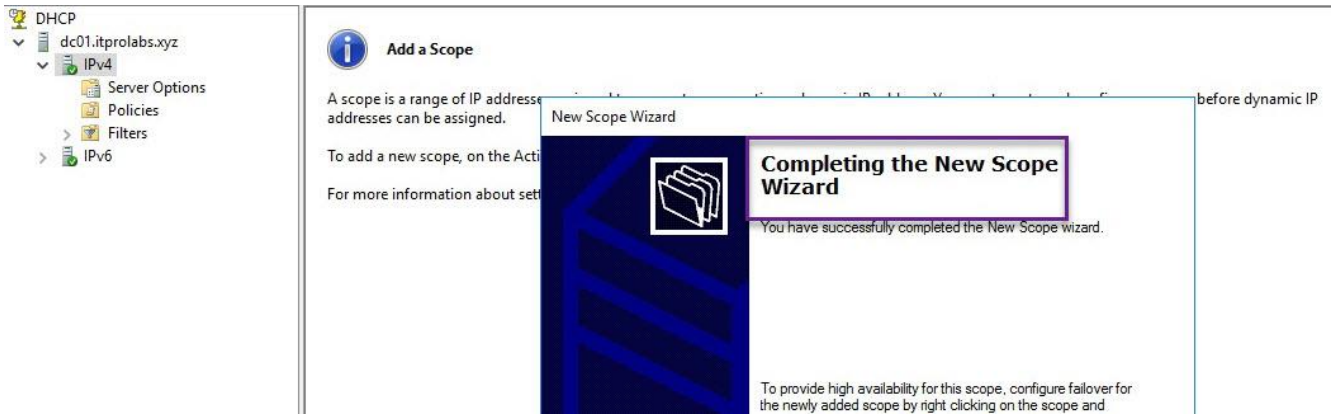




Enable your scope with the settings we've applied, or choose to enable it at another time.



Your configuration has been successfully completed, and the DHCP server is prepared to respond to client requests.



Test DHCP functionality from Windows Client (Windows 10)

How DHCP client obtain automatic IP address (DORA)

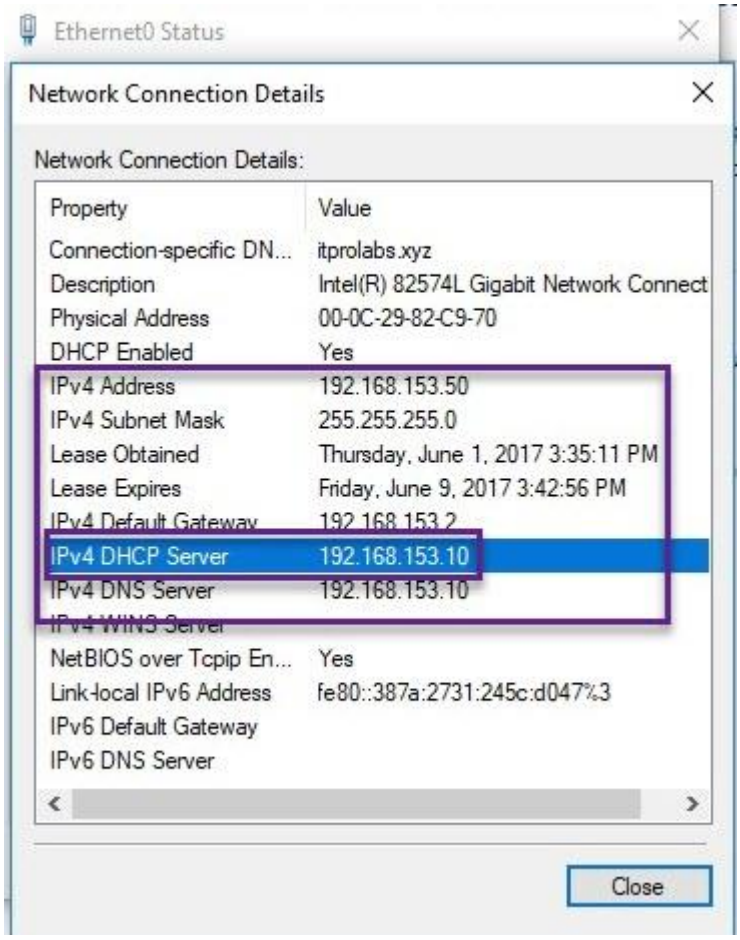
1- **DHCPDiscover, DHCP client send broadcast message to the network to detect the DHCP server.**

2- **DHCPOffer, DHCP server which receive the Discover message also send broadcast message to DHCP client that send the discover message to Offer TCP/IP configuration.**

3- **DHCPRequest, DHCP client broadcast request that contain accept for offered TCP/IP configuration.**

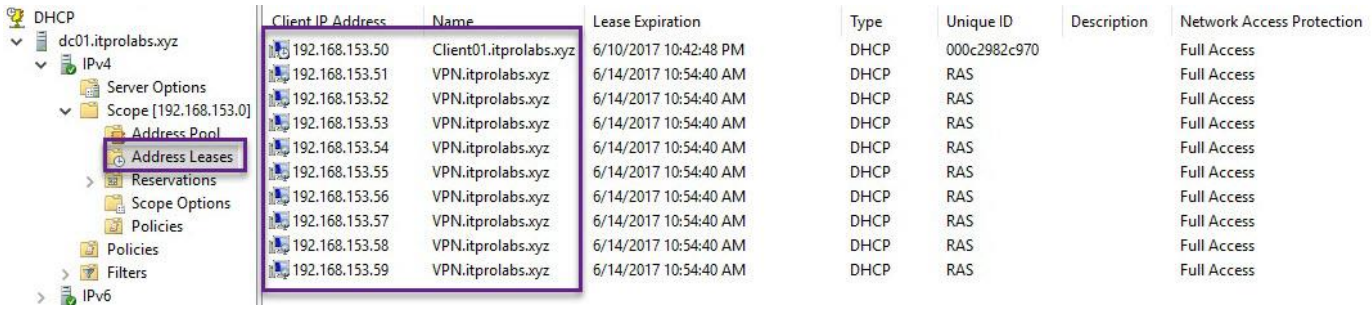
4- **DHCPACK, DHCP server replay broadcast with acknowledging client that now you have TCP/IP configuration with lease duration.**

When 50% of a lease duration has passed, the client asks the DHCP server via unicast to extend its lease. If the server is reachable, it responds with a DHCPAck to renew the lease. If there's a network issue, the client attempts to contact the server again at 87.5% of the lease time using a broadcast starting with a DHCPRequest. Should connectivity issues persist, the server may allocate the client's configuration to a different client.



DHCP Scope Options

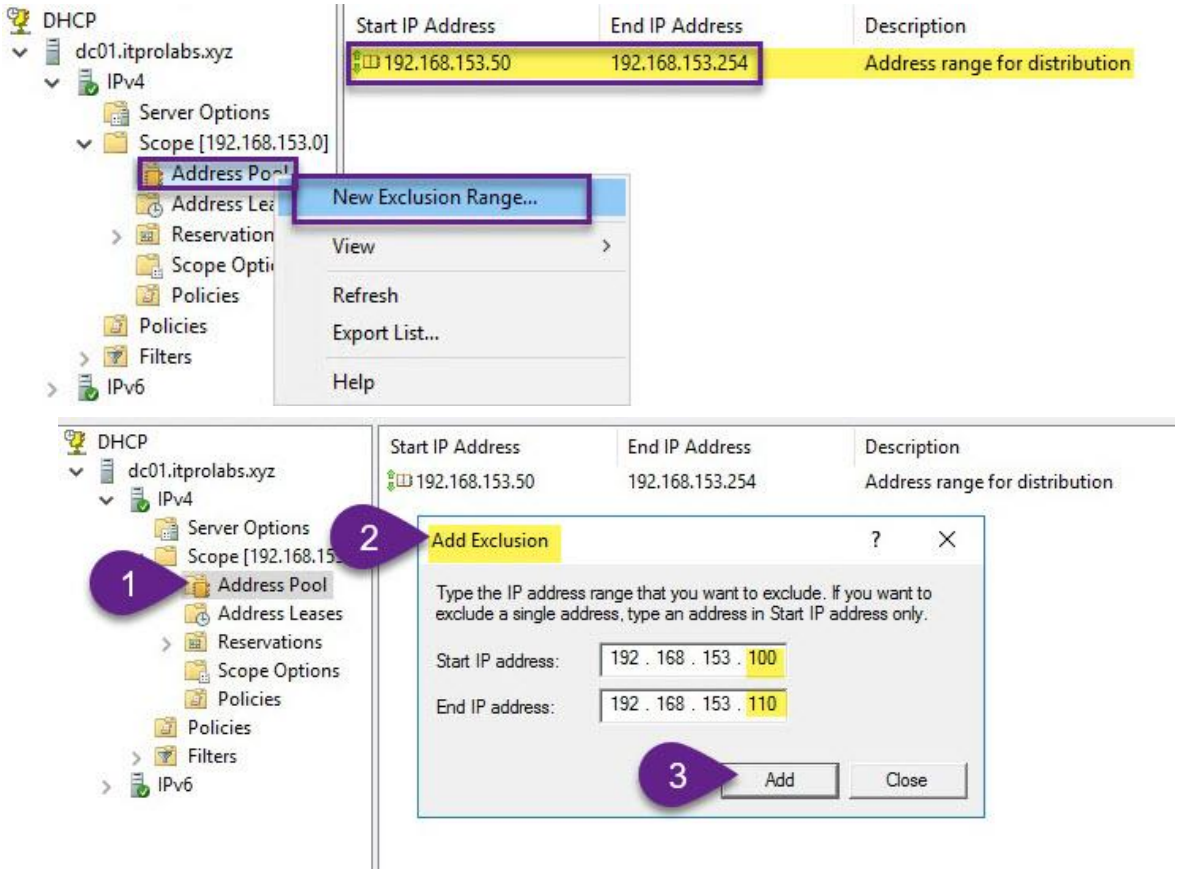
The Address Leases tab displays the computers that received TCP/IP configurations from the DHCP server, including details on when the lease expires and the MAC addresses of the clients.



Client IP Address	Name	Lease Expiration	Type	Unique ID	Description	Network Access Protection
192.168.153.50	Client01.itprolabs.xyz	6/10/2017 10:42:48 PM	DHCP	000c2982c970		Full Access
192.168.153.51	VPN.itprolabs.xyz	6/14/2017 10:54:40 AM	DHCP	RAS		Full Access
192.168.153.52	VPN.itprolabs.xyz	6/14/2017 10:54:40 AM	DHCP	RAS		Full Access
192.168.153.53	VPN.itprolabs.xyz	6/14/2017 10:54:40 AM	DHCP	RAS		Full Access
192.168.153.54	VPN.itprolabs.xyz	6/14/2017 10:54:40 AM	DHCP	RAS		Full Access
192.168.153.55	VPN.itprolabs.xyz	6/14/2017 10:54:40 AM	DHCP	RAS		Full Access
192.168.153.56	VPN.itprolabs.xyz	6/14/2017 10:54:40 AM	DHCP	RAS		Full Access
192.168.153.57	VPN.itprolabs.xyz	6/14/2017 10:54:40 AM	DHCP	RAS		Full Access
192.168.153.58	VPN.itprolabs.xyz	6/14/2017 10:54:40 AM	DHCP	RAS		Full Access
192.168.153.59	VPN.itprolabs.xyz	6/14/2017 10:54:40 AM	DHCP	RAS		Full Access

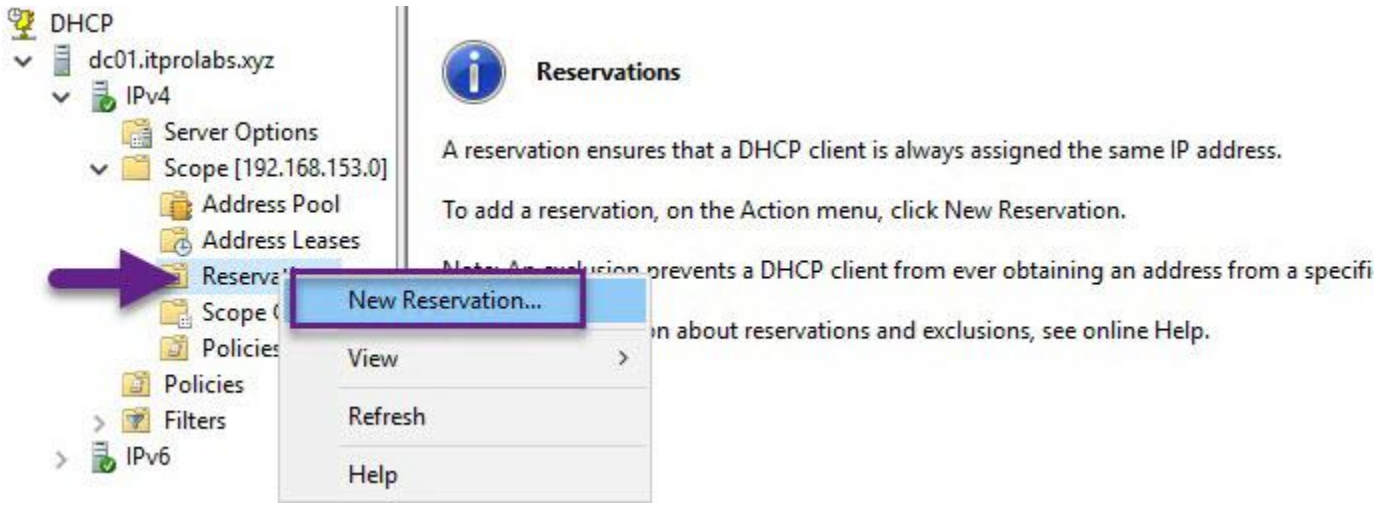
DHCP Exclusion

As previously noted, it is possible to exclude an IP or range from DHCP scope leases; this setting can be adjusted in this specific tab. Additionally, the DHCP scope range is visible within this tab, as illustrated in the figures provided below.

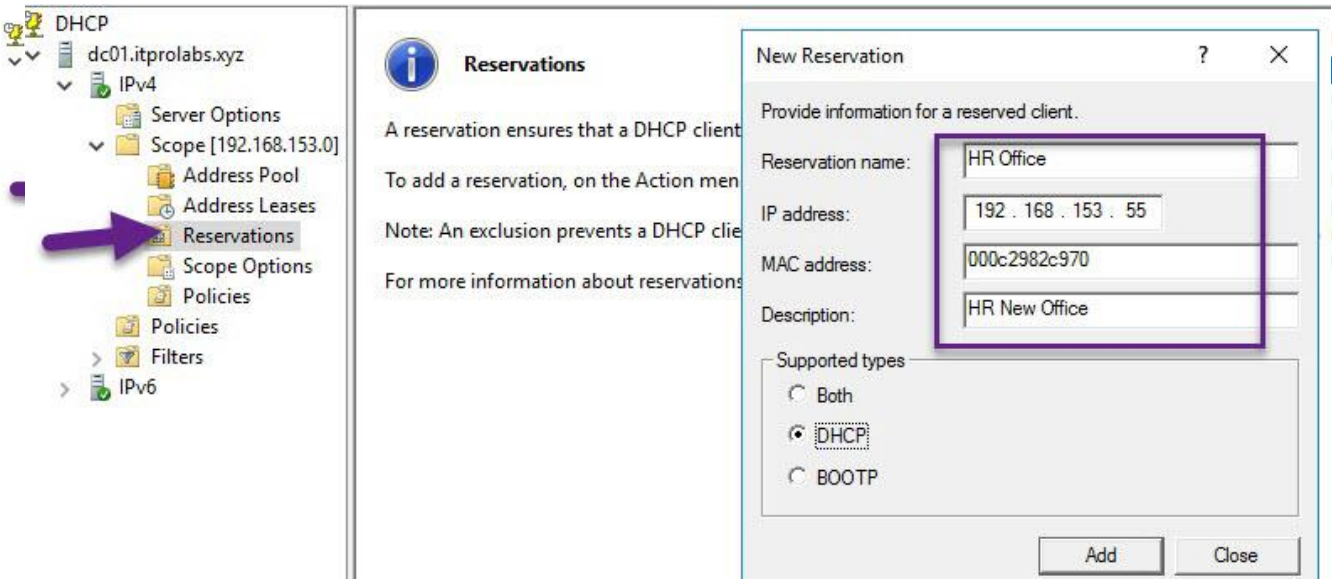


DHCP Reservation

It's possible to allocate a particular IP address to a specific client by linking it to the client's MAC address. This can be particularly useful when configuring network devices like printers, network storage, or servers.

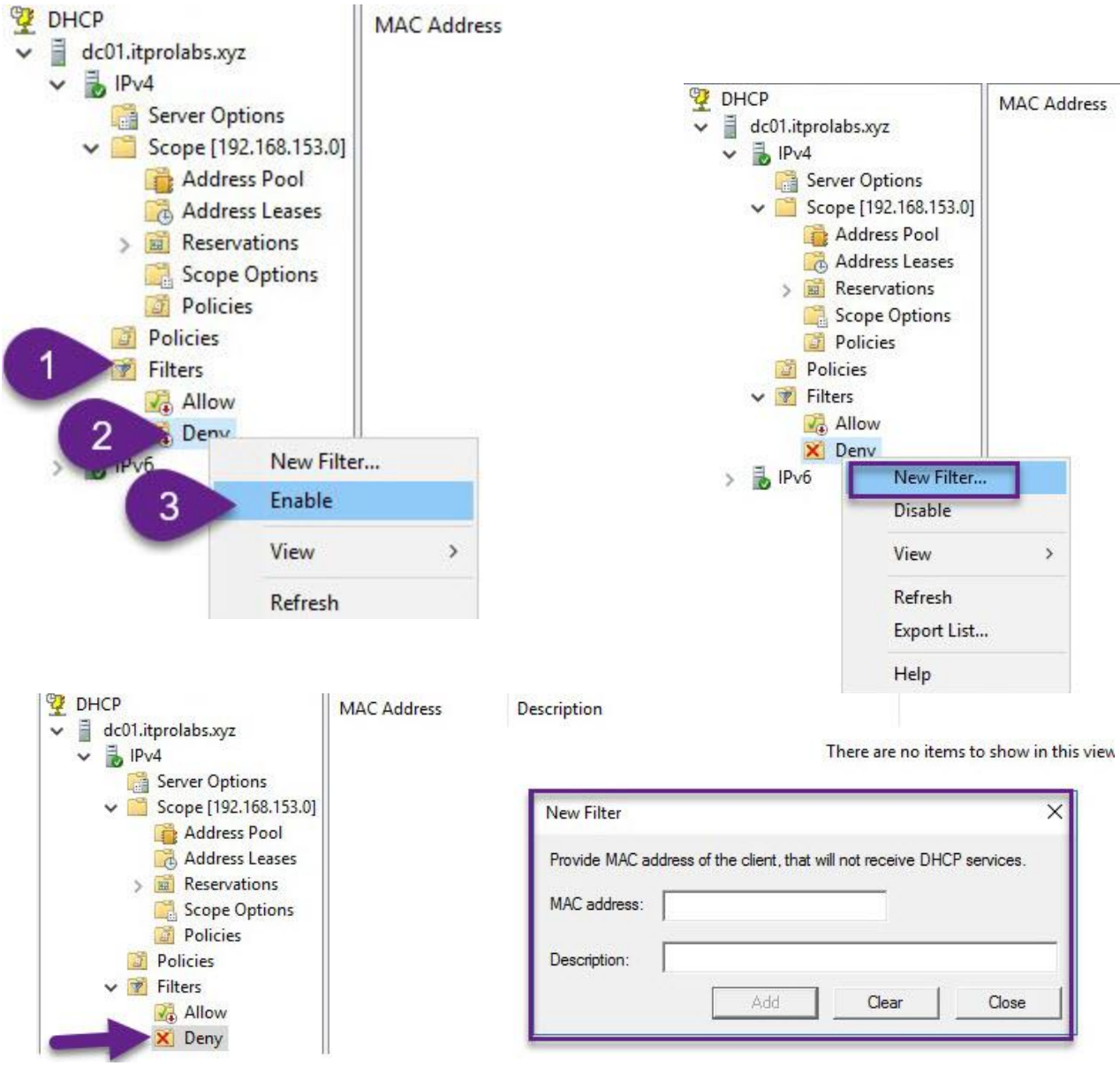


Additionally, you can assign a reserved IP address to a leased computer or network device, as depicted in the figure below.



DHCP Filter

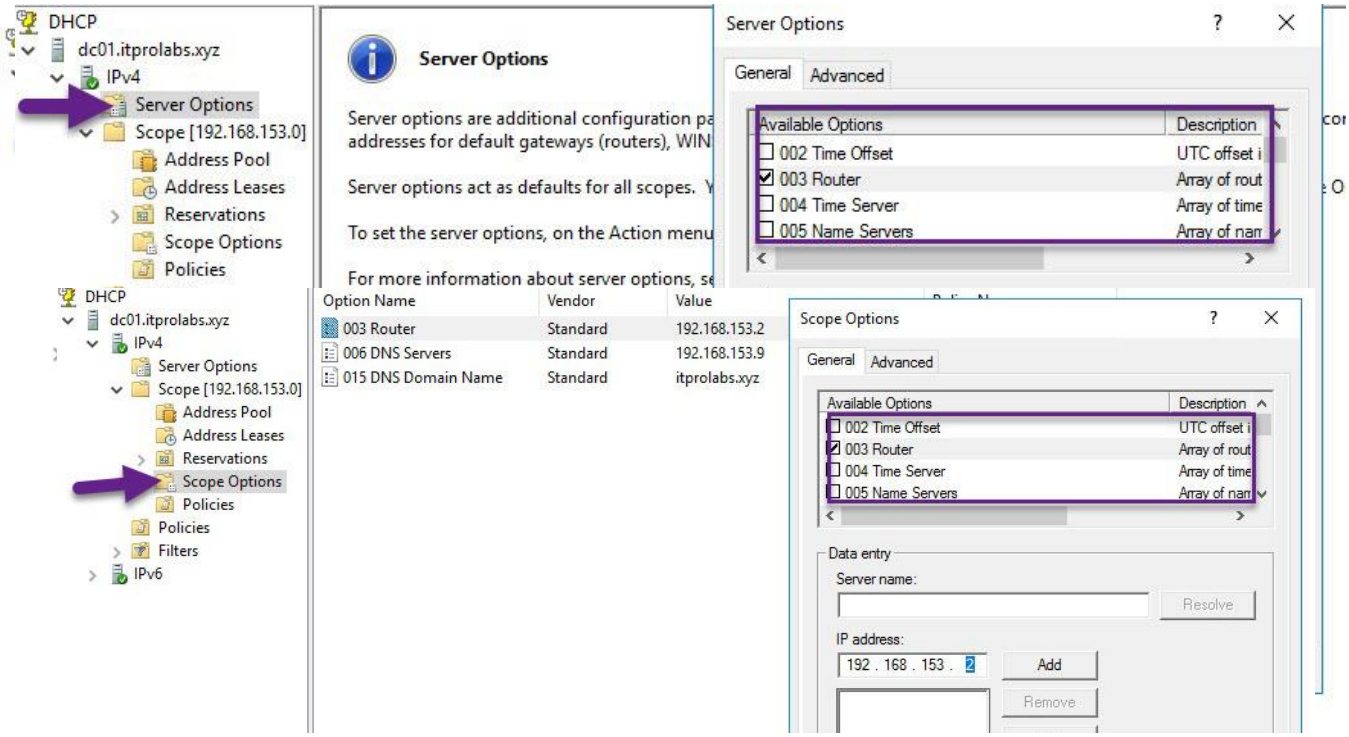
To restrict DHCP responses to certain clients, include their MAC addresses in an allow list filter. Conversely, to block DHCP requests from specific computers, add their MAC addresses to a deny list filter.



Please be aware that allow and deny lists are not active by default. If you activate the allow list, DHCP will only respond to clients on this list.

Scope and Server options

This section details how to configure or modify the scope and server settings, such as DNS and the default gateway. Scope options are specific to a particular scope, while server options apply to all scopes within the DHCP server. In our example, we will demonstrate how to modify the default gateway for both scope and server options.
Please note that if there is a discrepancy between scope and server options, the scope option prevails (it is more restrictive).

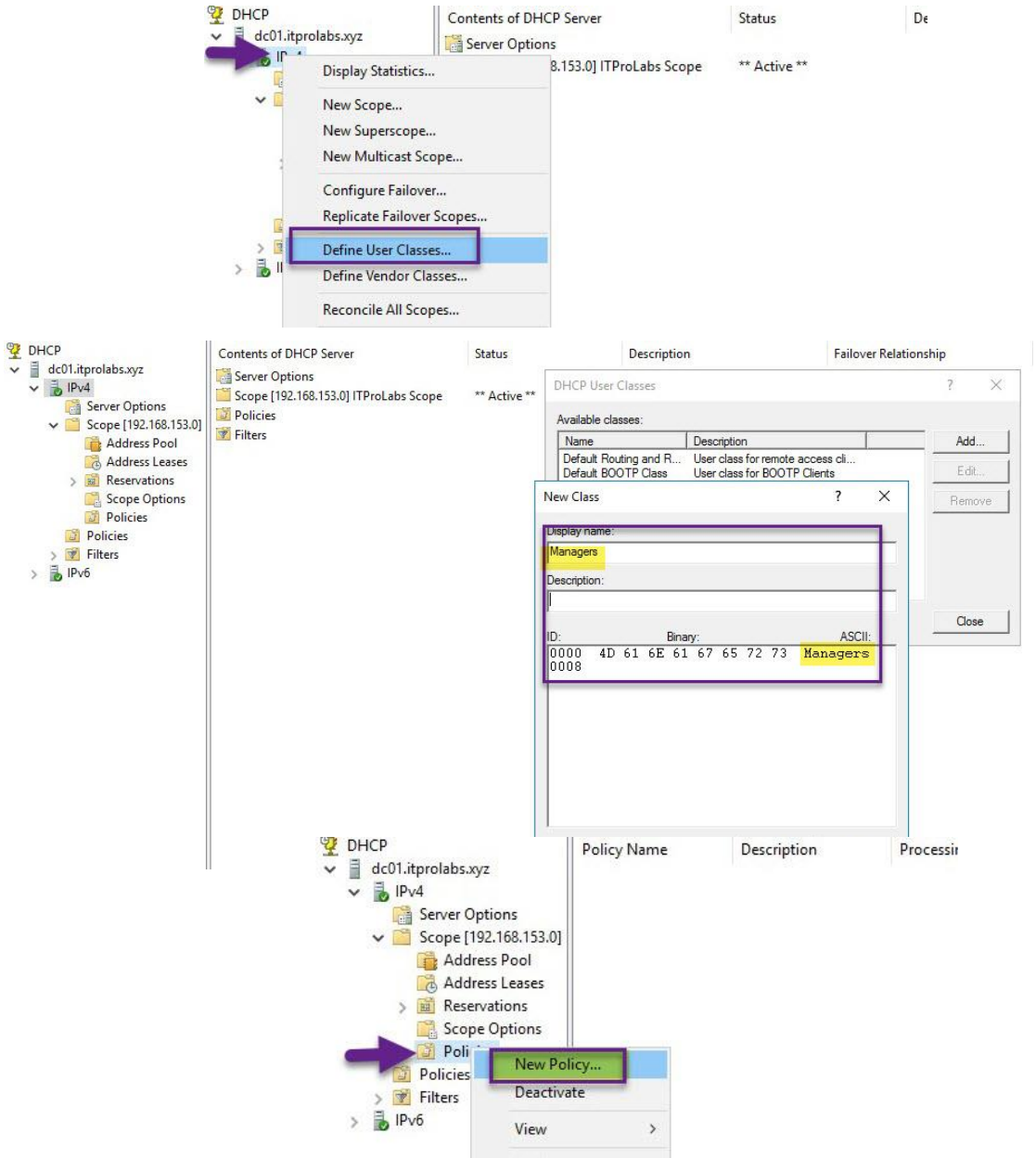


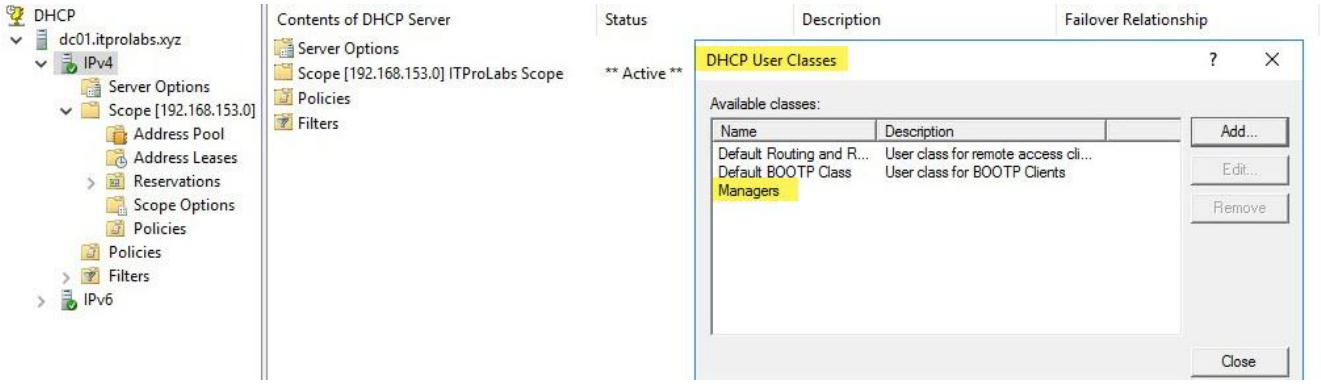
DHCP Classes

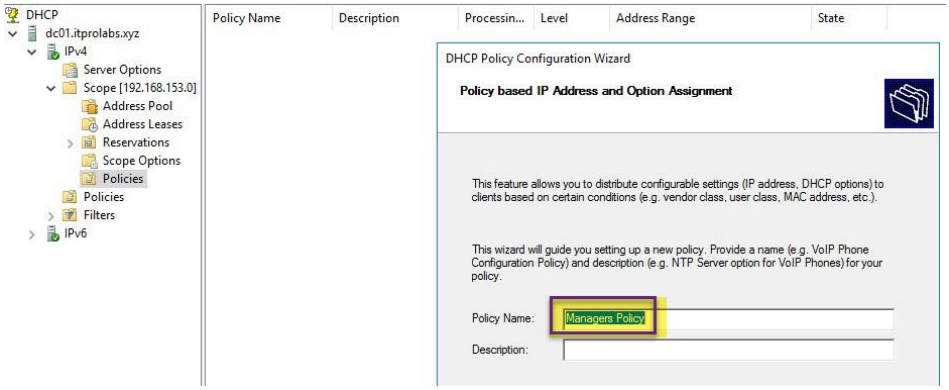
Describe a method for setting up distinct clients with unique parameters, such as DNS and Gateway. We recognize three classifications:

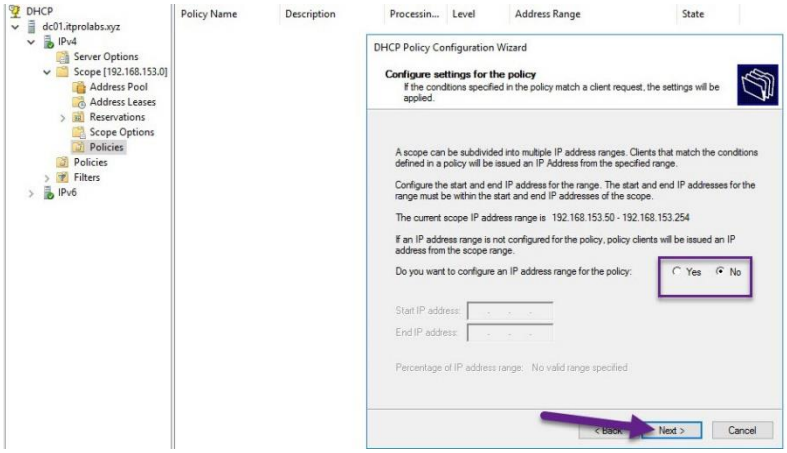
The Default Class is automatically generated upon DHCP setup, with all clients initially set as members of this class.
The Vendor Class requires manual creation and assigns specific TCP/IP settings to client computers based on the vendor—this is useful when certain options like DNS or Gateway need to be customized for machines running Windows 10, or for all devices from a manufacturer like Dell.
The User Class also needs to be manually established, and it allows distinct TCP/IP configurations for DHCP client computers.

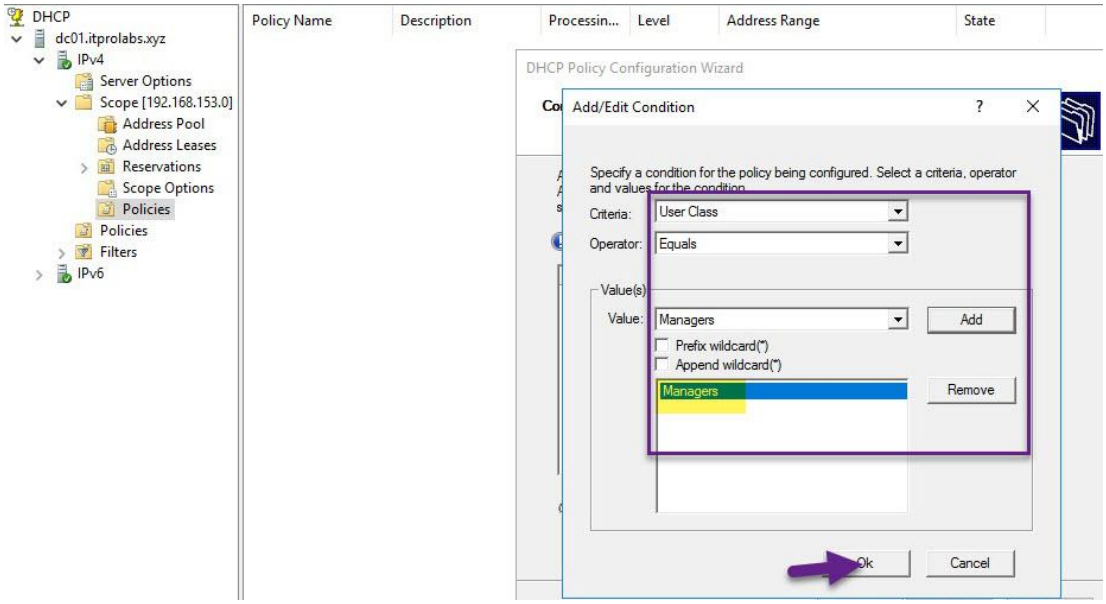
In the given example, the default DHCP DNS setting is 192.168.153.9, applied to all in the Default Class. We intend to create a DHCP User Class named 'managers' that will assign a different DNS, 192.168.153.10, to its members. To implement this, two steps are necessary: first, establishment of the DHCP User Class, followed by applying a DHCP policy that provides the alternate DNS server (192.168.153.10) specifically to the Manager class, as demonstrated in the following figures.

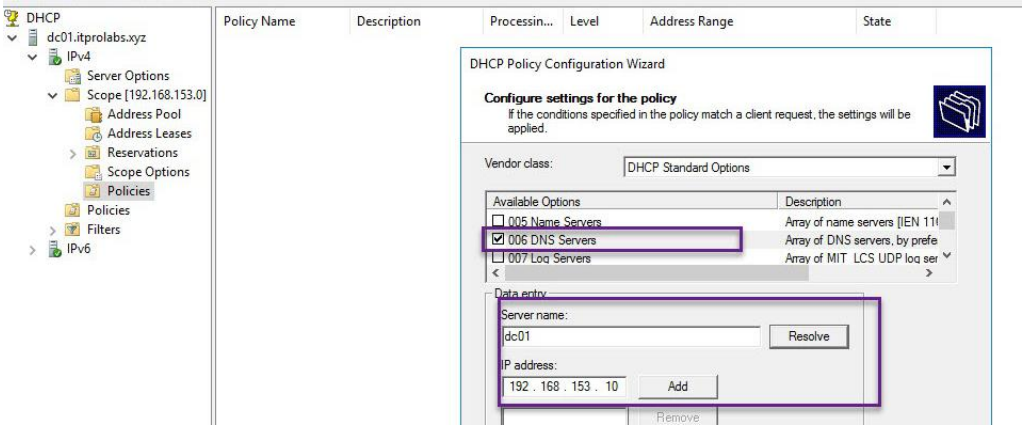


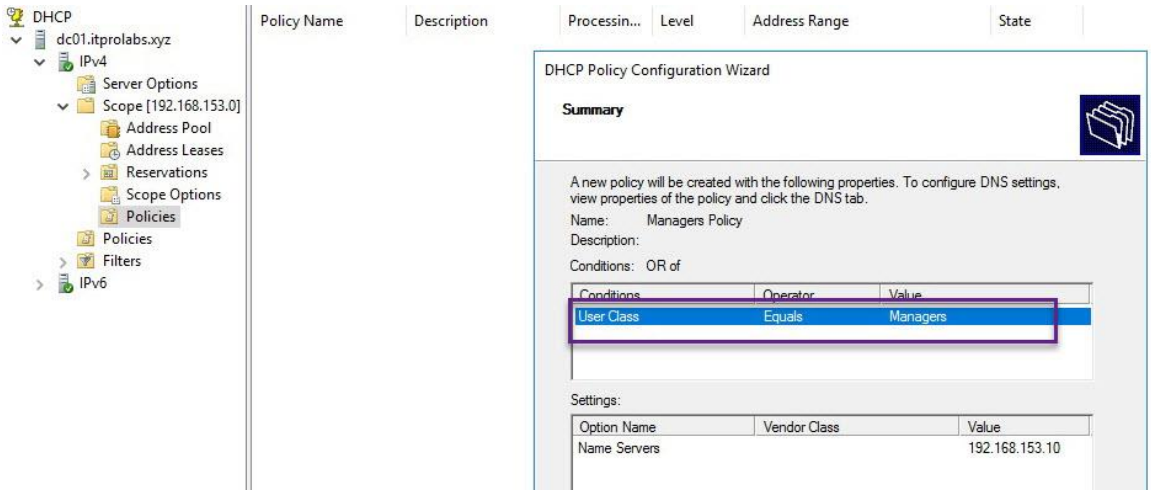

DHCP
dc01.itprolabs.xyz
IPv4
Server Options
Scope [192.168.153.0]
Address Pool
Address Leases
Reservations
Scope Options
Policies
Policies
Filters
IPv6
Contents of DHCP Server
Status
Description
Failover Relationship
Server Options
Scope [192.168.153.0] ITProLabs Scope
** Active **
Policies
Filters
DHCP User Classes
Available classes:
Name
Description
Default Routing and R...
User class for remote access cli...
Default BOOTP Class
User class for BOOTP Clients
Managers
Add...
Edit...
Remove
Close


DHCP
dc01.itprolabs.xyz
IPv4
Server Options
Scope [192.168.153.0]
Address Pool
Address Leases
Reservations
Scope Options
Policies
Policies
Filters
IPv6
Policy Name
Description
Processin...
Level
Address Range
State
DHCP Policy Configuration Wizard
Policy based IP Address and Option Assignment
This feature allows you to distribute configurable settings (IP address, DHCP options) to clients based on certain conditions (e.g. vendor class, user class, MAC address, etc.).
This wizard will guide you setting up a new policy. Provide a name (e.g. VoIP Phone Configuration Policy) and description (e.g. NTP Server option for VoIP Phones) for your policy.
Policy Name:
Managers Policy
Description:


DHCP
dc01.itprolabs.xyz
IPv4
Server Options
Scope [192.168.153.0]
Address Pool
Address Leases
Reservations
Scope Options
Policies
Policies
Filters
IPv6
Policy Name
Description
Processin...
Level
Address Range
State
DHCP Policy Configuration Wizard
Configure settings for the policy
If the conditions specified in the policy match a client request, the settings will be applied.
A scope can be subdivided into multiple IP address ranges. Clients that match the conditions defined in a policy will be issued an IP Address from the specified range.
Configure the start and end IP address for the range. The start and end IP addresses for the range must be within the start and end IP addresses of the scope.
The current scope IP address range is 192.168.153.50 - 192.168.153.254
If an IP address range is not configured for the policy, policy clients will be issued an IP address from the scope range.
Do you want to configure an IP address range for the policy:
Yes
No
Start IP address:
End IP address:
Percentage of IP address range: No valid range specified
< Back
Next >
Cancel

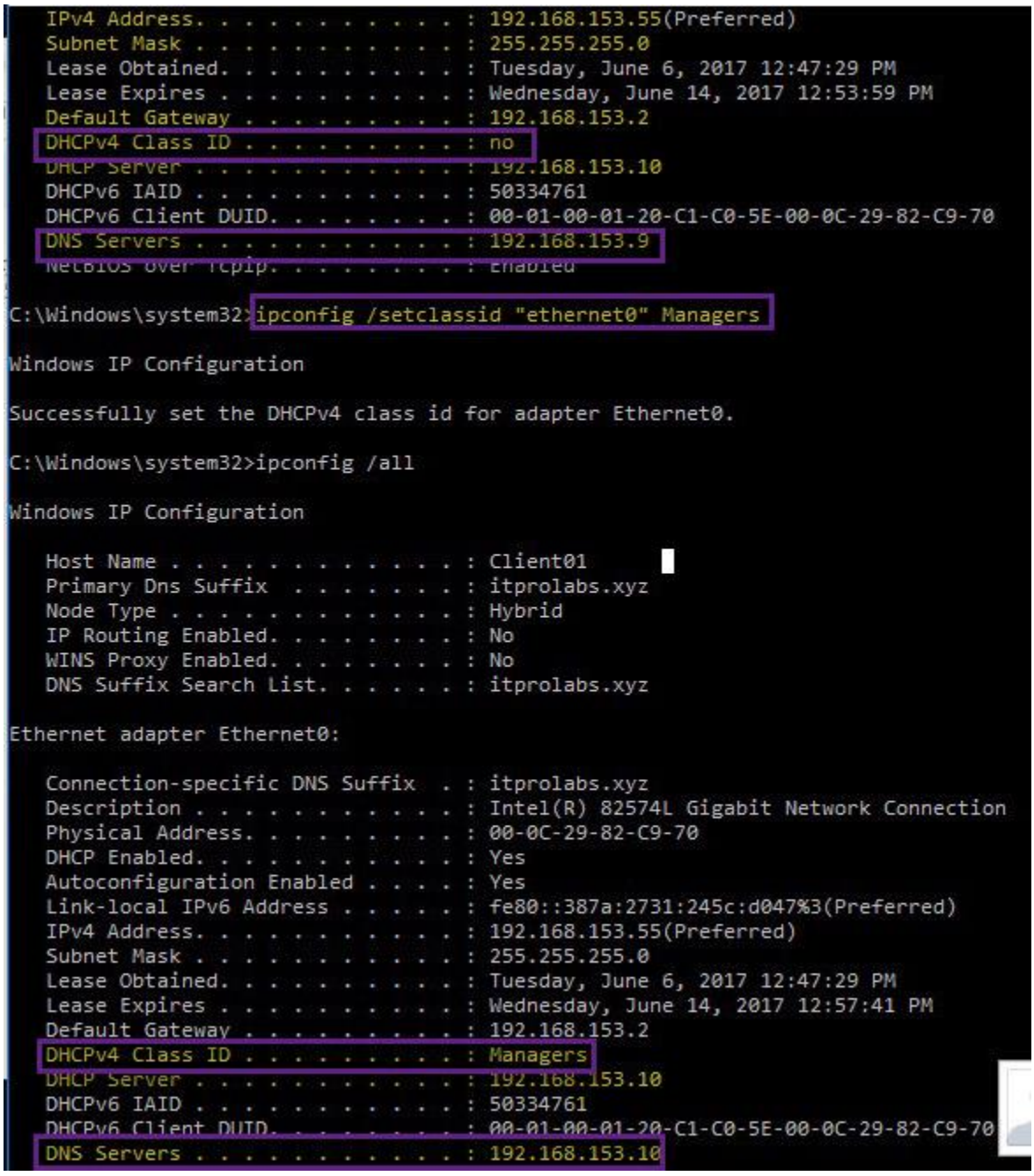

DHCP
dc01.itprolabs.xyz
IPv4
Server Options
Scope [192.168.153.0]
Address Pool
Address Leases
Reservations
Scope Options
Policies
Policies
Filters
IPv6
Policy Name
Description
Processin...
Level
Address Range
State
DHCP Policy Configuration Wizard
Add/Edit Condition
Specify a condition for the policy being configured. Select a criteria, operator and values for the condition.
Criteria:
User Class
Operator:
Equals
Value(s)
Value:
Managers
Add
Prefix wildcard(*)
Append wildcard(*)
Managers
Remove
Ok
Cancel


DHCP
dc01.itprolabs.xyz
IPv4
Server Options
Scope [192.168.153.0]
Address Pool
Address Leases
Reservations
Scope Options
Policies
Policies
Filters
IPv6
Policy Name
Description
Processin...
Level
Address Range
State
DHCP Policy Configuration Wizard
Configure settings for the policy
If the conditions specified in the policy match a client request, the settings will be applied.
Vendor class:
DHCP Standard Options
Available Options
Description
005 Name Servers
Array of name servers [IEN 11
006 DNS Servers
Array of DNS servers, by prefe
007 Log Servers
Array of MIT LCS UDP log ser
Data entry
Server name:
dc01
Resolve
IP address:
192 . 168 . 153 . 10
Add
Remove


DHCP
dc01.itprolabs.xyz
IPv4
Server Options
Scope [192.168.153.0]
Address Pool
Address Leases
Reservations
Scope Options
Policies
Policies
Filters
IPv6
Policy Name
Description
Processin...
Level
Address Range
State
DHCP Policy Configuration Wizard
Summary
A new policy will be created with the following properties. To configure DNS settings, view properties of the policy and click the DNS tab.
Name: Managers Policy
Description:
Conditions: OR of
Conditions
Operator
Value
User Class
Equals
Managers
Settings:
Option Name
Vendor Class
Value
Name Servers
192.168.153.10

Testing DHCP Class

Execute ipconfig /all on the client assigned to the default class, then reclassify the client's network interface card to the Managers group using the command ipconfig /setclassid "ethernet0" Managers. Confirm or check the changes by running ipconfig /all again. Where ethernet0 is the NIC name

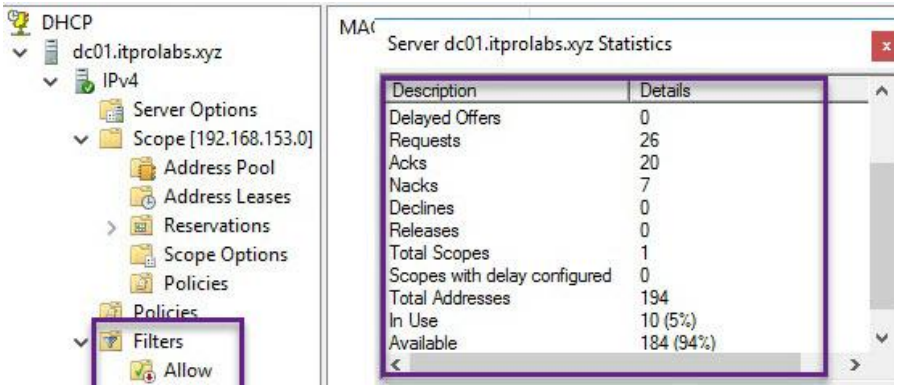


- **To revert the client to the default class, execute the command `ipconfig /setclassid "ethernet0" none` to remove the Managers class.**

```
C:\Windows\system32>ipconfig /setclassid "ethernet0" no

Windows IP Configuration

Successfully set the DHCPv4 class id for adapter Ethernet0.

C:\Windows\system32>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : Client01
   Primary Dns Suffix  . . . . . . . : itprolabs.xyz
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : itprolabs.xyz

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : itprolabs.xyz
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-0C-29-82-C9-70
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::387a:2731:245c:d047%3(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.153.55(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Tuesday, June 6, 2017 12:47:29 PM
   Lease Expires . . . . . . . . . . : Wednesday, June 14, 2017 1:02:24 PM
   Default Gateway . . . . . . . . . : 192.168.153.2
   DHCPv4 Class ID . . . . . . . . . : no
   DHCP Server . . . . . . . . . . . : 192.168.153.10
   DHCPv6 IAID . . . . . . . . . . . : 50334761
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-20-C1-C0-5E-00-0C-29-82-C9-70
   DNS Servers . . . . . . . . . . . : 192.168.153.9
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

DHCP Statistics

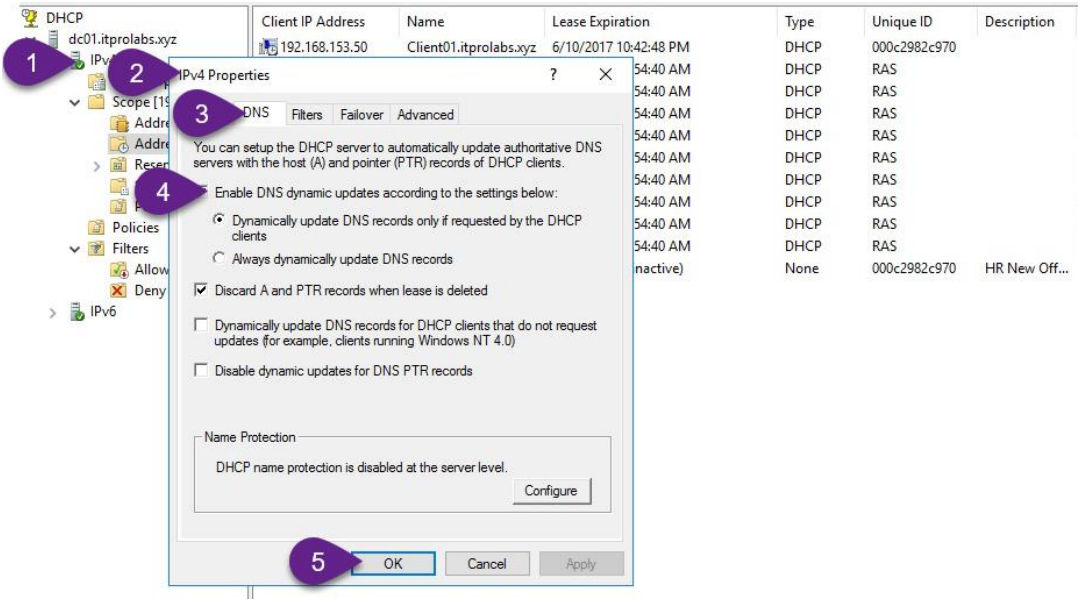
Here you can find crucial statistics such as the count of leased IP addresses and the pool of available addresses.



DHCP Advanced Options

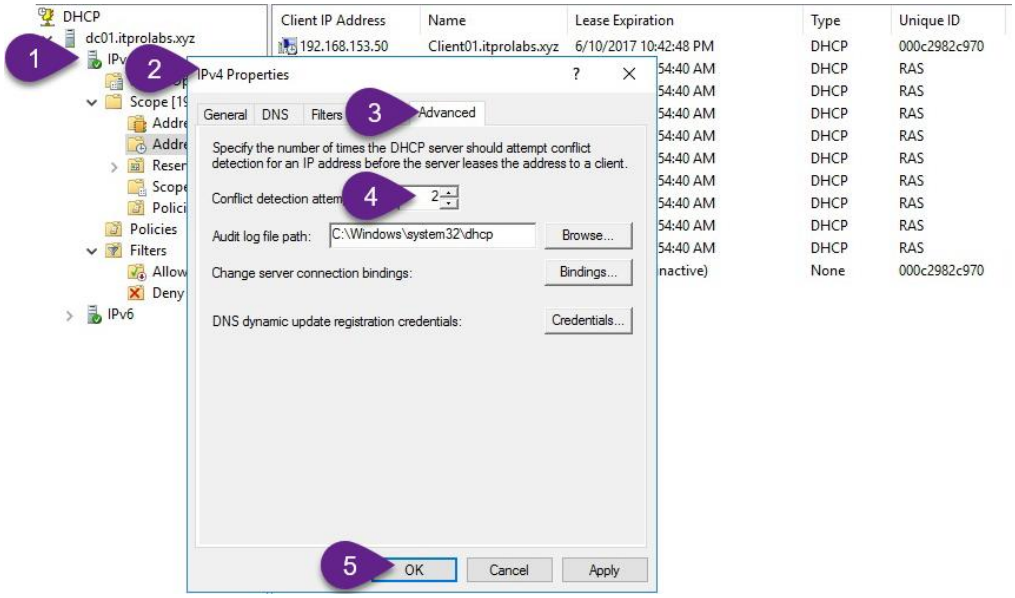
Integration with DNS

There's a feature that permits the DHCP server to create an A record in the DNS server on behalf of the client when it assigns an IP address.



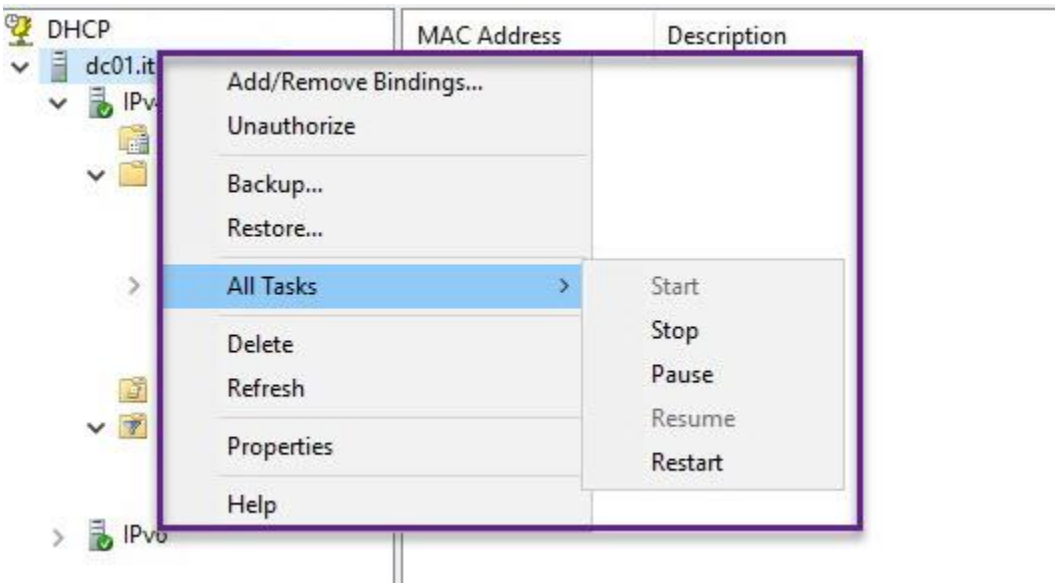
Conflict detection

A DHCP server can be configured to check for IP address conflicts before assigning them to a client.



DHCP Maintenance

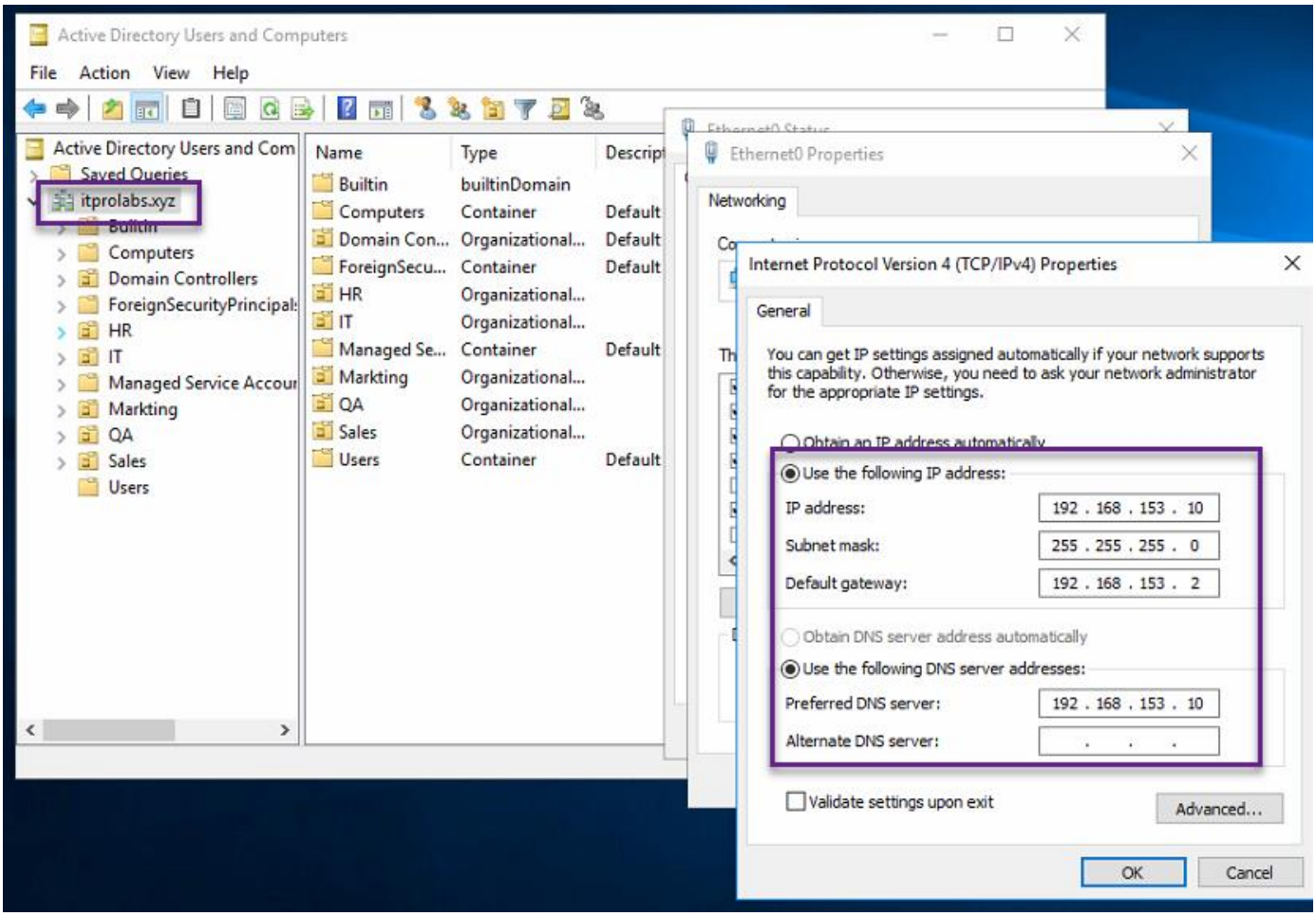
Some standard and crucial maintenance activities include backing up and restoring to a different server, as well as stopping and restarting the DHCP service, particularly when you need to unauthorize your server.



Storage

Current Environment

1. OS: Windows server 2016
2. Domain Name: ITPROLABS.XYZ
3. Domain IP: 192.168.153.10/24
4. IP Scheme: 192.168.153.0/24
5. Storage server Name: FSRM01 (test server)
6. Storage Server IP: 192.168.153.60

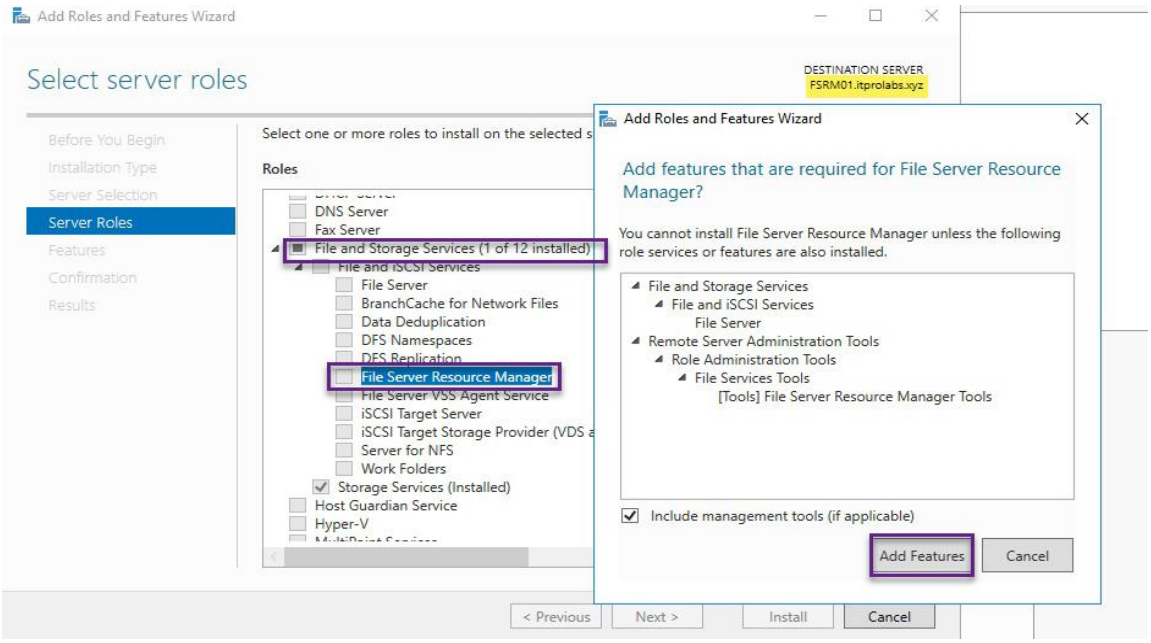


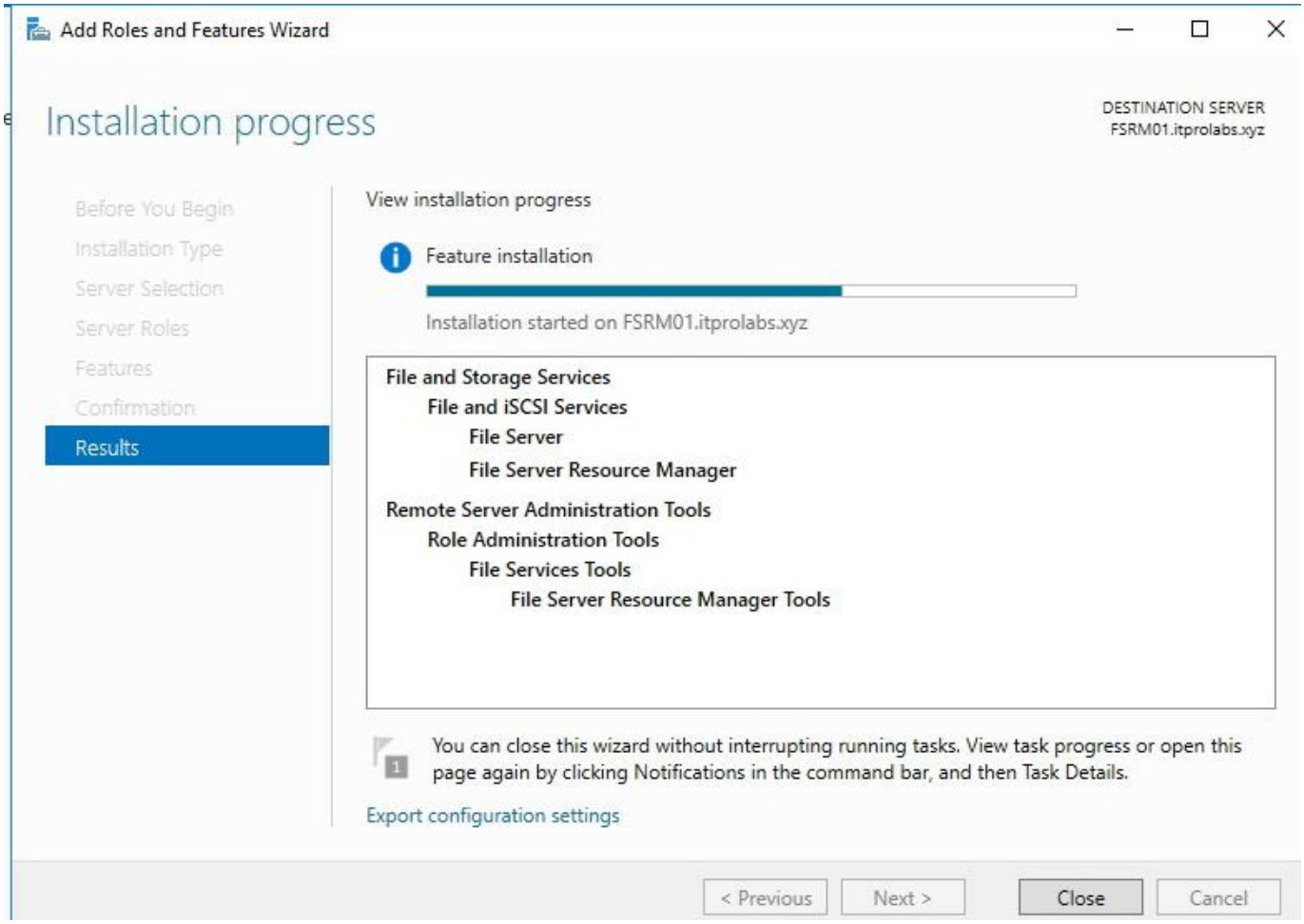
File Server Resource Manager (FSRM)

File Server Resource Manager is a suite of capabilities within the File and Storage Services role of Windows Server, aiding administrators in organizing and controlling storage data on file servers. FSRM facilitates the management of storage through folder-specific quotas, filtering of certain file types, and detailed reports on file system usage.

Task 1: add file Server Resource Manager

1- On **FSRM01**, in Server Manager, click Add roles and features.
2- In the Add Roles and Features Wizard, click Next
3- On the Select server roles page, expand File and Storage Services, expand File and iSCSI Services, and then select the File Server Resource Manager check box.



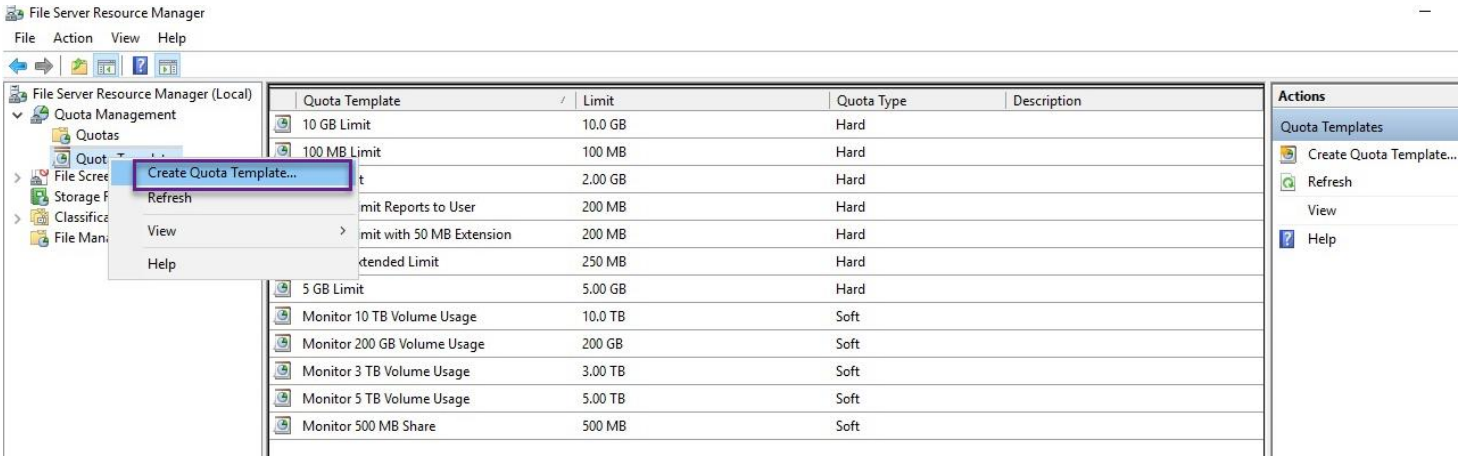

Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
FSRM01.itprolabs.xyz
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
View installation progress
Feature installation
Installation started on FSRM01.itprolabs.xyz
File and Storage Services
File and iSCSI Services
File Server
File Server Resource Manager
Remote Server Administration Tools
Role Administration Tools
File Services Tools
File Server Resource Manager Tools
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

Task 2: Create a quota template

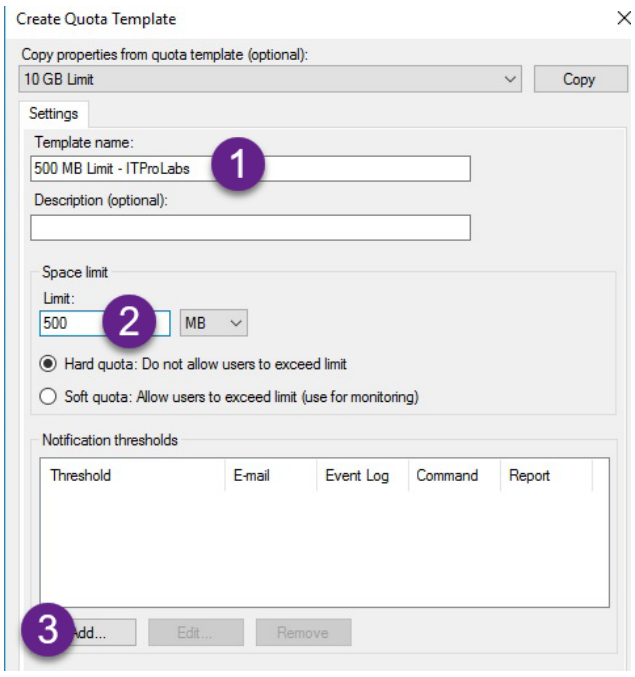
Quotas are categorized into two types: a hard quota and a soft quota.

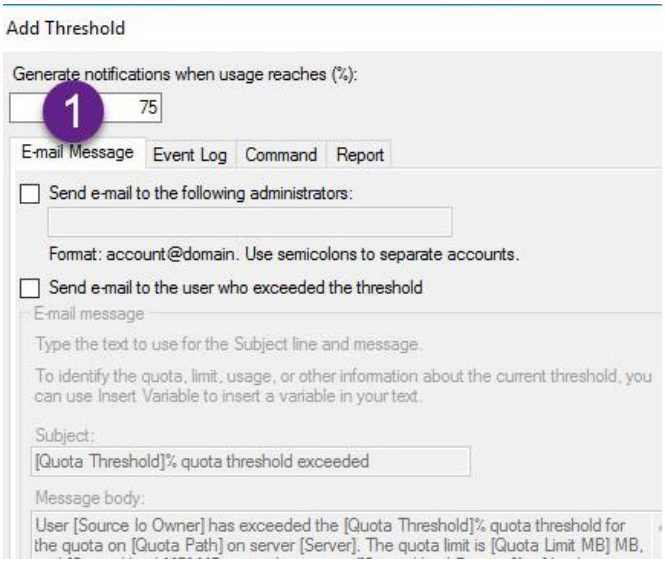
- A **hard quota** prevents users from saving files after the space limit is reached and generates notifications when the volume of data reaches each configured threshold.
- A soft quota does not enforce the quota limit but generates all configured notifications.

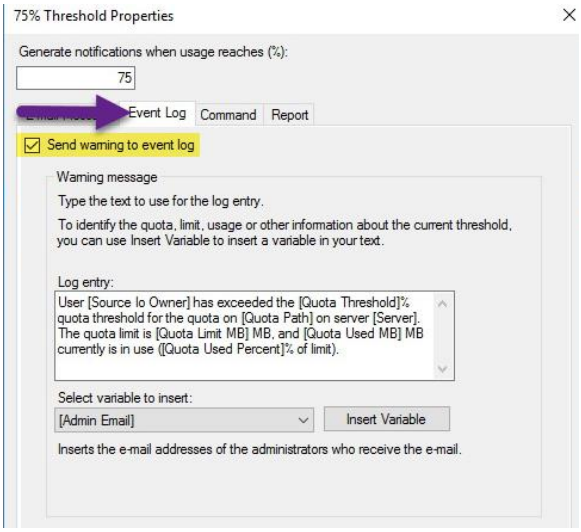
1- In Server Manager, click Tools, and then click File Server Resource Manager.



In this wizard, set up a custom template with a 500 MB quota.



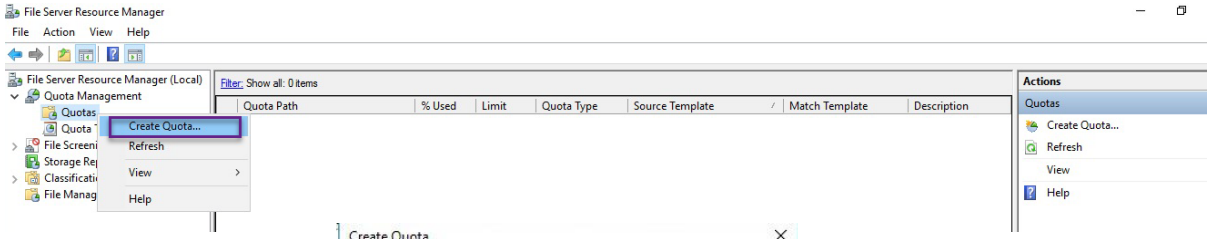


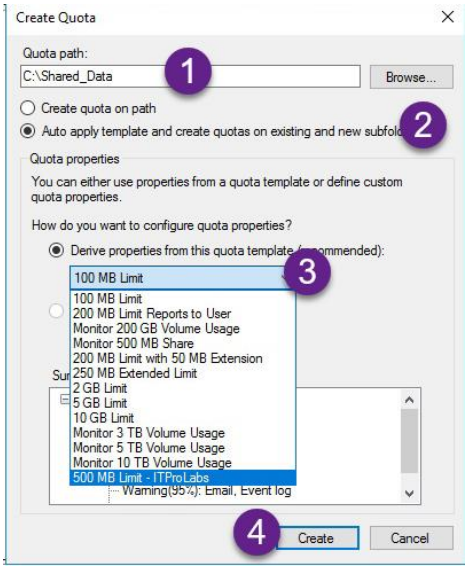


Task 3: Configure a quota based on the quota template

1- In the **File Server Resource Manager** console, click **Quotas**.

2- Right-click **Quotas**, and then click **Create Quota** using 500 MB custom quota that we just created, apply this quota policy to folder named **Shared_Data** in C drive.

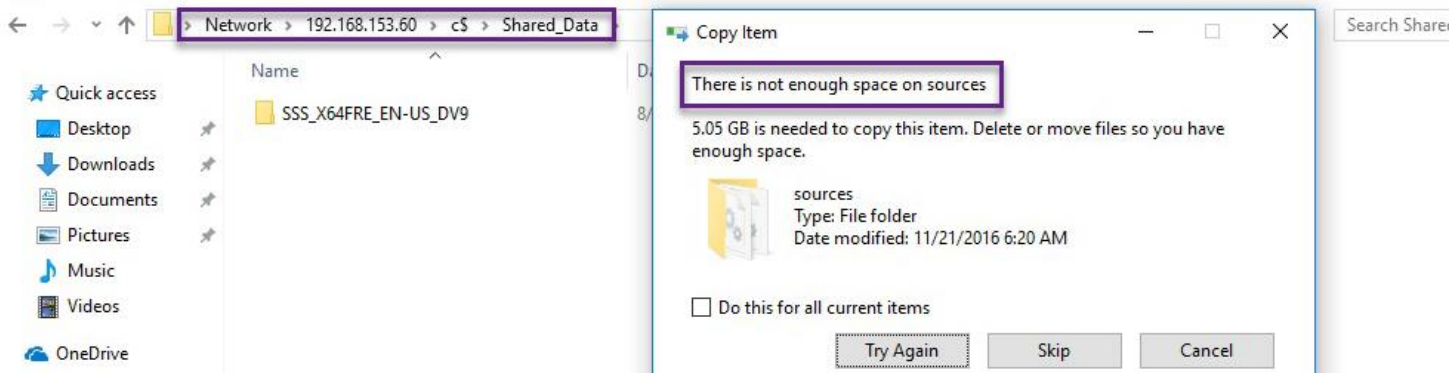




Task 3: Test that the quota is functional

1- Switch to Client01

2- On **Client01** (Windows 10 client) open run and type \\192.168.153.60\c$ to access **FSRM01** server share then access our file named **Shared_Data** and copy large file (more than allowed quota 500 MB)

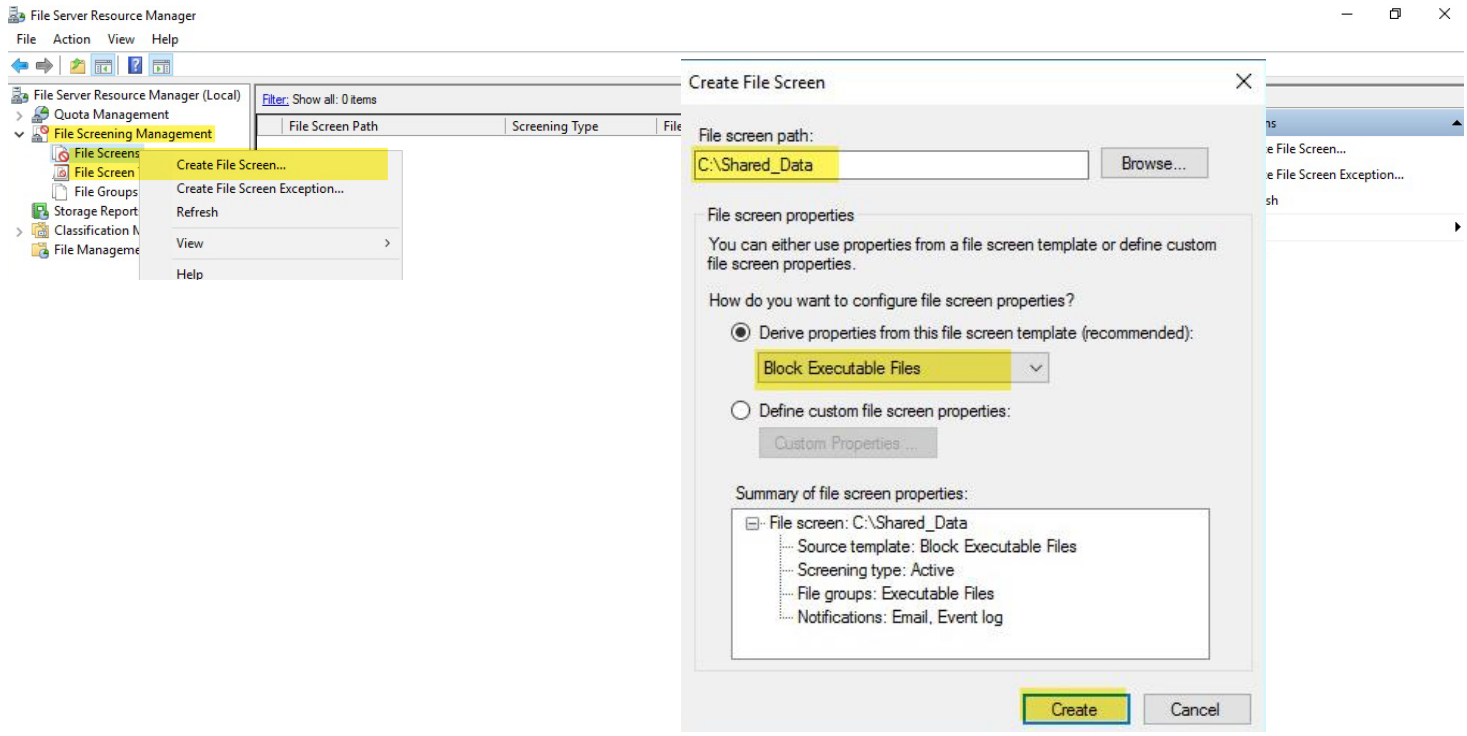


Task 4: Create a file screen (Block executable files)

1- Switch to **FSRM01**

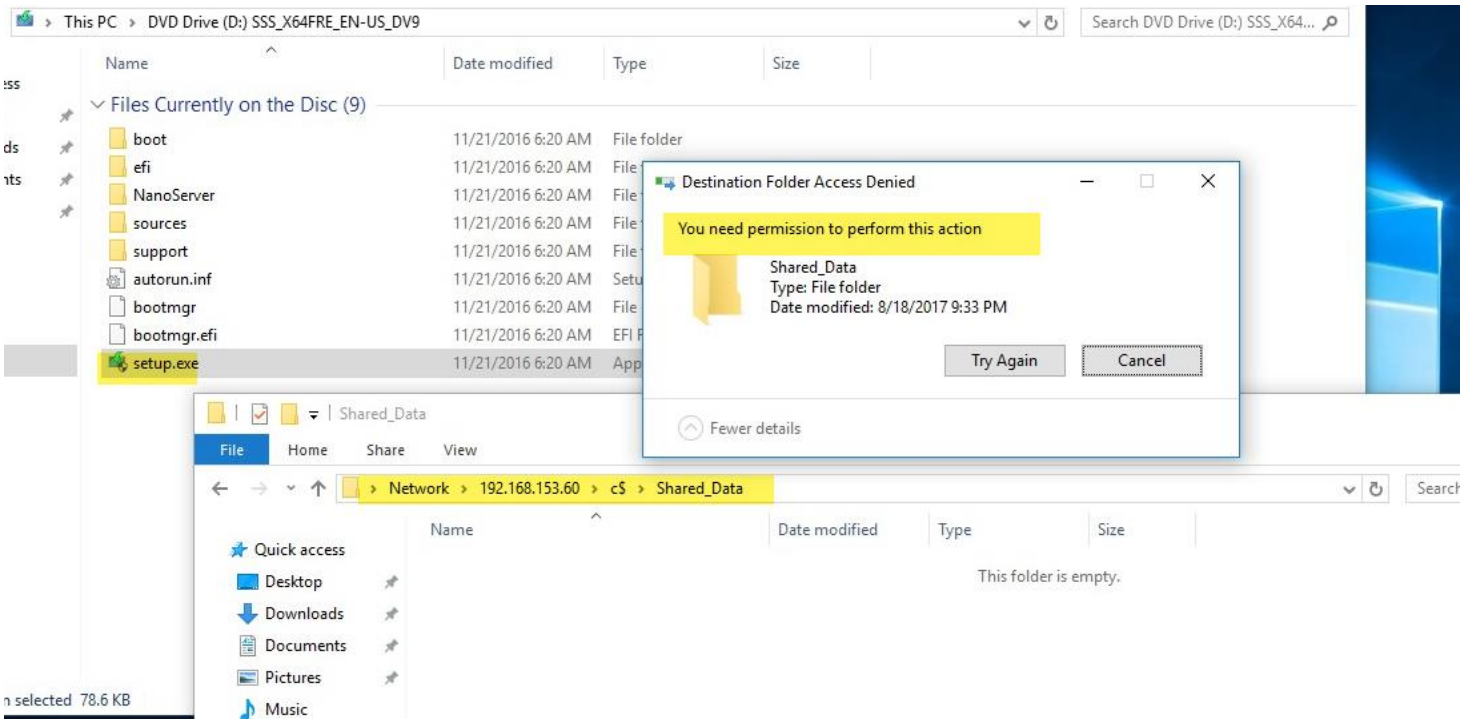
2- In the File Server Resource Manager console tree, expand File Screening Management, and then click File Screens.

In the following example, we will apply screening policy that prevent users to store any executable files on **Shared_Data** folder



Task 5: Test that the File Screen is functional

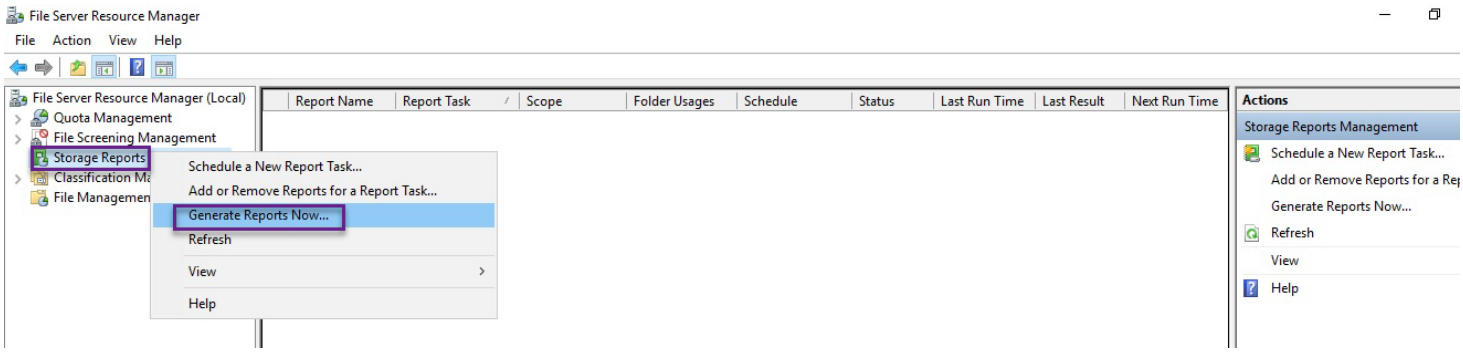
Switch to **Client01** and then access **Shared_Data** and try to copy any executable file

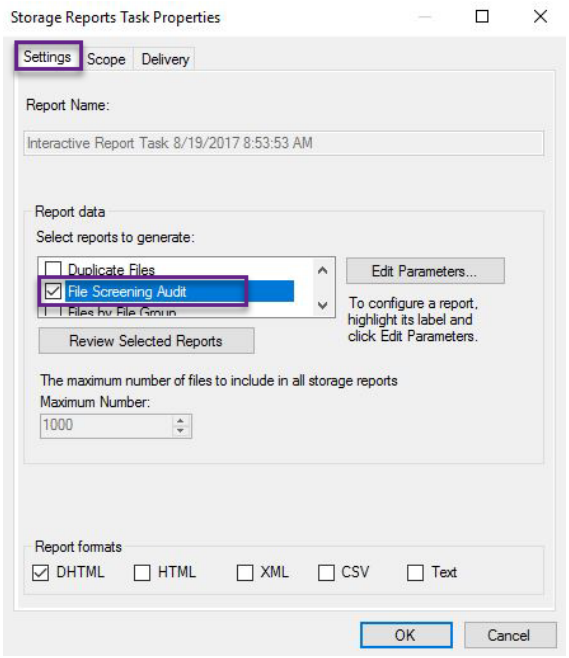


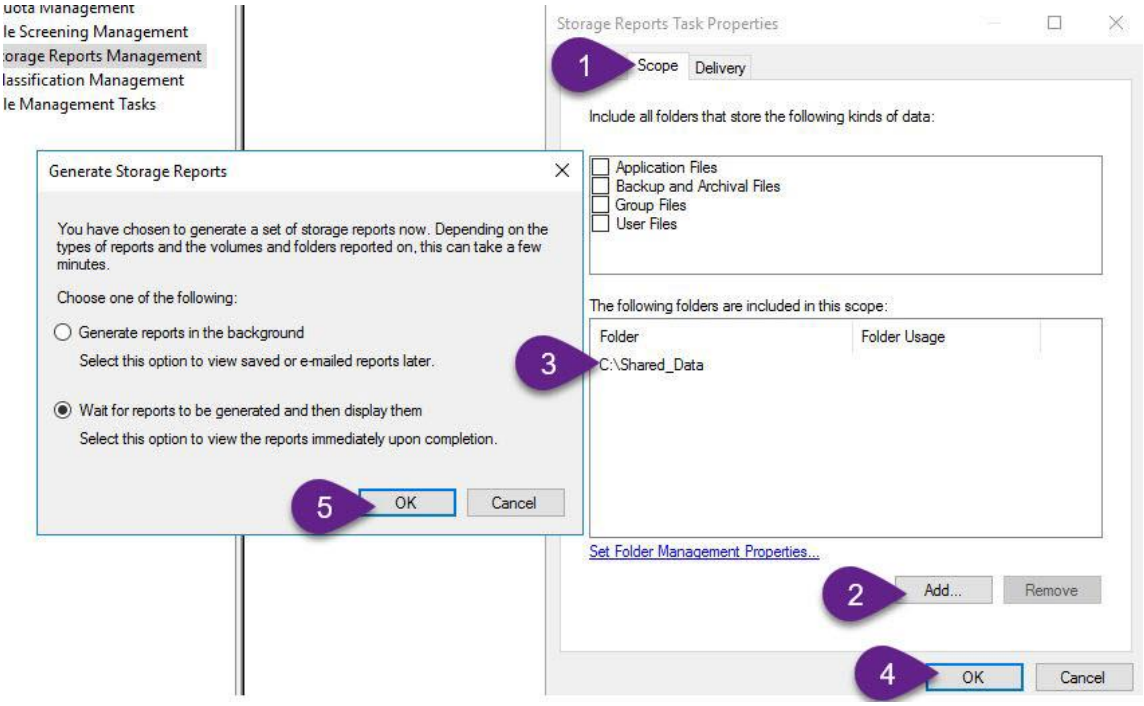
Task 7: Generate an on-demand storage report

1- Switch to **FSRM01**

2- In the **File Server Resource Manager** console, click **Storage Reports Management**.




Storage Reports Task Properties
Settings
Scope
Delivery
Report Name:
Interactive Report Task 8/19/2017 8:53:53 AM
Report data
Select reports to generate:
Duplicate Files
File Screening Audit
Edit Parameters...
To configure a report, highlight its label and click Edit Parameters.
Review Selected Reports
The maximum number of files to include in all storage reports
Maximum Number:
1000
Report formats
DHTML
HTML
XML
CSV
Text
OK
Cancel

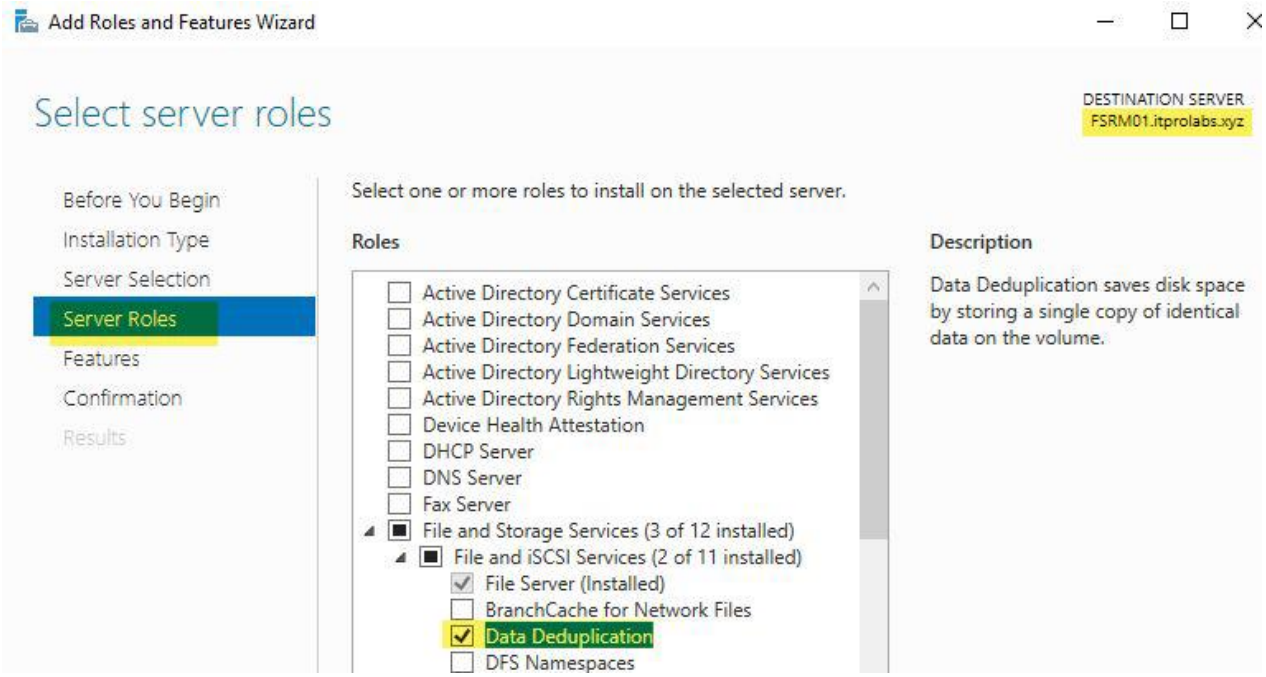

Storage Reports Task Properties
1
Scope
Delivery
Include all folders that store the following kinds of data:
Application Files
Backup and Archival Files
Group Files
User Files
The following folders are included in this scope:
Folder
Folder Usage
C:\Shared_Data
3
Set Folder Management Properties...
2
Add...
Remove
4
OK
Cancel
Generate Storage Reports
You have chosen to generate a set of storage reports now. Depending on the types of reports and the volumes and folders reported on, this can take a few minutes.
Choose one of the following:
Generate reports in the background
Select this option to view saved or e-mailed reports later.
Wait for reports to be generated and then display them
Select this option to view the reports immediately upon completion.
5
OK
Cancel

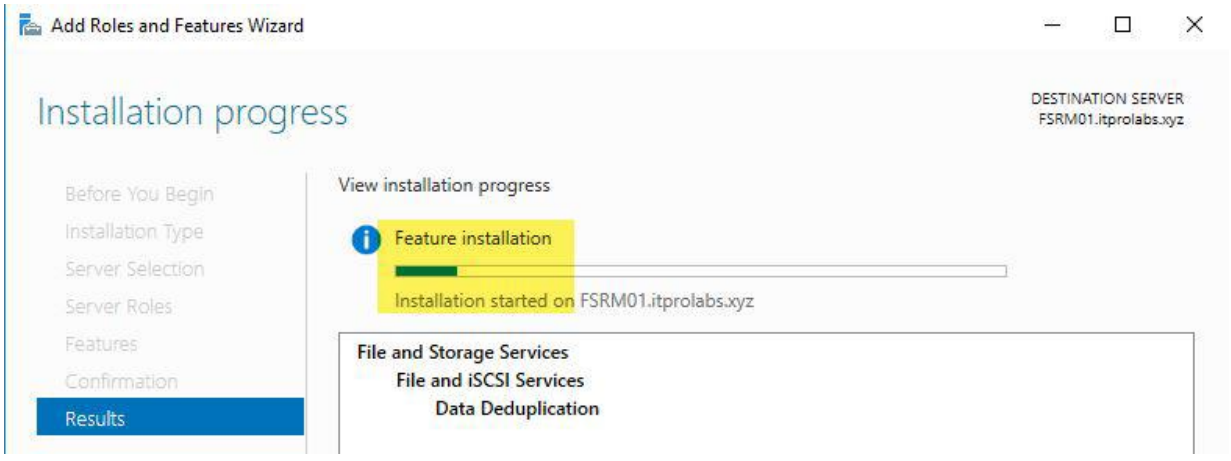
Lab 2: Data Deduplication

Data Deduplication, a feature of Windows Server, detects and eliminates data duplicates while preserving its integrity, allowing for enhanced storage efficiency. This guide discusses the implementation of Data Deduplication on Windows Server. Introduced in Server and refined in, it supports partitions up to 64 terabytes and file sizes up to 1TB, but it's compatible only with NTFS or REFS file systems and is not offered for client operating systems such as Windows 10.

Task 1: Install the Data Deduplication role service

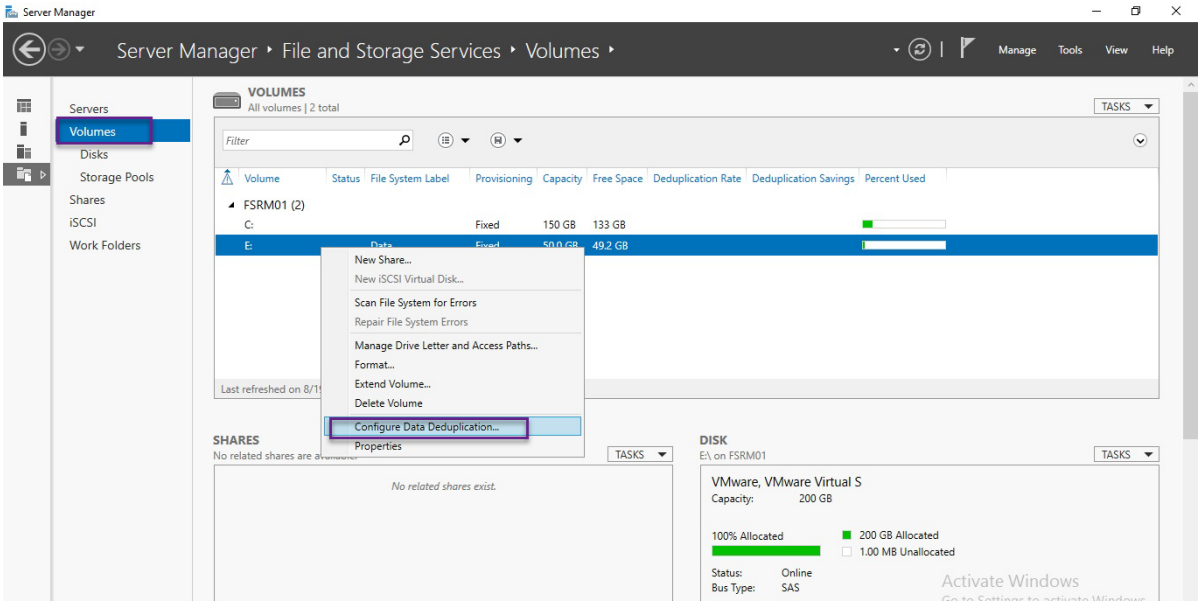
1- On **FSRM01**, in Server Manager, click **Add roles and features**.

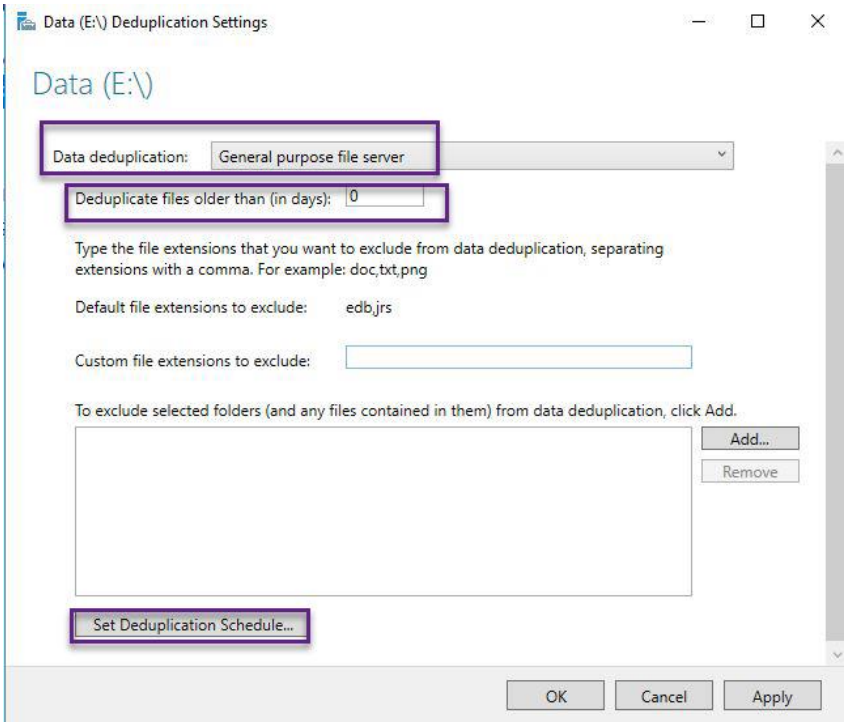


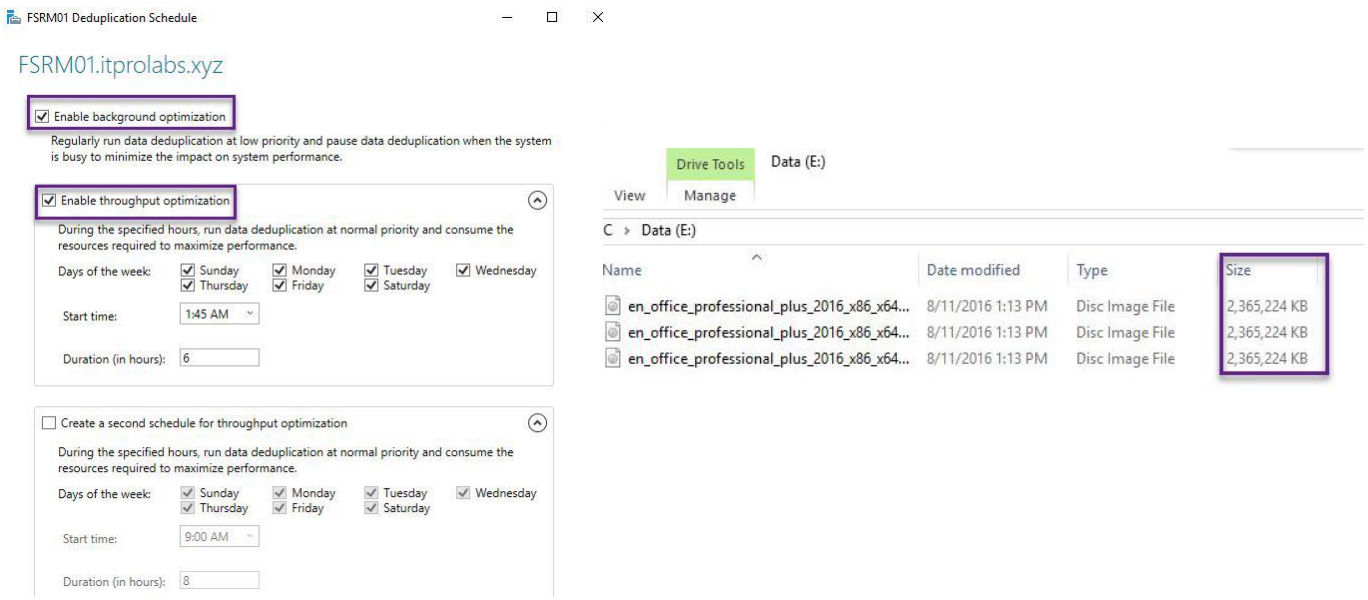


Task 2: Enable, configure and test Data Deduplication

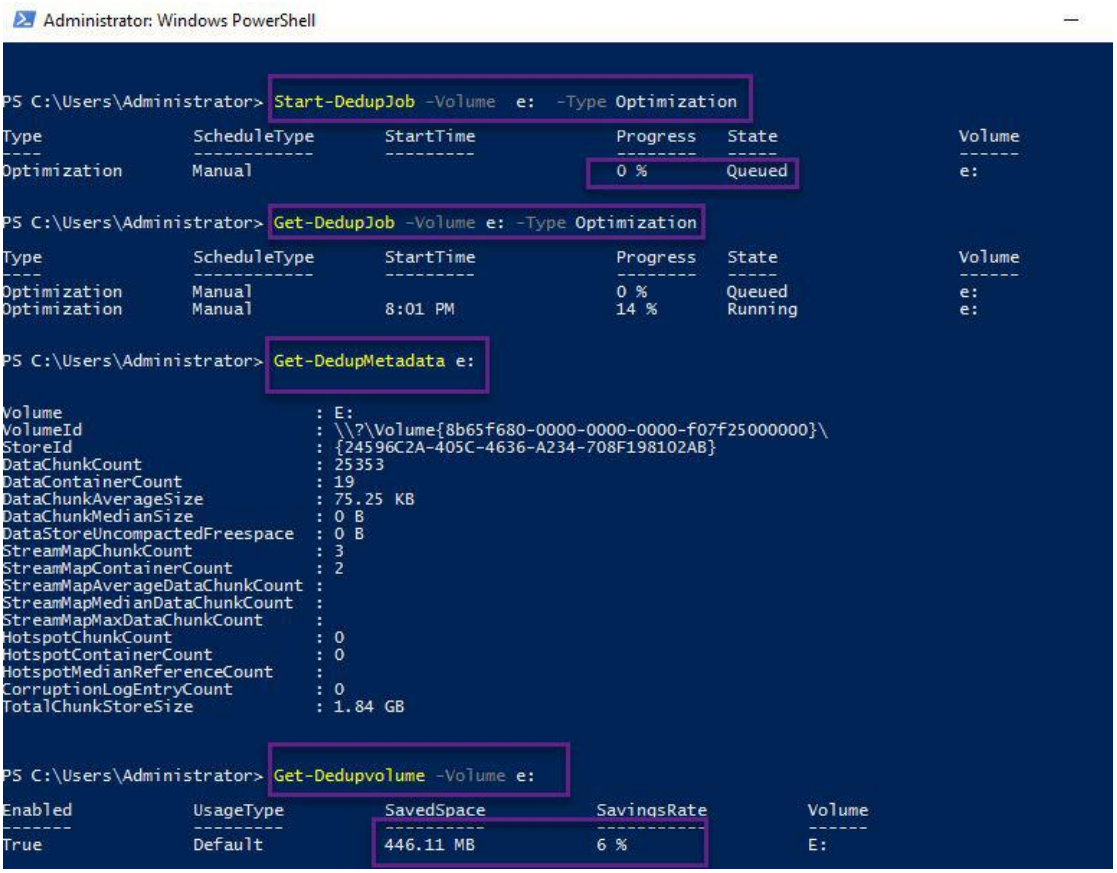
1- On **FSRM01**, right-click Start, and then click Run.
2- In Server Manager, in the navigation pane, click File and Storage Services, and then click VOLUMES.
3- Copy some files to this volume and duplicate same file to same volume and check the free size of volume







4- In the Windows PowerShell window, type the following command to start Deduplication process

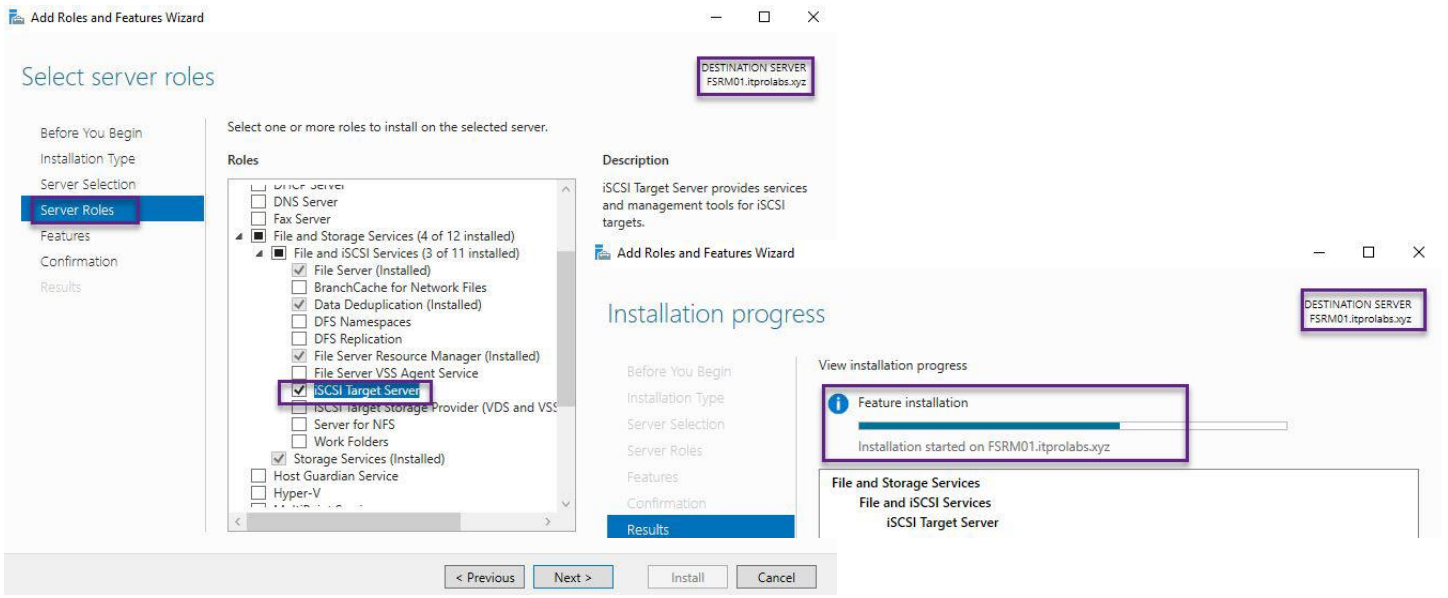


Lab 3: ISCSI Storage

iSCSI storage enables a Windows Server to share storage over an Ethernet network without needing specialized hardware.

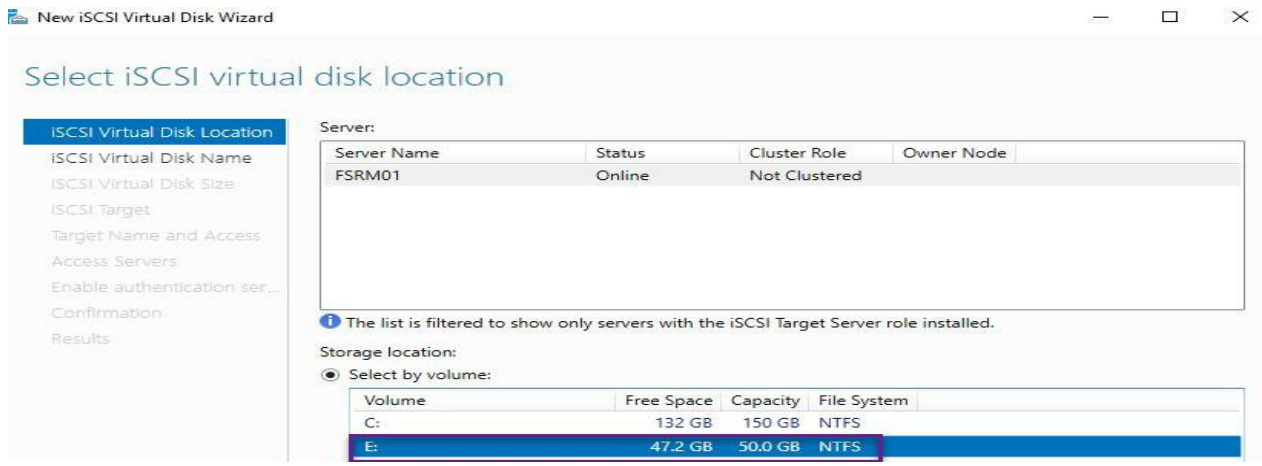
Task 1: Install the Internet small computer system interface (iSCSI) target role services

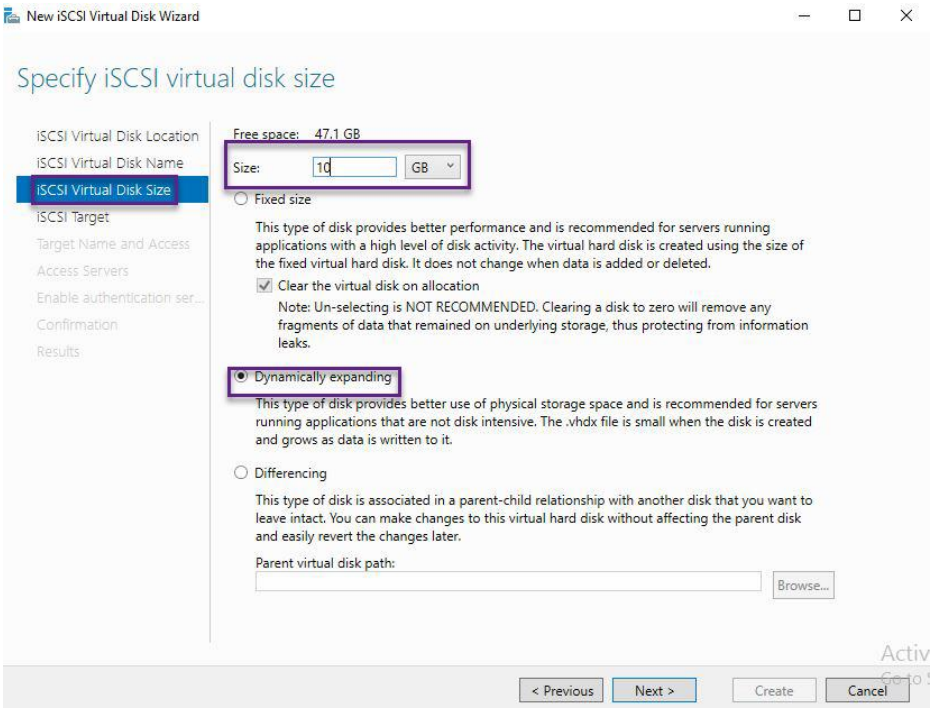
1. Switch to **FSRM01**.
2. On the taskbar, click **Start**, and then click **Server Manager**.
3. In Server Manager, click **Add roles and features**.

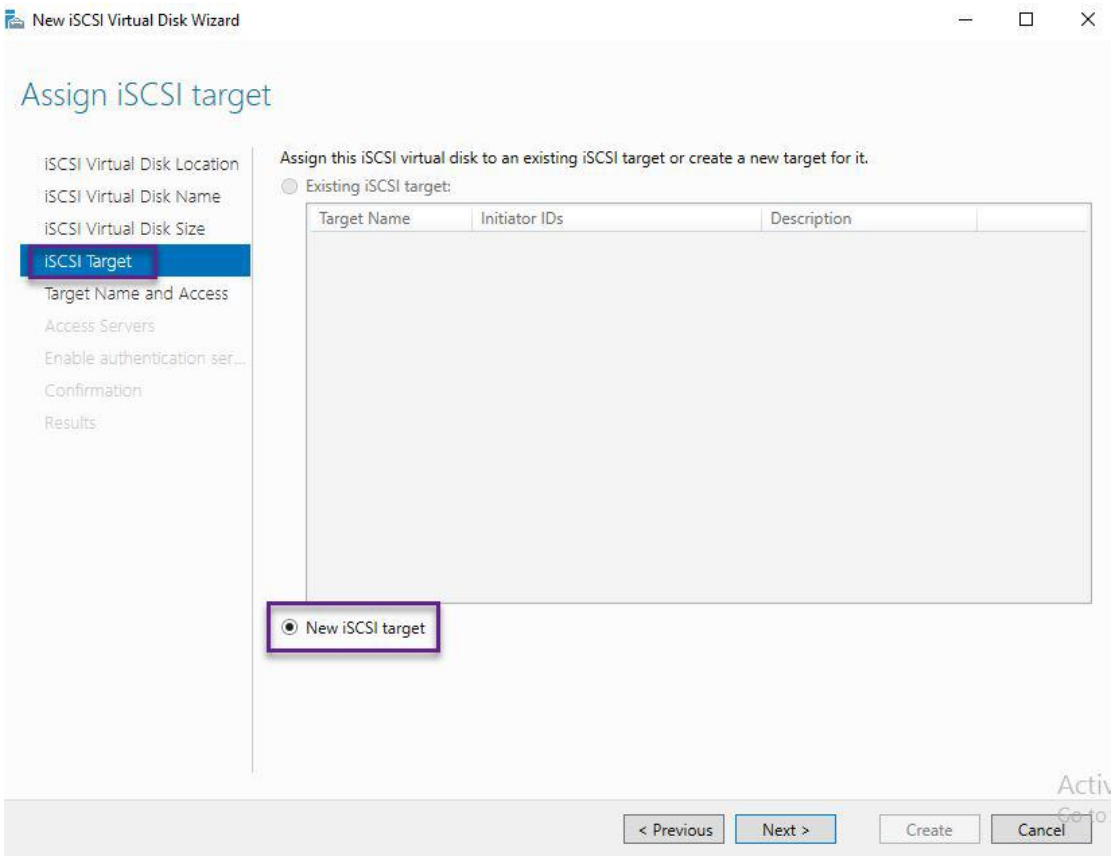


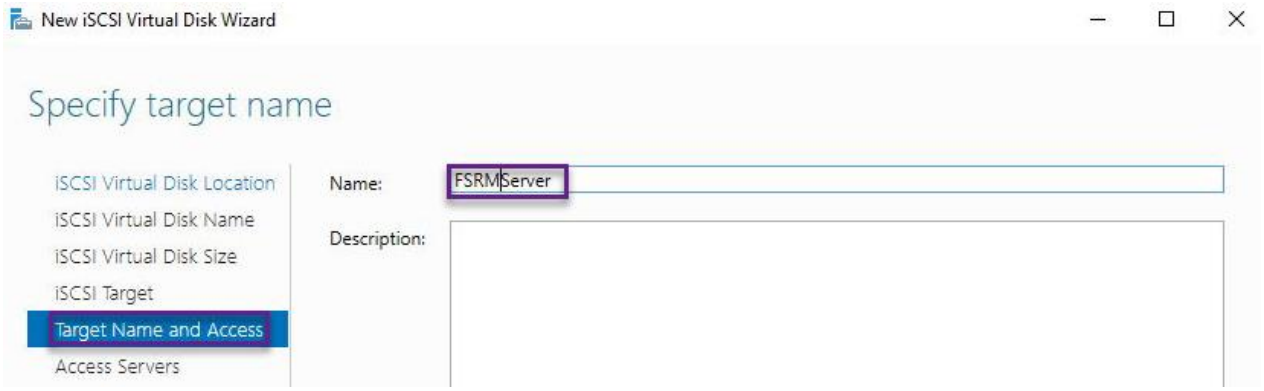
Task 2: Configure the iSCSI targets

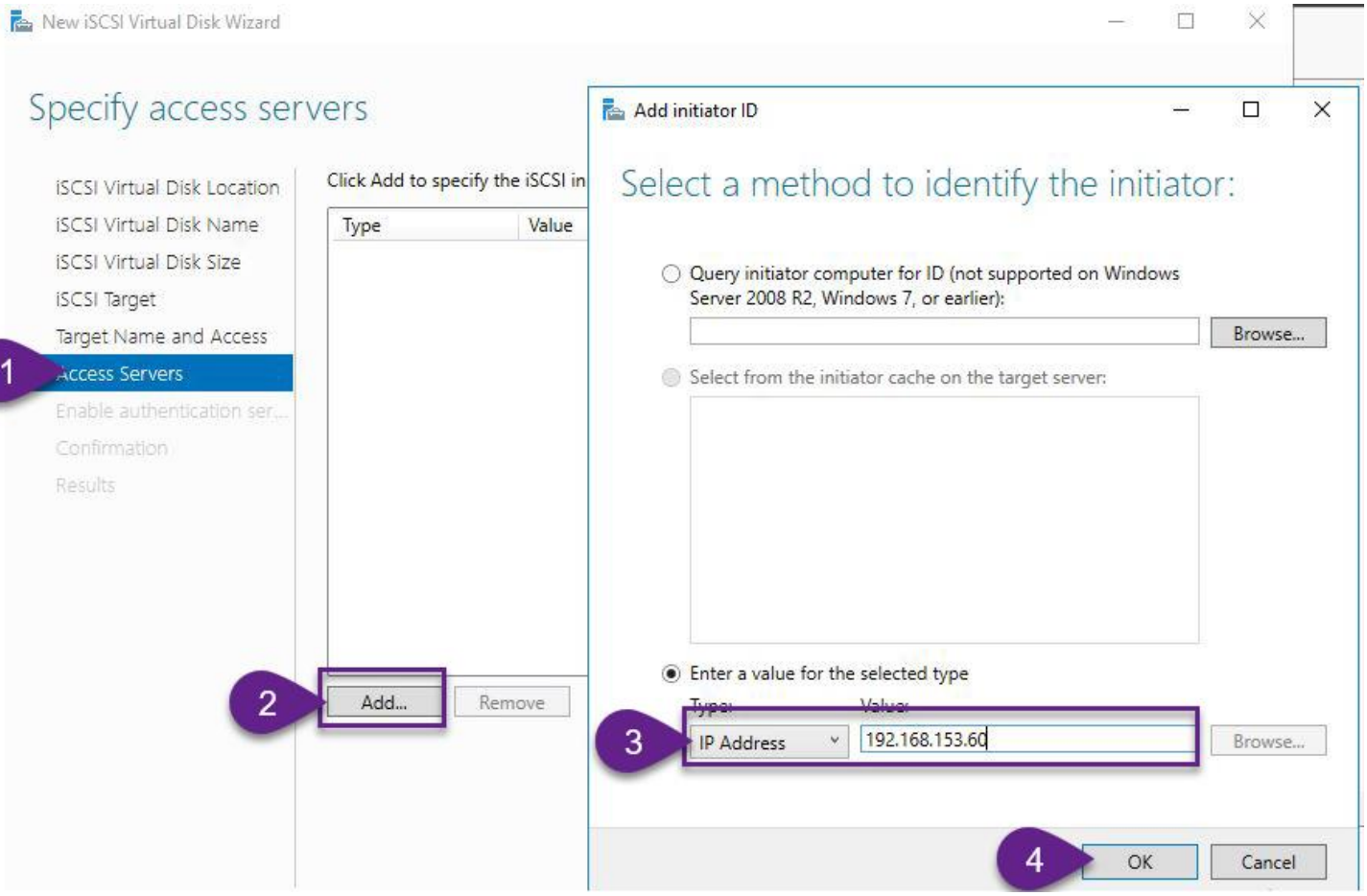
1- On **FSRM01**, in Server Manager, in the navigation pane, click File and Storage Services

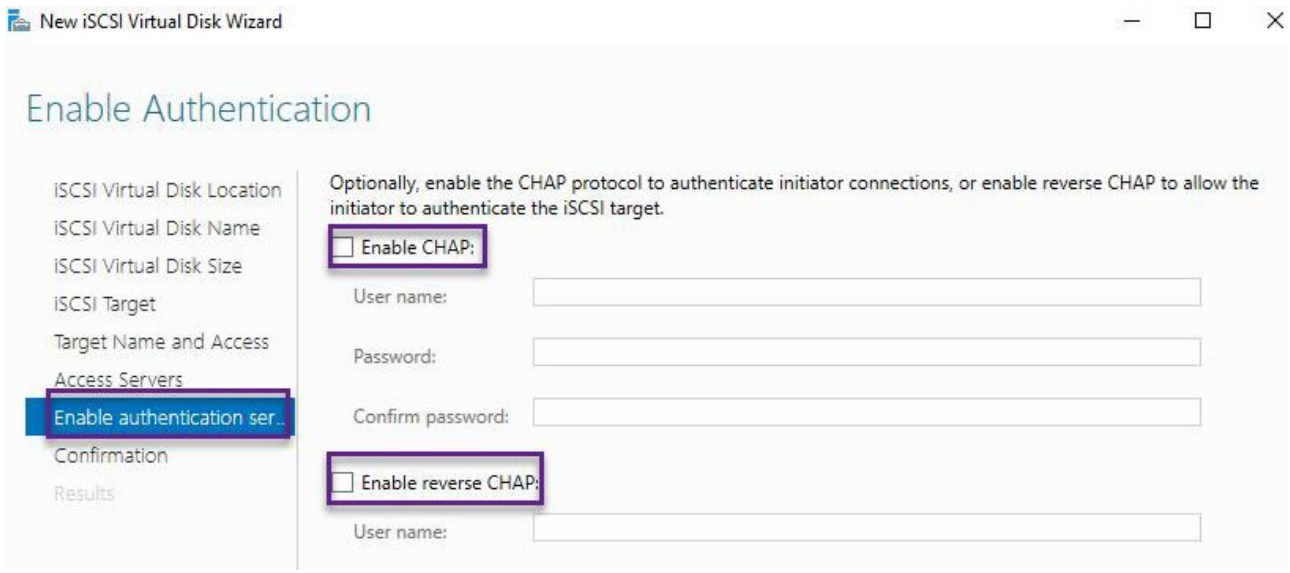


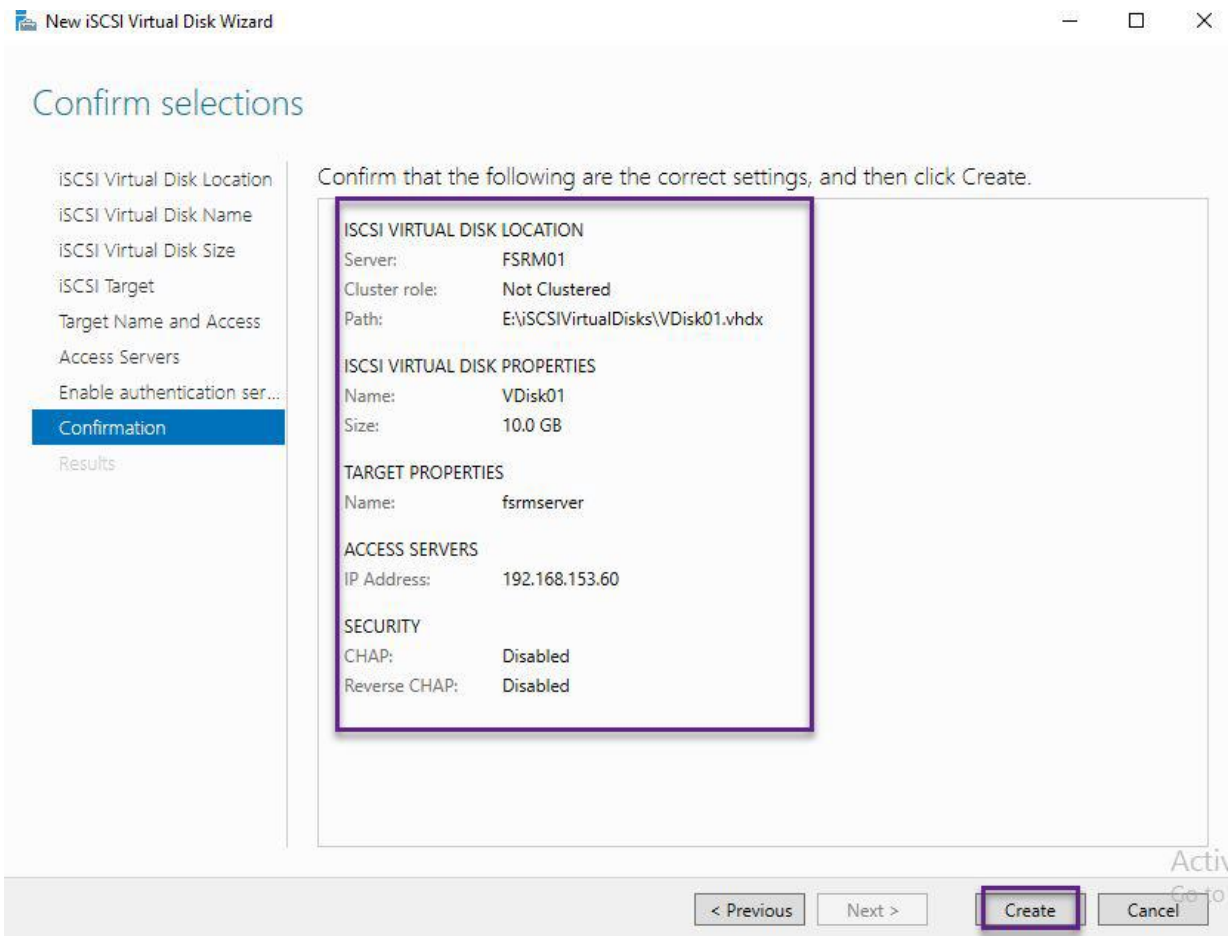

New iSCSI Virtual Disk Wizard
Specify iSCSI virtual disk size
iSCSI Virtual Disk Location
iSCSI Virtual Disk Name
iSCSI Virtual Disk Size
iSCSI Target
Target Name and Access
Access Servers
Enable authentication ser...
Confirmation
Results
Free space: 47.1 GB
Size: 10 GB
Fixed size
This type of disk provides 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:
Browse...
< Previous
Next >
Create
Cancel

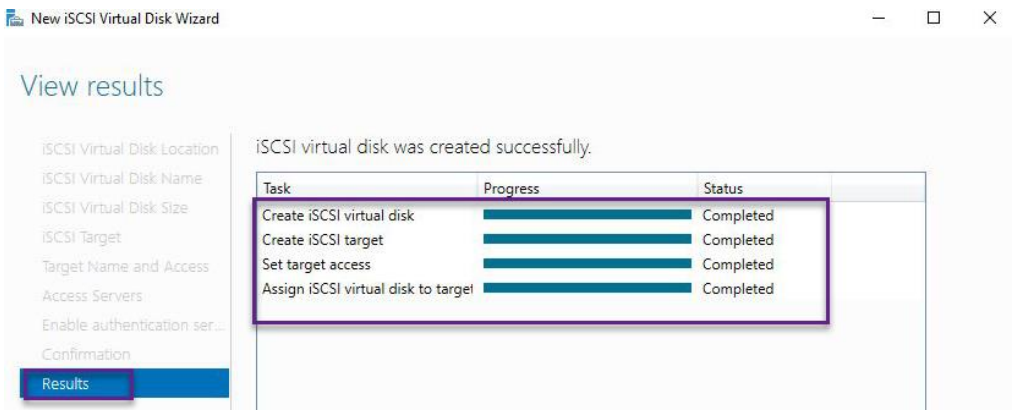

New iSCSI Virtual Disk Wizard
Assign iSCSI target
iSCSI Virtual Disk Location
iSCSI Virtual Disk Name
iSCSI Virtual Disk Size
iSCSI Target
Target Name and Access
Access Servers
Enable authentication ser...
Confirmation
Results
Assign this iSCSI virtual disk to an existing iSCSI target or create a new target for it.
Existing iSCSI target:
Target Name
Initiator IDs
Description
New iSCSI target
< Previous
Next >
Create
Cancel


New iSCSI Virtual Disk Wizard
Specify target name
iSCSI Virtual Disk Location
iSCSI Virtual Disk Name
iSCSI Virtual Disk Size
iSCSI Target
Target Name and Access
Access Servers
Name:
FSRMServer
Description:


New iSCSI Virtual Disk Wizard
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
1
Click Add to specify the iSCSI in
Type
Value
2
Add...
Remove
Add initiator ID
Select a method to identify the initiator:
Query initiator computer for ID (not supported on Windows Server 2008 R2, Windows 7, or earlier):
Browse...
Select from the initiator cache on the target server:
Enter a value for the selected type
Type:
Value:
3
IP Address
192.168.153.60
Browse...
4
OK
Cancel


New iSCSI Virtual Disk Wizard
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:

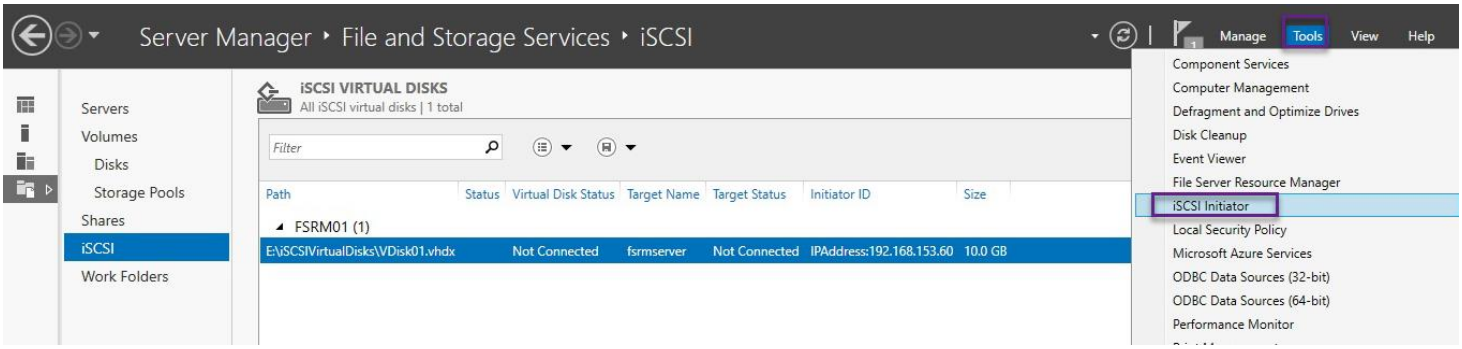

New iSCSI Virtual Disk Wizard
Confirm selections
iSCSI Virtual Disk Location
iSCSI Virtual Disk Name
iSCSI Virtual Disk Size
iSCSI Target
Target Name and Access
Access Servers
Enable authentication ser...
Confirmation
Results
Confirm that the following are the correct settings, and then click Create.
ISCSI VIRTUAL DISK LOCATION
Server: FSRM01
Cluster role: Not Clustered
Path: E:\iSCSIVirtualDisks\VDisk01.vhdx
ISCSI VIRTUAL DISK PROPERTIES
Name: VDisk01
Size: 10.0 GB
TARGET PROPERTIES
Name: fsrmserver
ACCESS SERVERS
IP Address: 192.168.153.60
SECURITY
CHAP: Disabled
Reverse CHAP: Disabled
< Previous
Next >
Create
Cancel

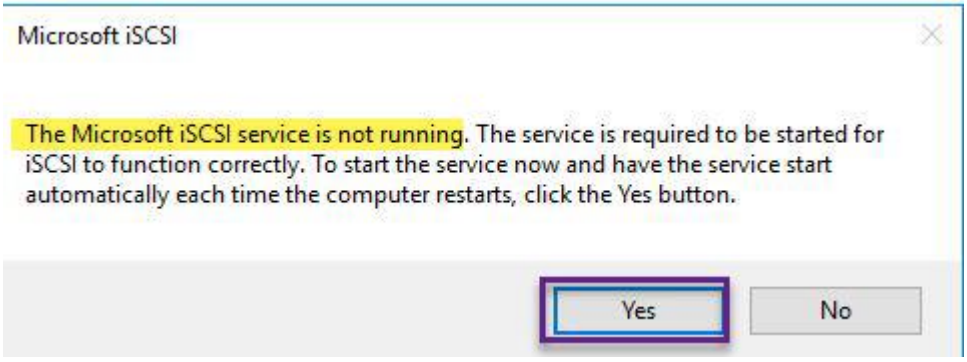


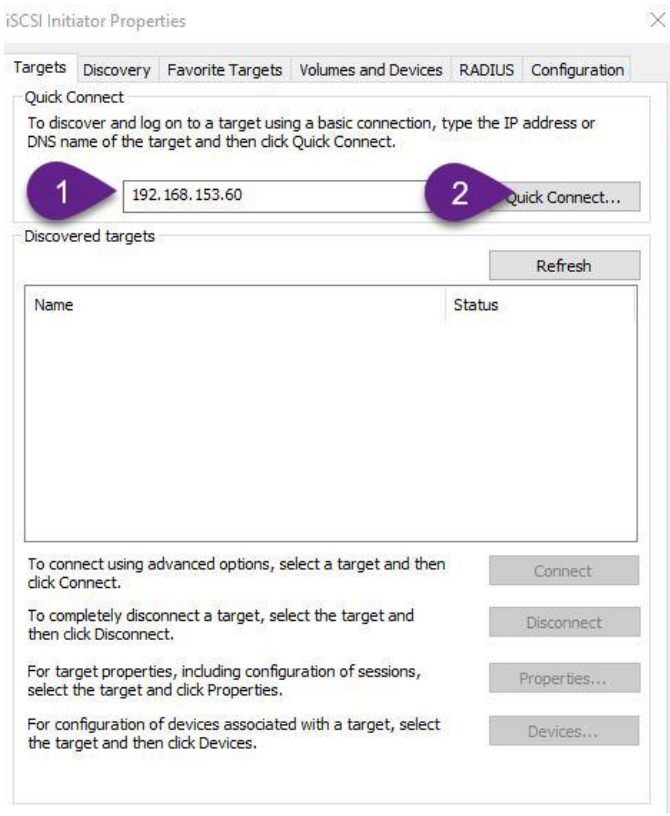
Task 4: Connect to and configure the iSCSI targets

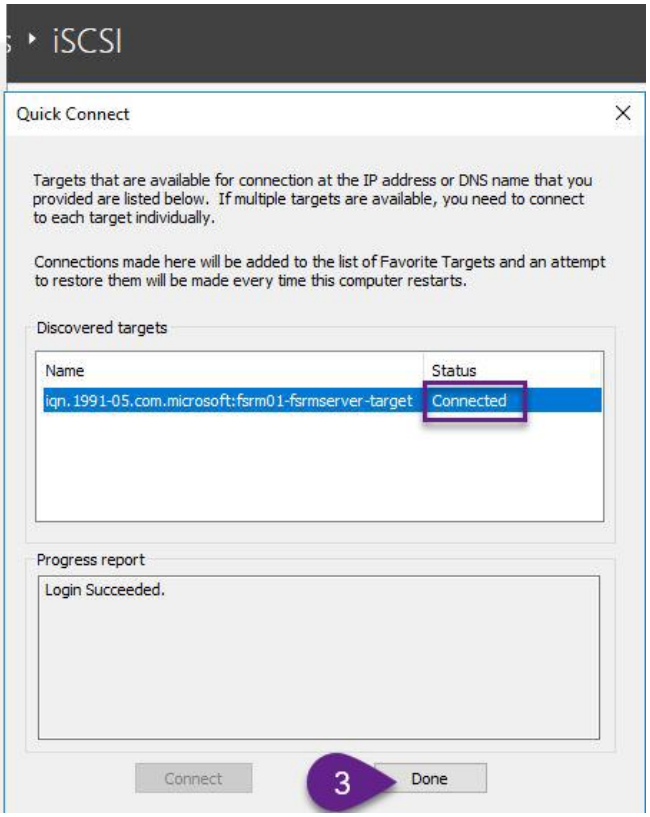
1- On **FSRM01**, in Server Manager, click Tools, and then click iSCSI Initiator.

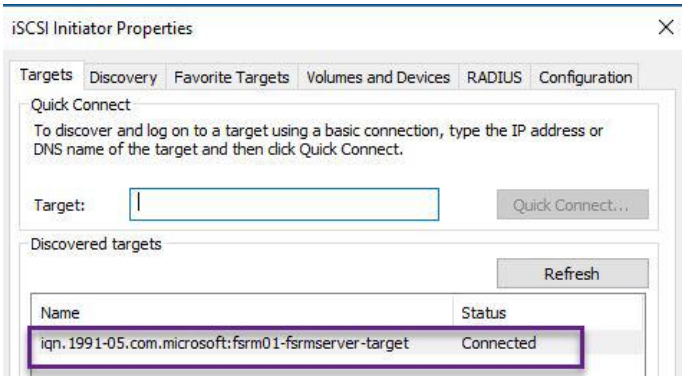
Please be aware that you have the ability to connect to an ISCSI target using the ISCSI initiator on any client operating with Windows 7 or newer.



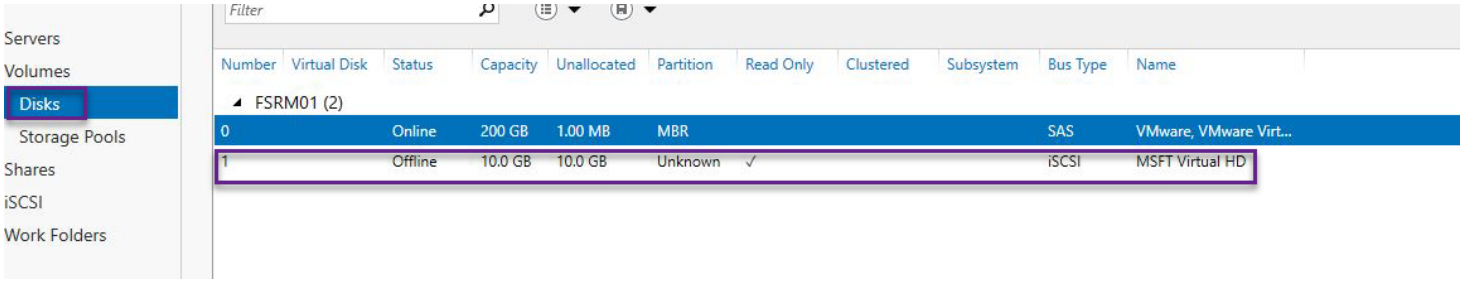


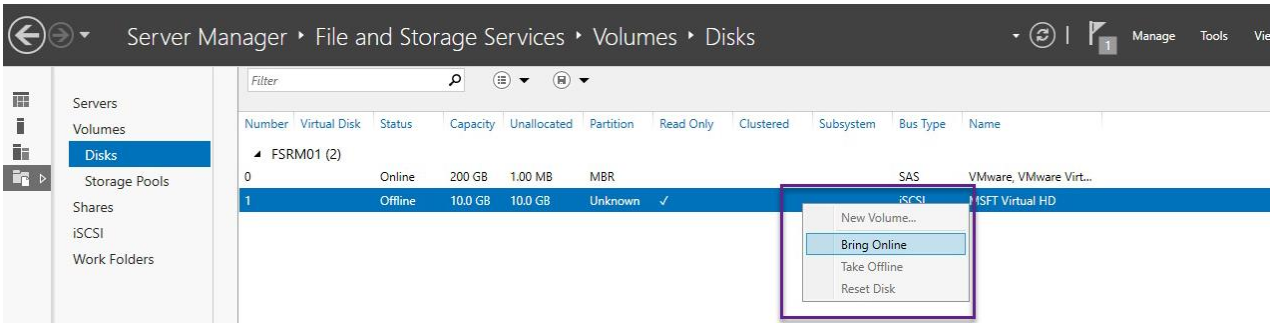

iSCSI Initiator Properties
Targets
Discovery
Favorite Targets
Volumes and Devices
RADIUS
Configuration
Quick Connect
To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect.
1
192.168.153.60
2
Quick Connect...
Discovered targets
Refresh
Name
Status
To connect using advanced options, select a target and then click Connect.
Connect
To completely disconnect a target, select the target and then click Disconnect.
Disconnect
For target properties, including configuration of sessions, select the target and click Properties.
Properties...
For configuration of devices associated with a target, select the target and then click Devices.
Devices...

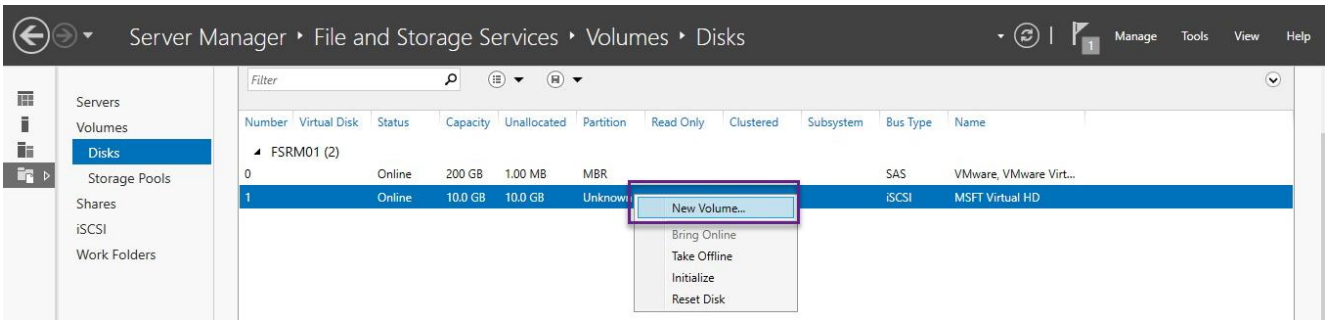

iSCSI
Quick Connect
Targets that are available for connection at the IP address or DNS name that you provided are listed below. If multiple targets are available, you need to connect to each target individually.
Connections made here will be added to the list of Favorite Targets and an attempt to restore them will be made every time this computer restarts.
Discovered targets
Name
Status
iqn.1991-05.com.microsoft:fsrm01-fsrmserver-target
Connected
Progress report
Login Succeeded.
Connect
3
Done

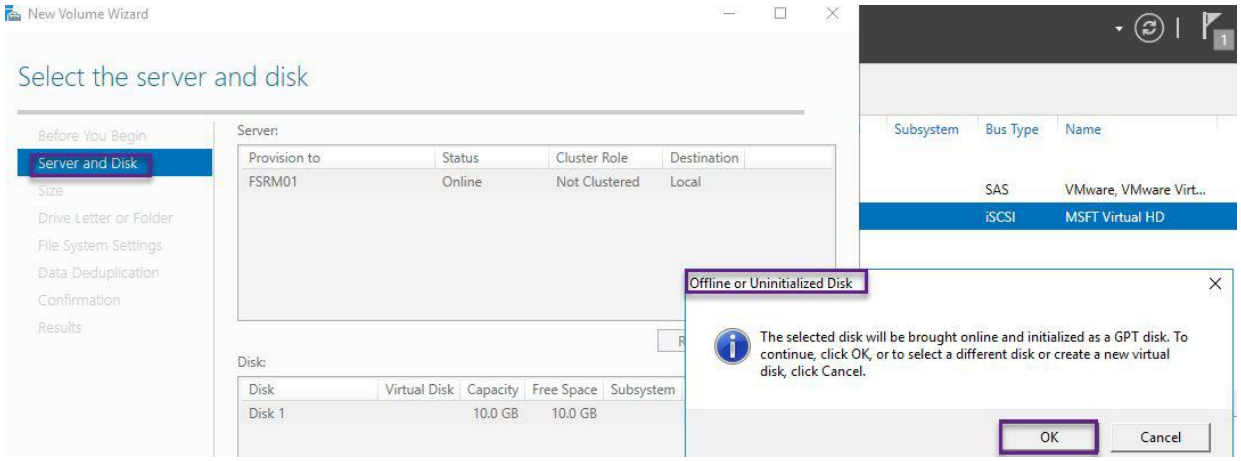

iSCSI Initiator Properties
Targets
Discovery
Favorite Targets
Volumes and Devices
RADIUS
Configuration
Quick Connect
To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect.
Target:
Quick Connect...
Discovered targets
Refresh
Name
Status
iqn.1991-05.com.microsoft:fsrm01-fsrmserver-target
Connected

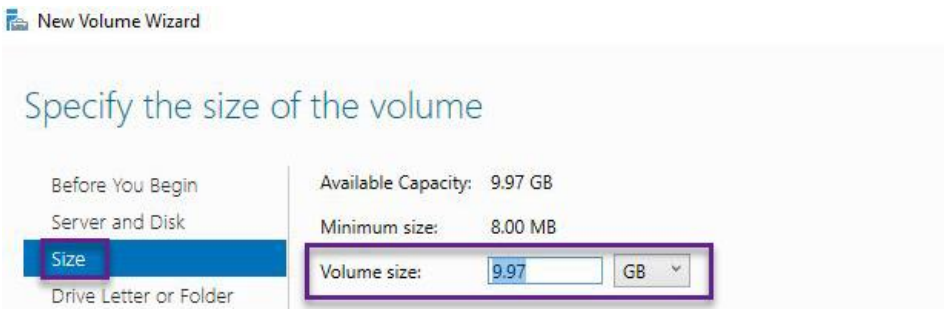
2. Return to the server manager and use the following steps to set up the connected virtual disk.

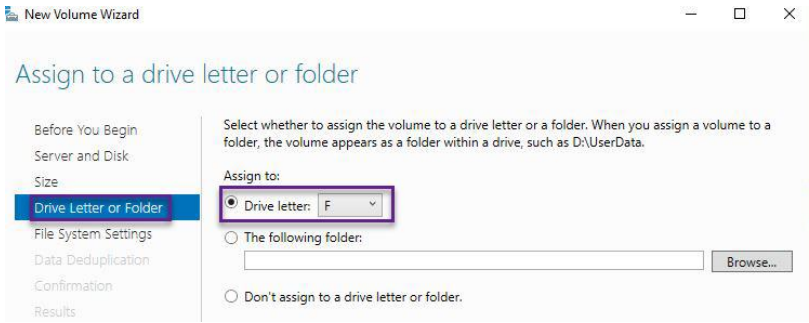


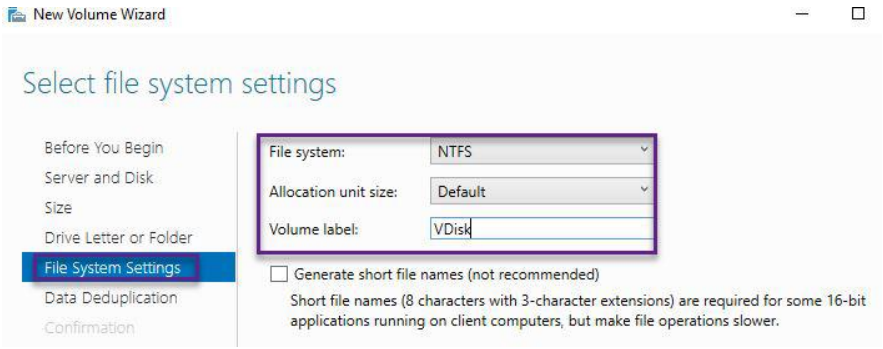


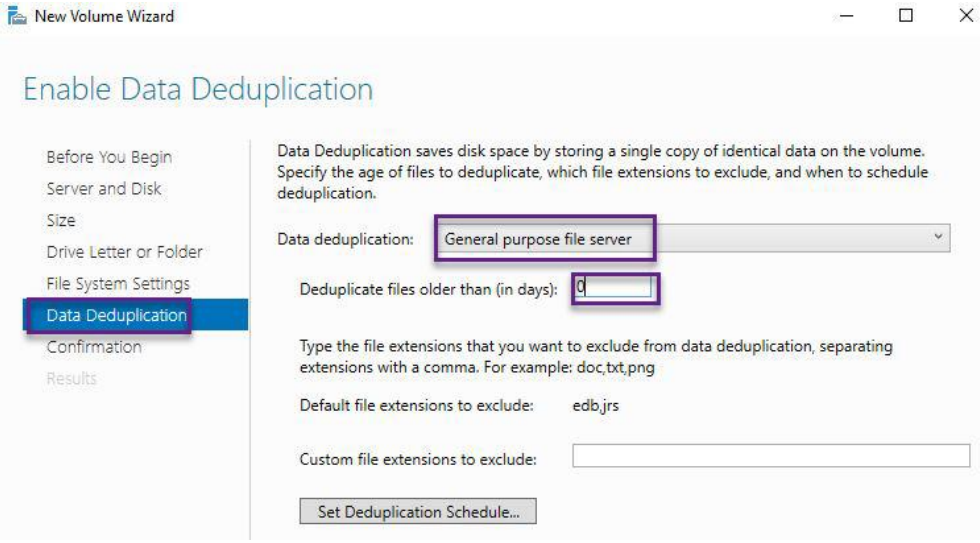


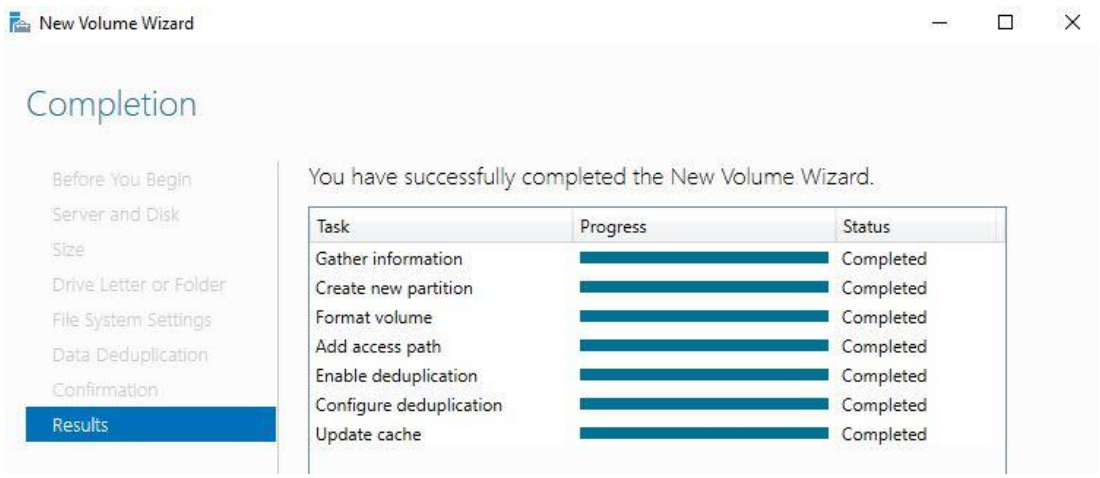



New Volume Wizard
Specify the size of the volume
Before You Begin
Server and Disk
Size
Drive Letter or Folder
Available Capacity: 9.97 GB
Minimum size: 8.00 MB
Volume size: 9.97 GB

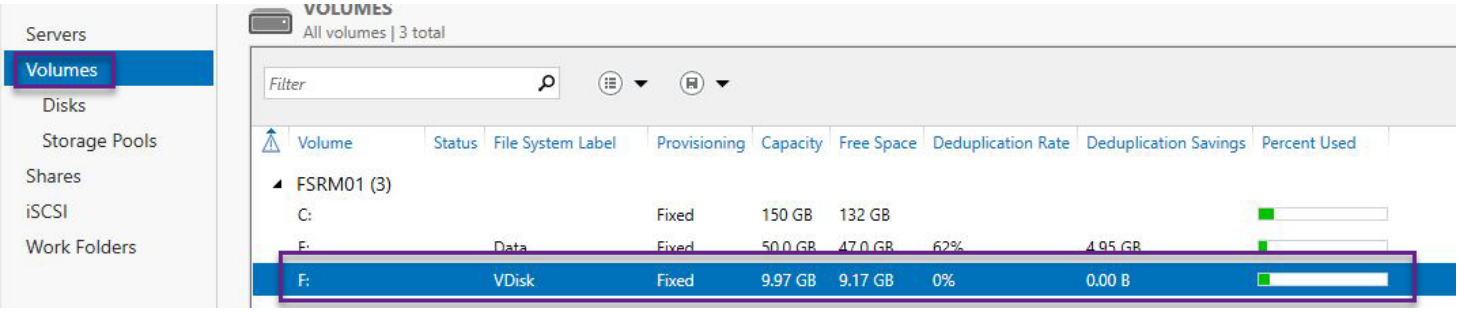

New Volume Wizard
Assign to a drive letter or folder
Before You Begin
Server and Disk
Size
Drive Letter or Folder
File System Settings
Data Deduplication
Confirmation
Results
Select whether to assign the volume to a drive letter or a folder. When you assign a volume to a folder, the volume appears as a folder within a drive, such as D:\UserData.
Assign to:
Drive letter: F
The following folder:
Browse...
Don't assign to a drive letter or folder.


New Volume Wizard
Select file system settings
Before You Begin
Server and Disk
Size
Drive Letter or Folder
File System Settings
Data Deduplication
Confirmation
File system: NTFS
Allocation unit size: Default
Volume label: VDisk
Generate short file names (not recommended)
Short file names (8 characters with 3-character extensions) are required for some 16-bit applications running on client computers, but make file operations slower.


New Volume Wizard
Enable Data Deduplication
Before You Begin
Server and Disk
Size
Drive Letter or Folder
File System Settings
Data Deduplication
Confirmation
Results
Data Deduplication saves disk space by storing a single copy of identical data on the volume. Specify the age of files to deduplicate, which file extensions to exclude, and when to schedule deduplication.
Data deduplication: General purpose file server
Deduplicate files older than (in days): 0
Type the file extensions that you want to exclude from data deduplication, separating extensions with a comma. For example: doc,txt,png
Default file extensions to exclude: edb,jrs
Custom file extensions to exclude:
Set Deduplication Schedule...



2- Virtual disk is ready to use

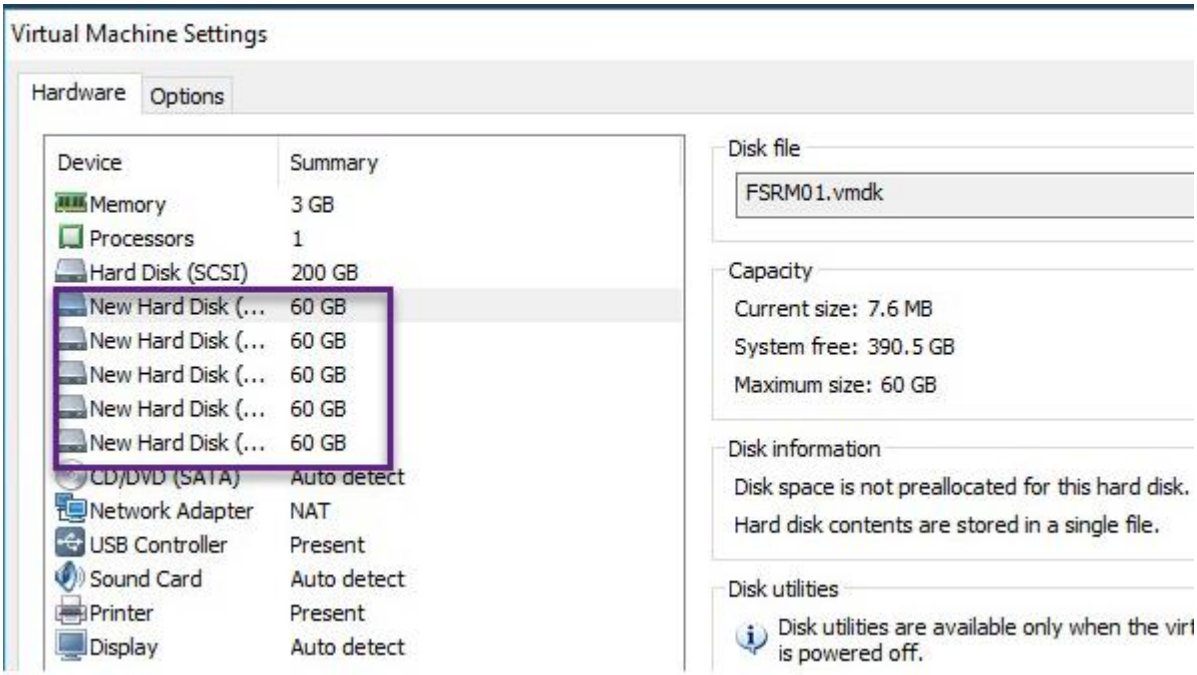


Lab 4: Storage Pool

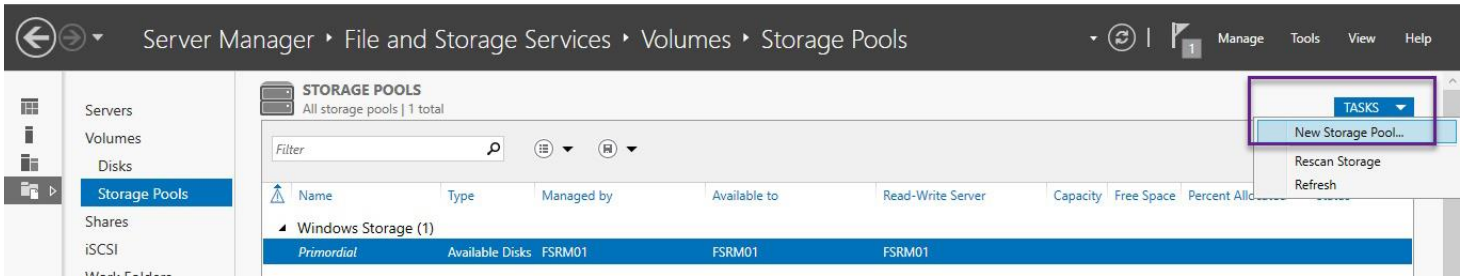
An array of virtual or physical drives that provides an economical, resilient, expandable, and adaptable storage solution.

Task 1: Create a storage pool

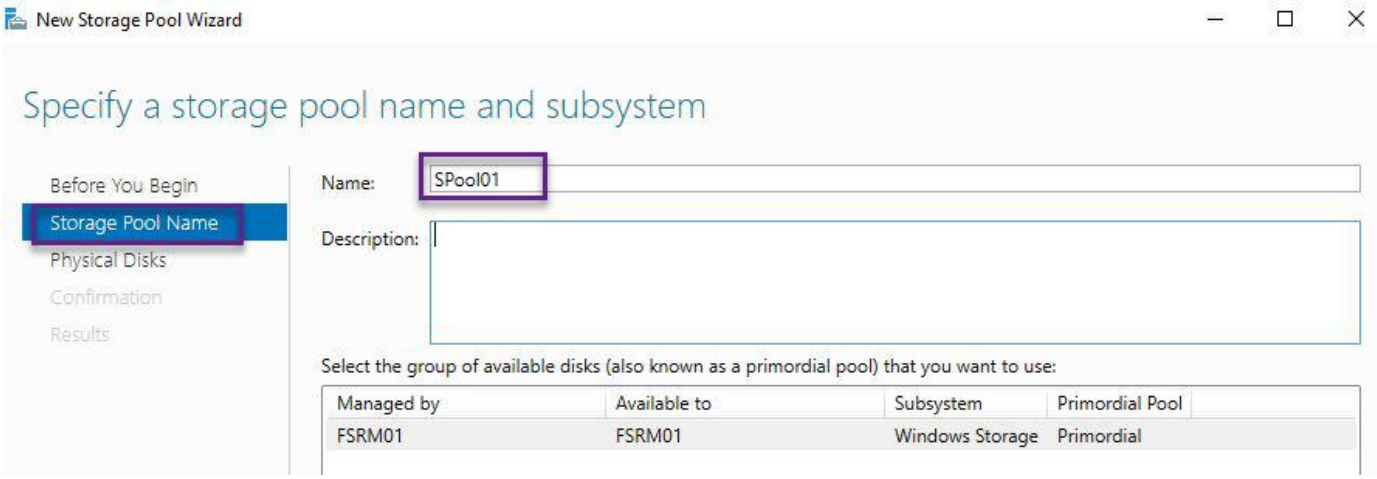
1- In VMWare, increase the number of virtual disks through the virtual machine settings by adding five.

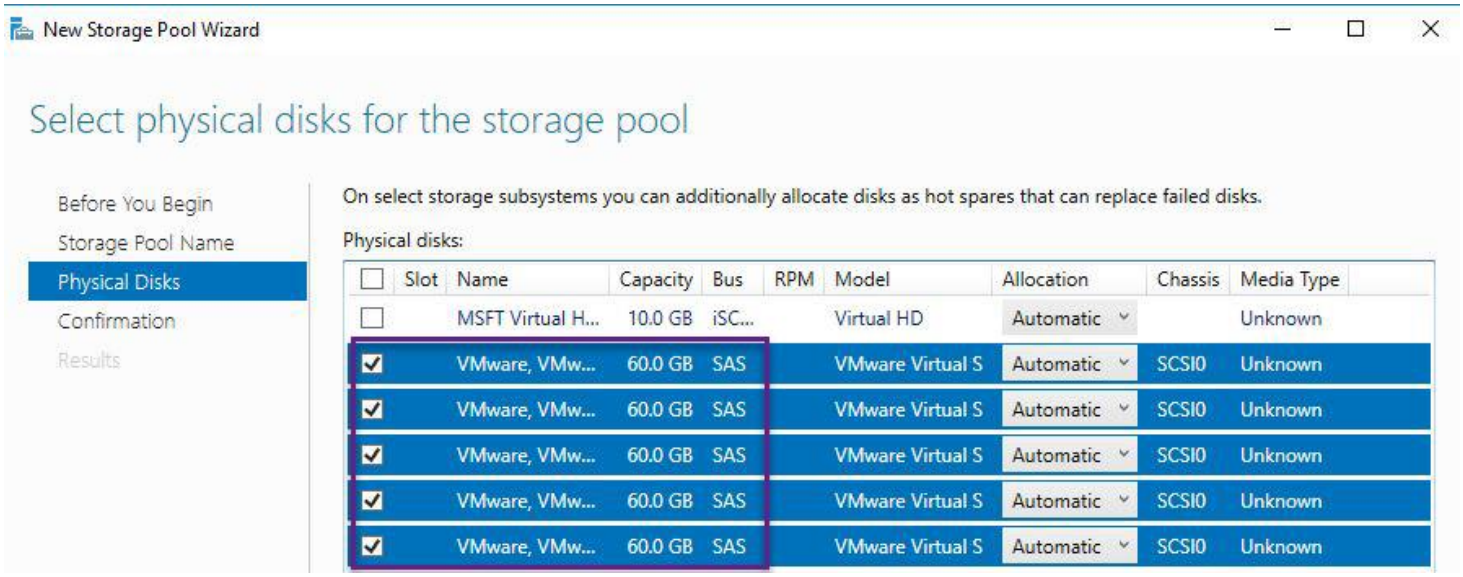


2- On **FSRM01**, in Server Manager, in the navigation pane, click Storage Pools.



Initiate the first storage pool, labeled as SPool01, utilizing five hard drives.

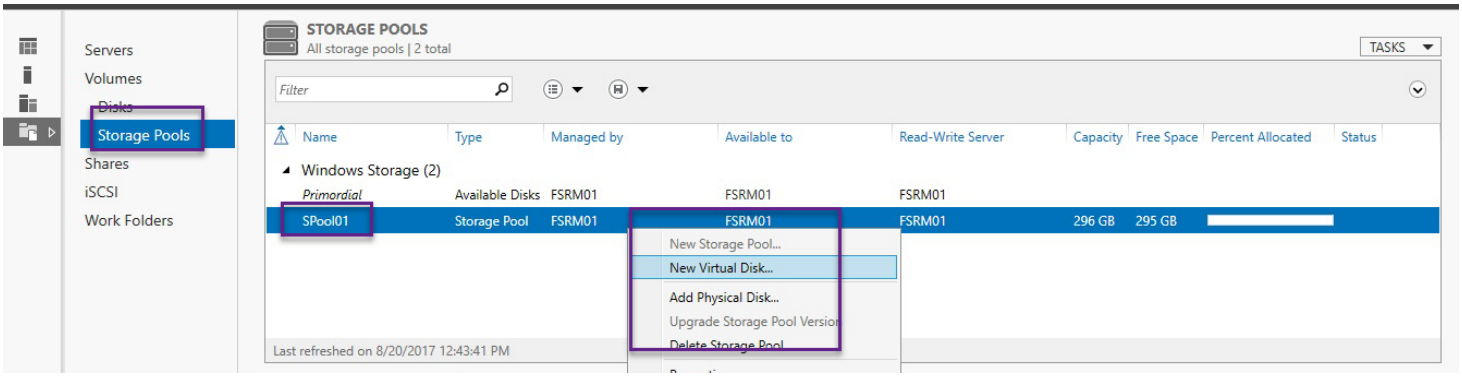


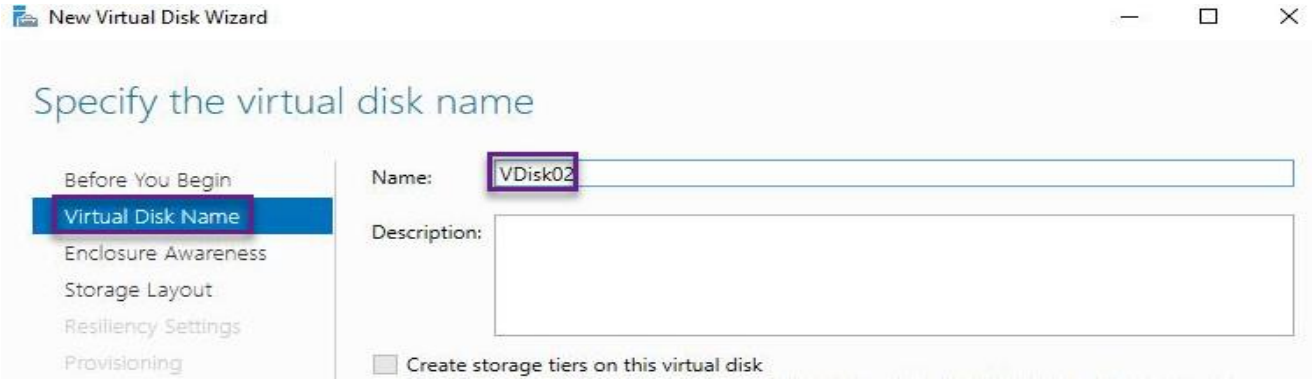


Currently, the initial storage pool has been set up using five hard drives, culminating in a combined capacity of 300GB.

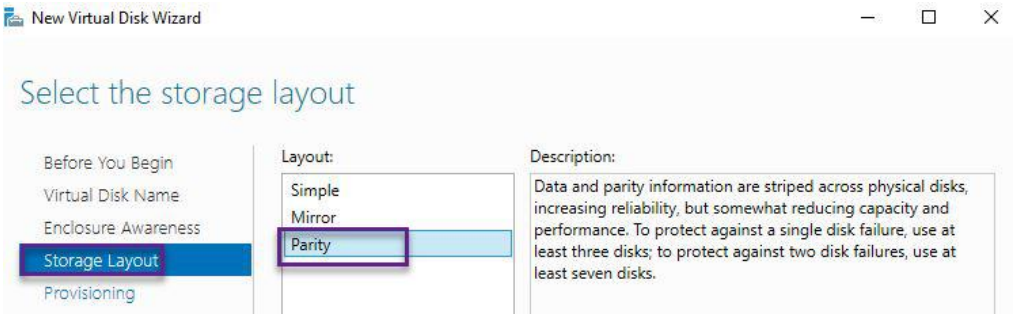
Task 2: Create a parity disk using created Storage Pool (Spool01)

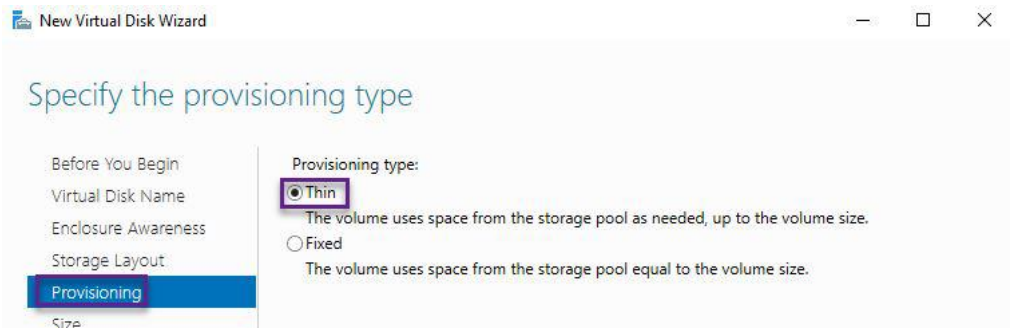
1- In Server Manager, in the STORAGE POOLS pane, click **SPool1**, and follow the below figures

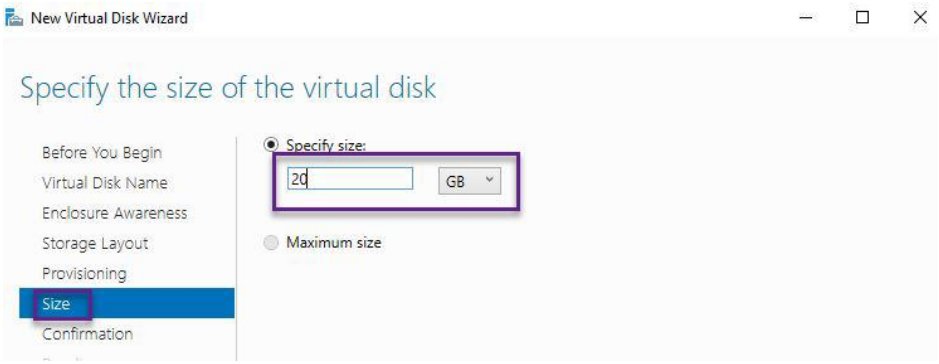


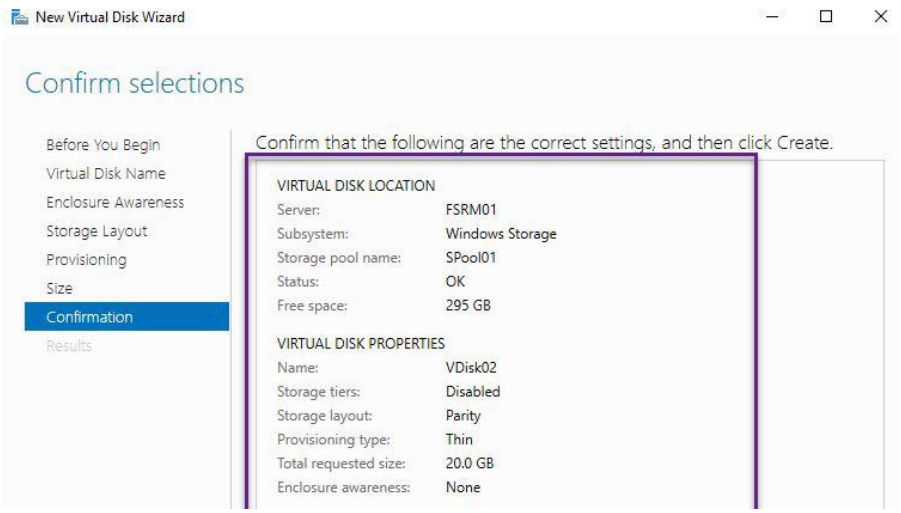


For this lab, we allocate just 20 GB from Spool01, which has a capacity of 300 GB, leaving the rest available for creating an additional virtual disk.

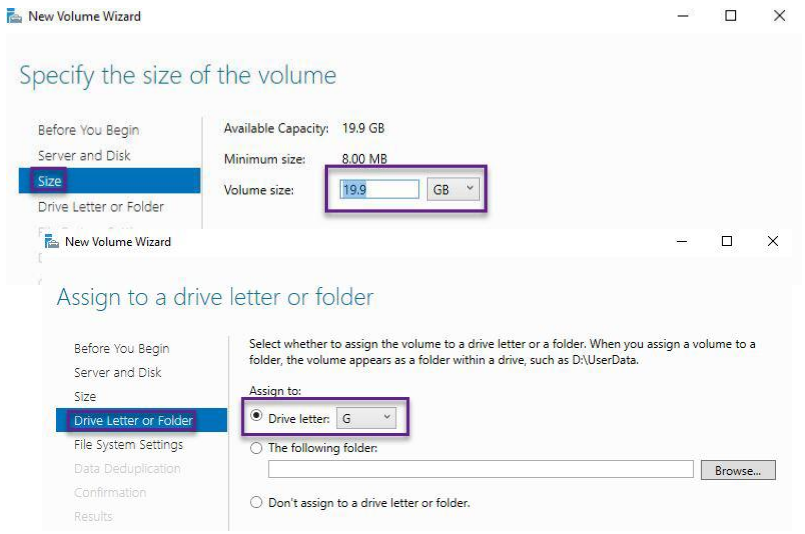


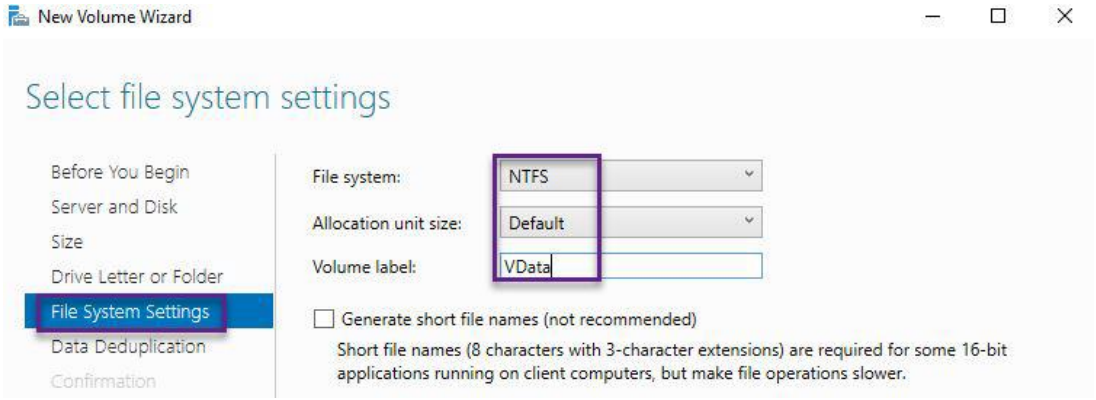


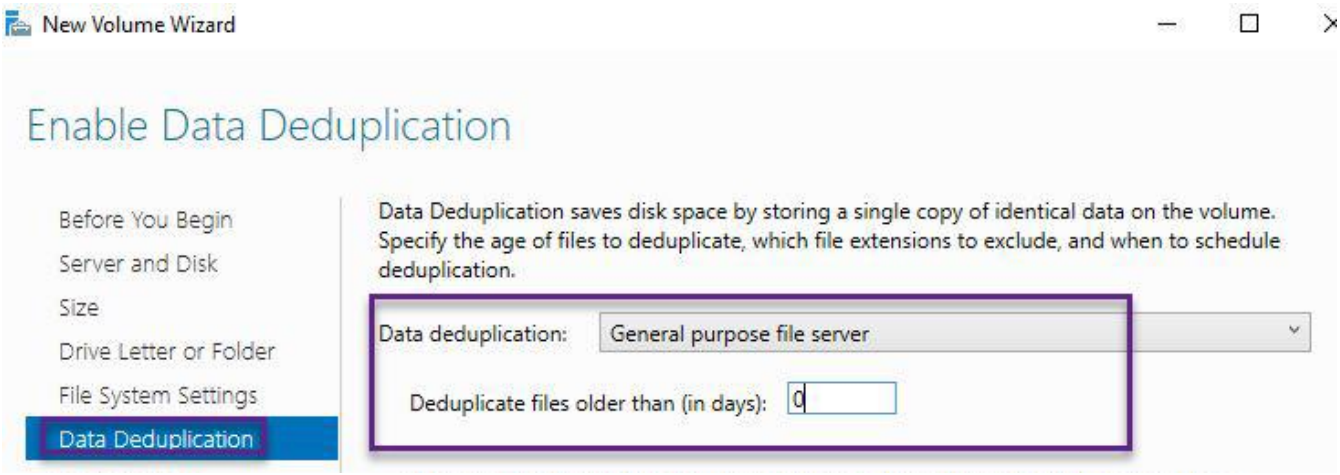

New Virtual Disk Wizard
Specify the size of the virtual disk
Before You Begin
Virtual Disk Name
Enclosure Awareness
Storage Layout
Provisioning
Size
Confirmation
Specify size:
20
GB
Maximum size

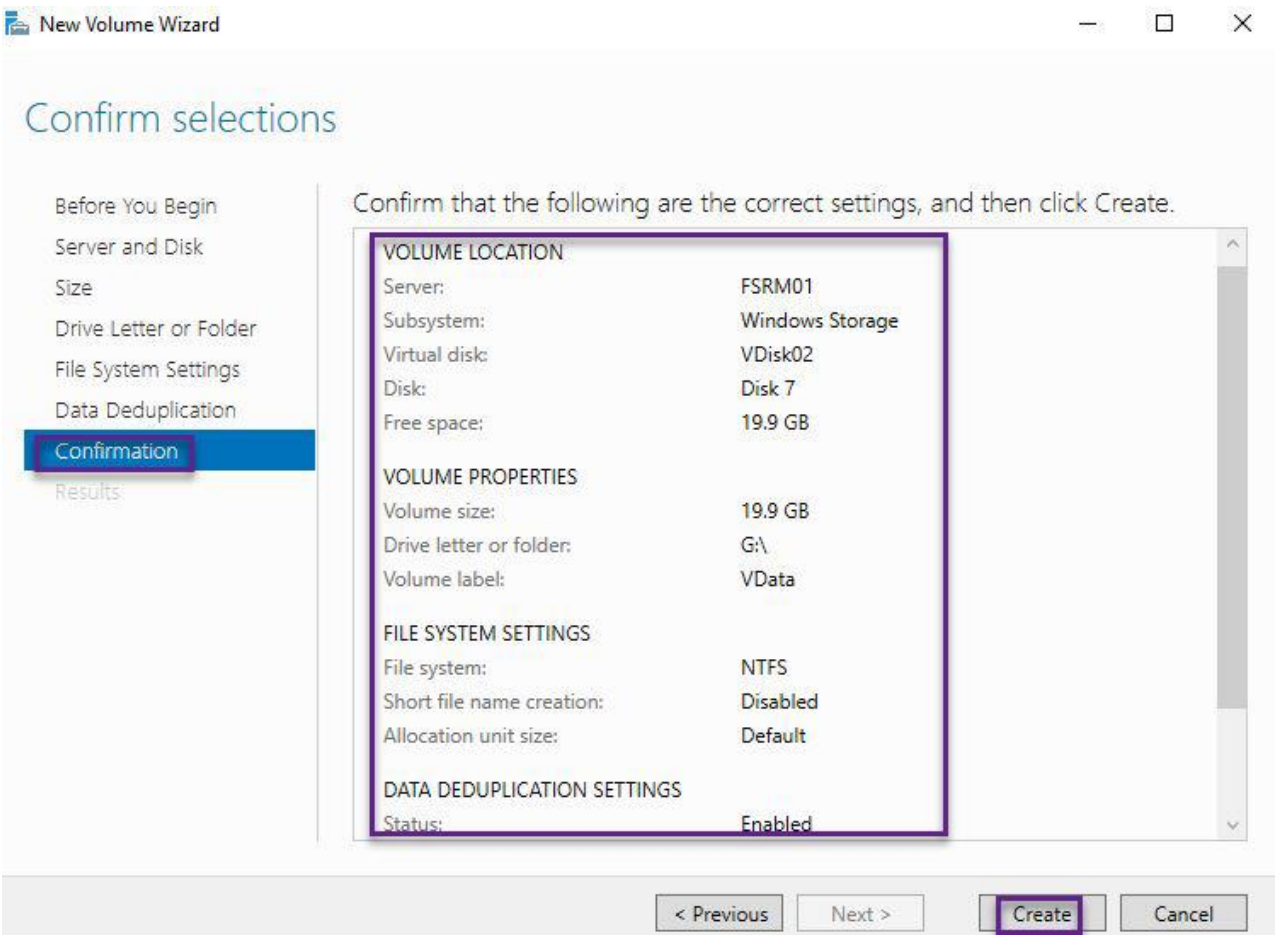

New Virtual Disk Wizard
Confirm selections
Before You Begin
Virtual Disk Name
Enclosure Awareness
Storage Layout
Provisioning
Size
Confirmation
Results
Confirm that the following are the correct settings, and then click Create.
VIRTUAL DISK LOCATION
Server: FSRM01
Subsystem: Windows Storage
Storage pool name: SPool01
Status: OK
Free space: 295 GB
VIRTUAL DISK PROPERTIES
Name: VDisk02
Storage tiers: Disabled
Storage layout: Parity
Provisioning type: Thin
Total requested size: 20.0 GB
Enclosure awareness: None

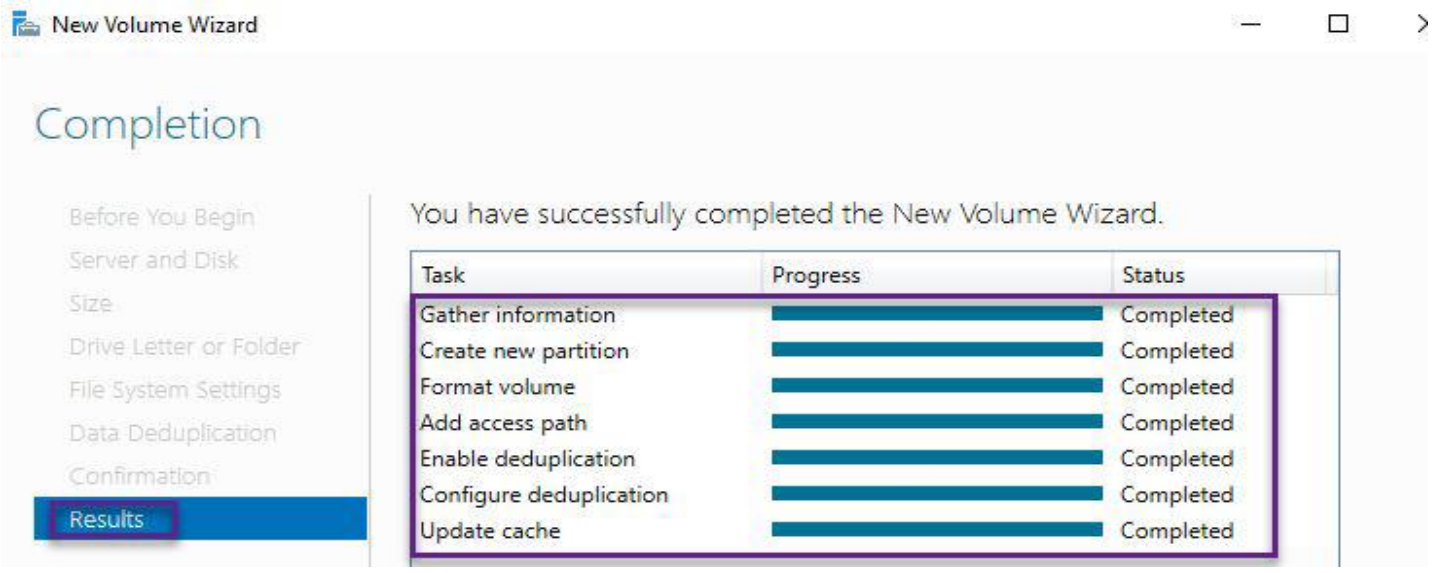
Task 3: create a volume based on parity disk that we just created



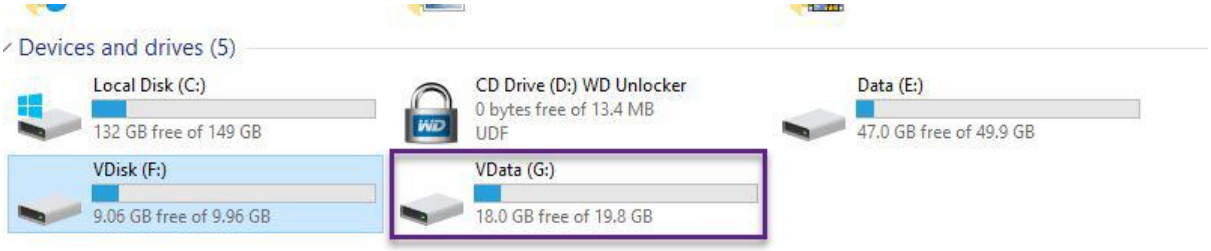





New Volume Wizard
Confirm selections
Before You Begin
Server and Disk
Size
Drive Letter or Folder
File System Settings
Data Deduplication
Confirmation
Results
Confirm that the following are the correct settings, and then click Create.
VOLUME LOCATION
Server: FSRM01
Subsystem: Windows Storage
Virtual disk: VDisk02
Disk: Disk 7
Free space: 19.9 GB
VOLUME PROPERTIES
Volume size: 19.9 GB
Drive letter or folder: G:\
Volume label: VData
FILE SYSTEM SETTINGS
File system: NTFS
Short file name creation: Disabled
Allocation unit size: Default
DATA DEDUPLICATION SETTINGS
Status: Enabled
< Previous
Next >
Create
Cancel

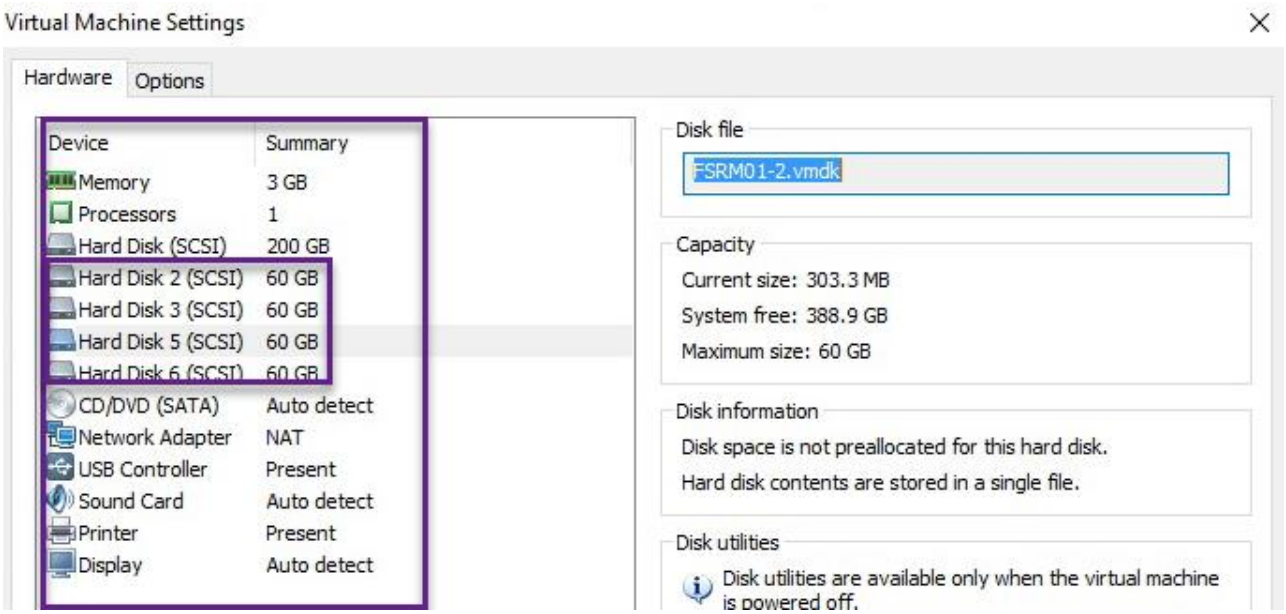

New Volume Wizard
Completion
Before You Begin
Server and Disk
Size
Drive Letter or Folder
File System Settings
Data Deduplication
Confirmation
Results
You have successfully completed the New Volume Wizard.
Task
Progress
Status
Gather information Completed
Create new partition Completed
Format volume Completed
Add access path Completed
Enable deduplication Completed
Configure deduplication Completed
Update cache Completed

Volume with parity is create

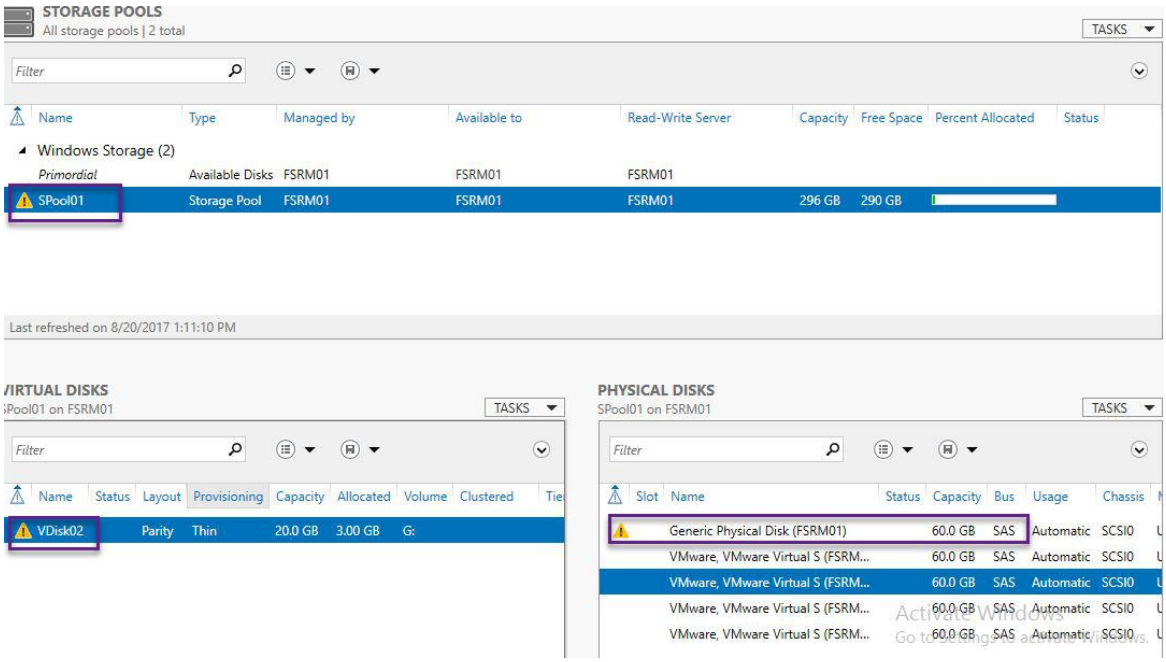


Task 4: test What does the parity do when one disk fail (Disconnect one disk)

In this task, detach one of the five disks that were incorporated into the storage pool.

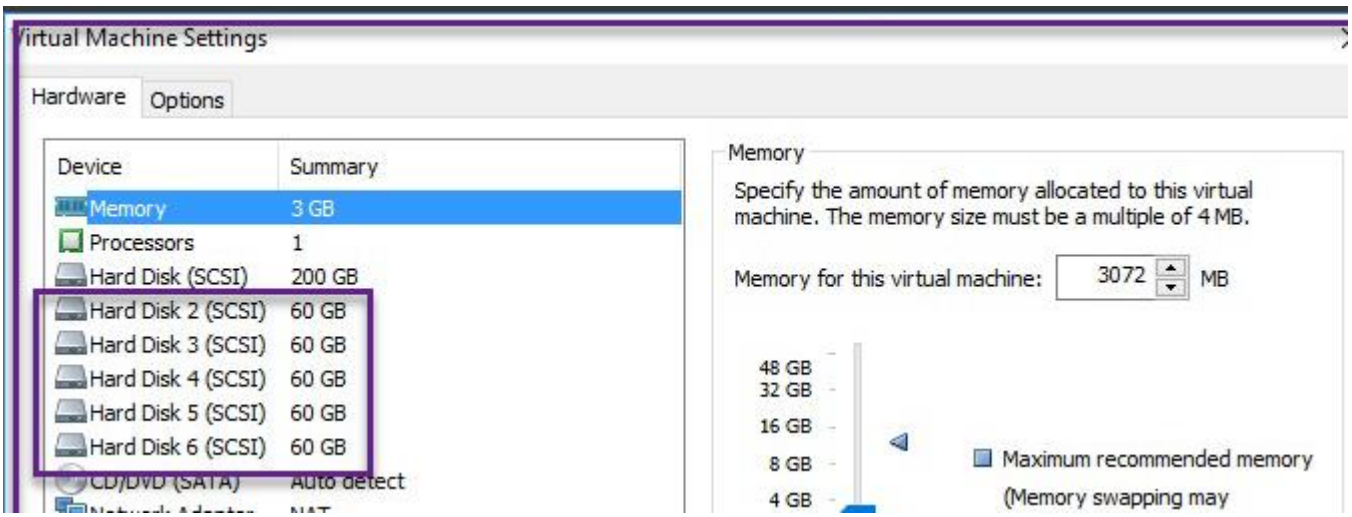


Once the disk is removed, a warning message shows up on our virtual parity disk. However, the disk remains accessible, as the parity disk system can operate with a minimum of three disks and we currently have four available.

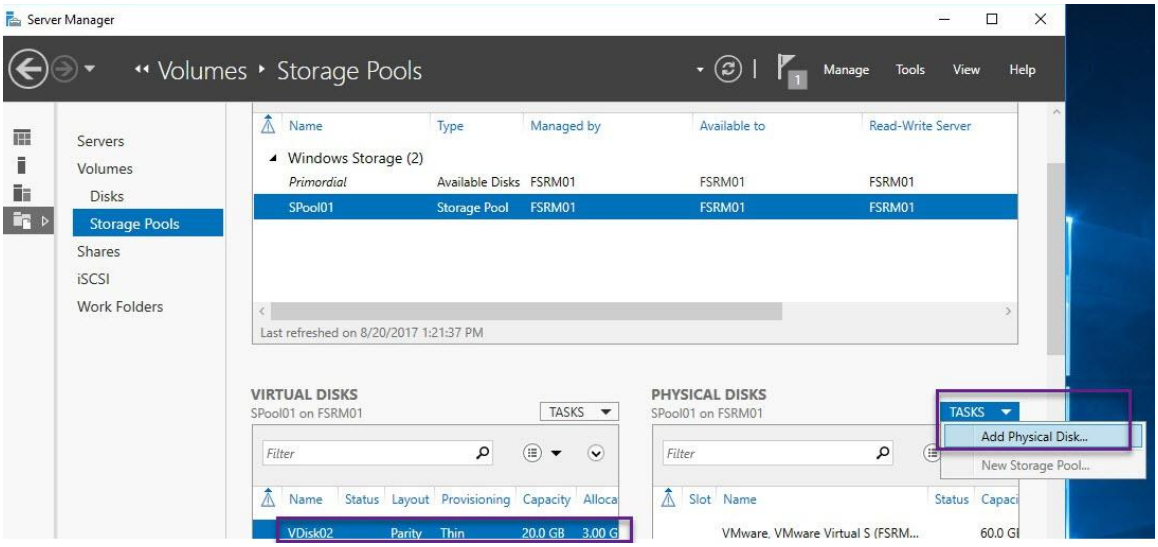


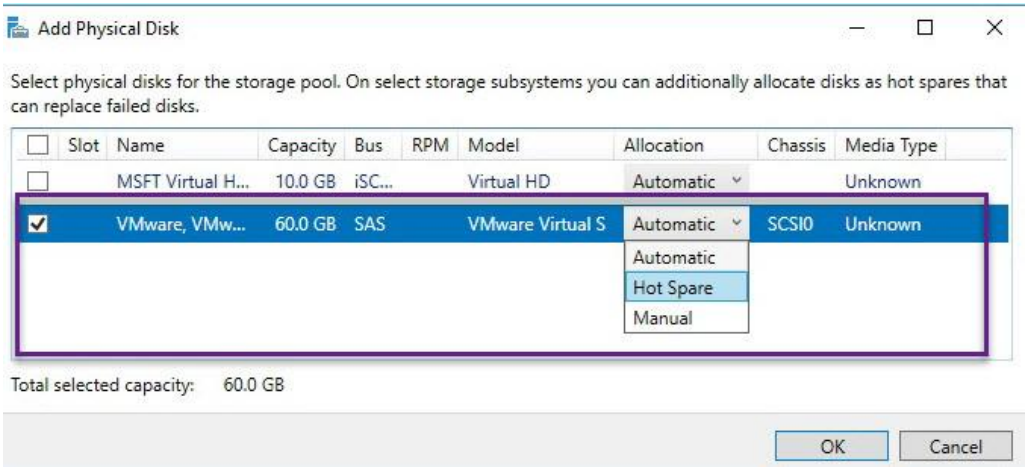
Task 5: recover disk failure with parity

1- Install a new disk with the same size as the one that was removed to the server.

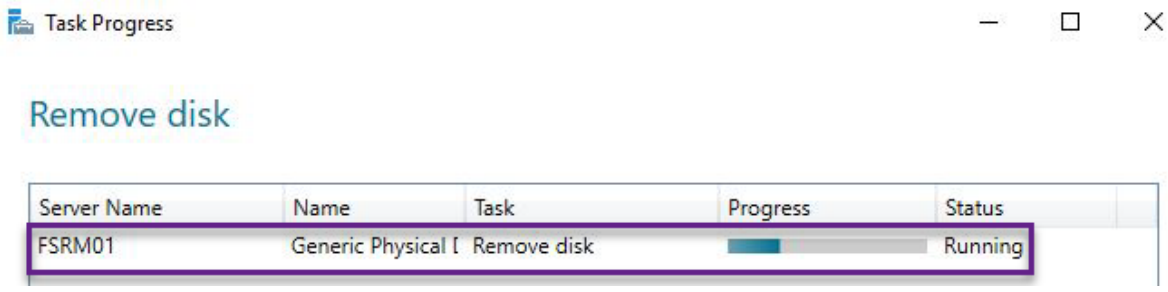


2- Add the new disk to parity disk group so we can replace the failed disk, as explained in below figures

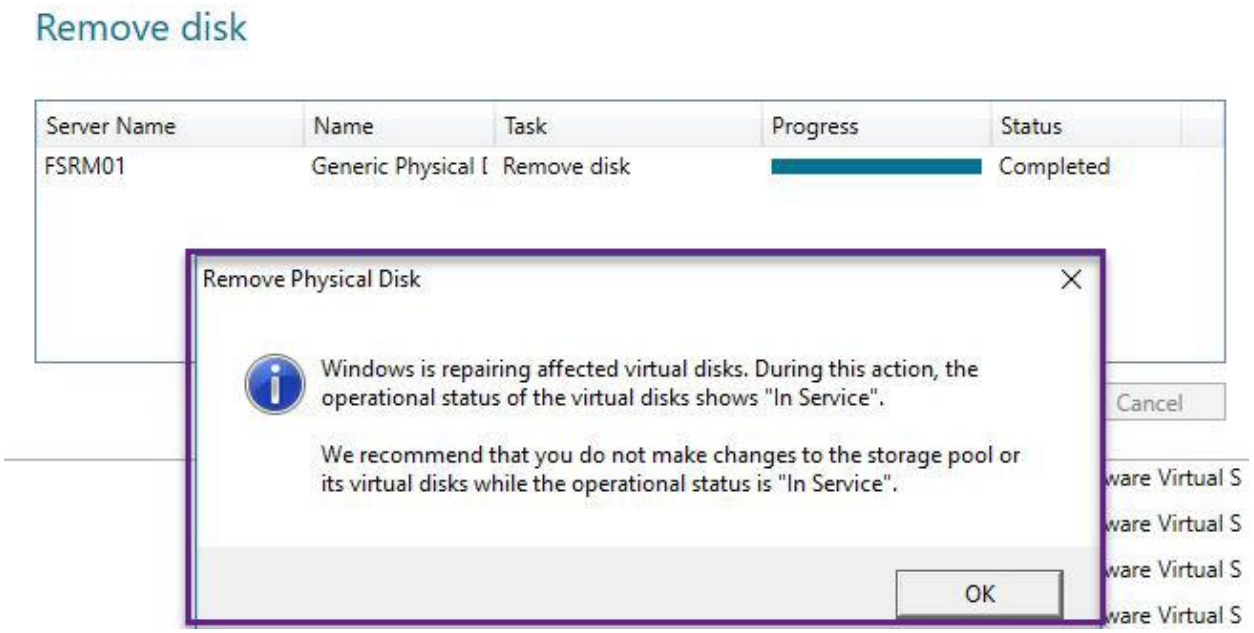




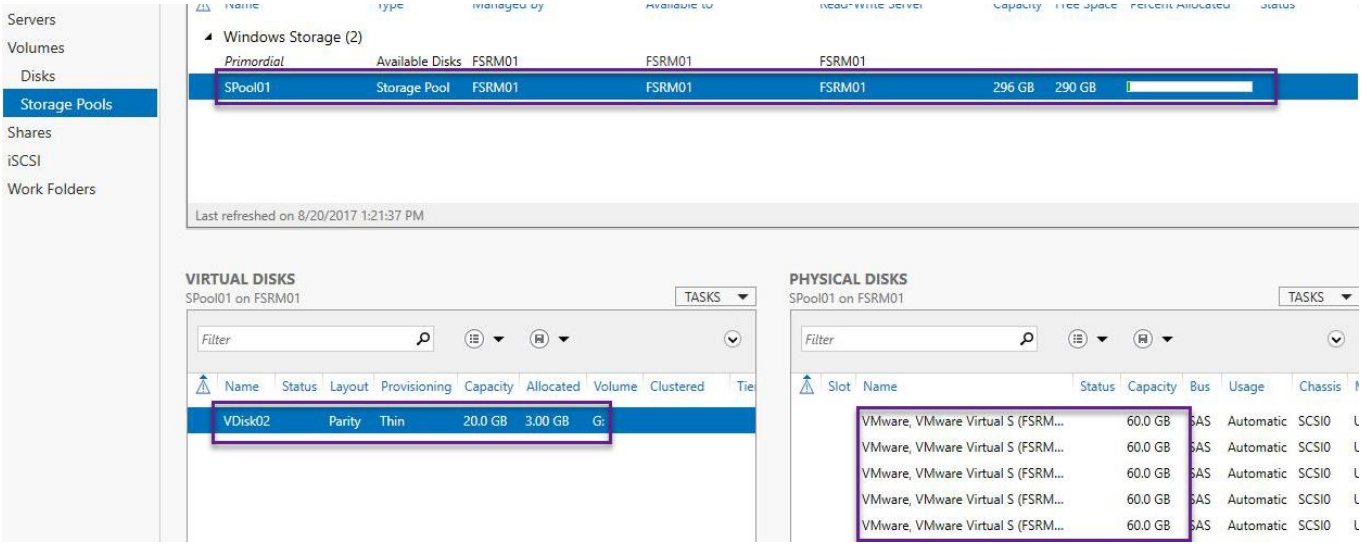
3- After disk added successfully, you can remove failed disk from the pool



4- Parity will resolve the issue by integrating the new disk into the RAID 5 array.

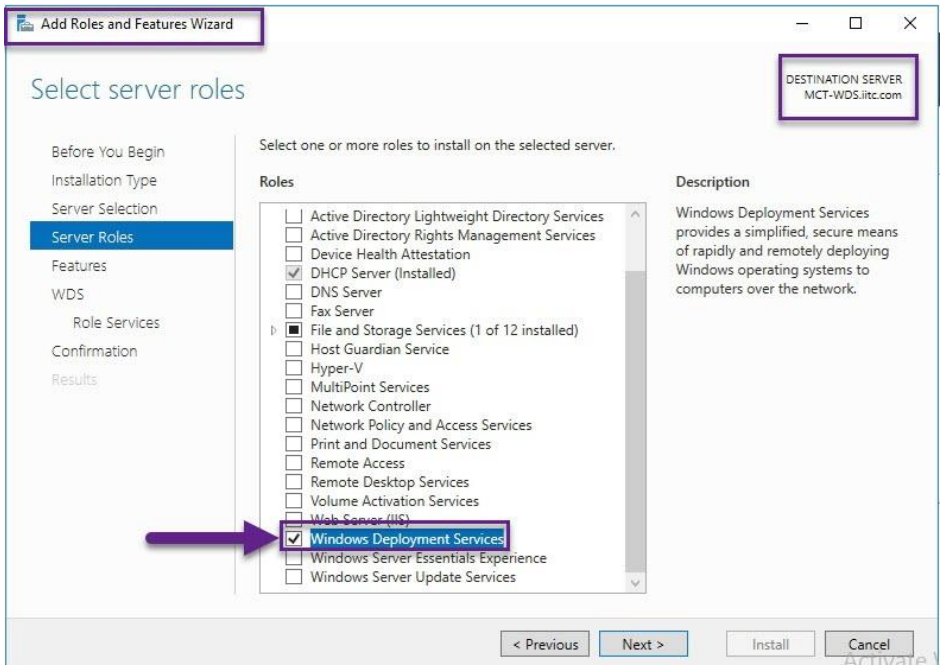


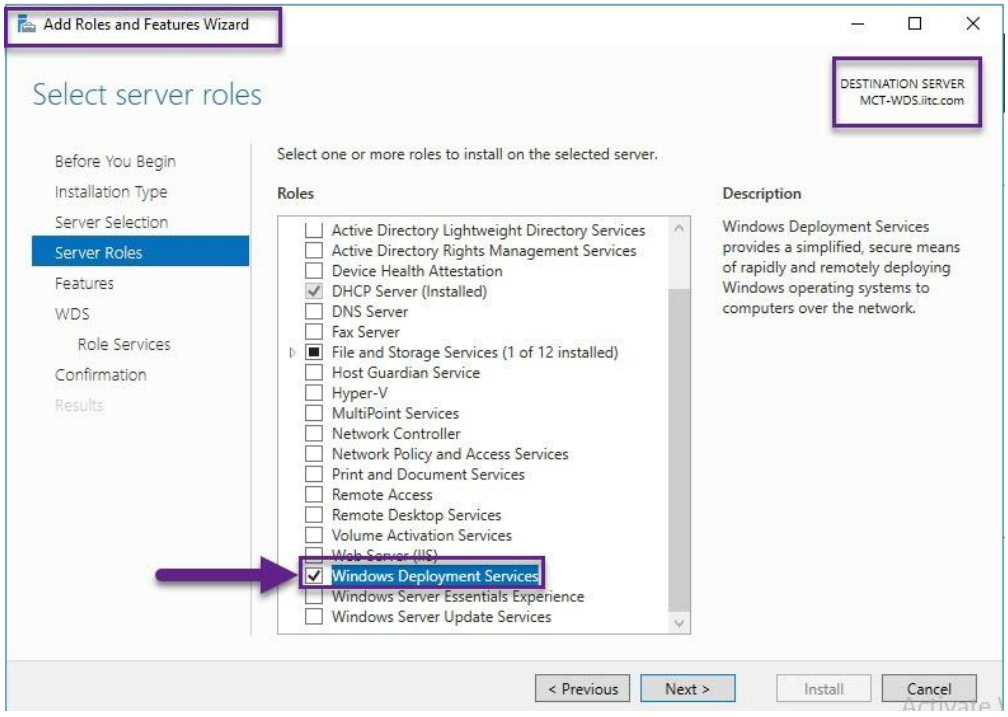
5- The faulty disk has been successfully replaced.

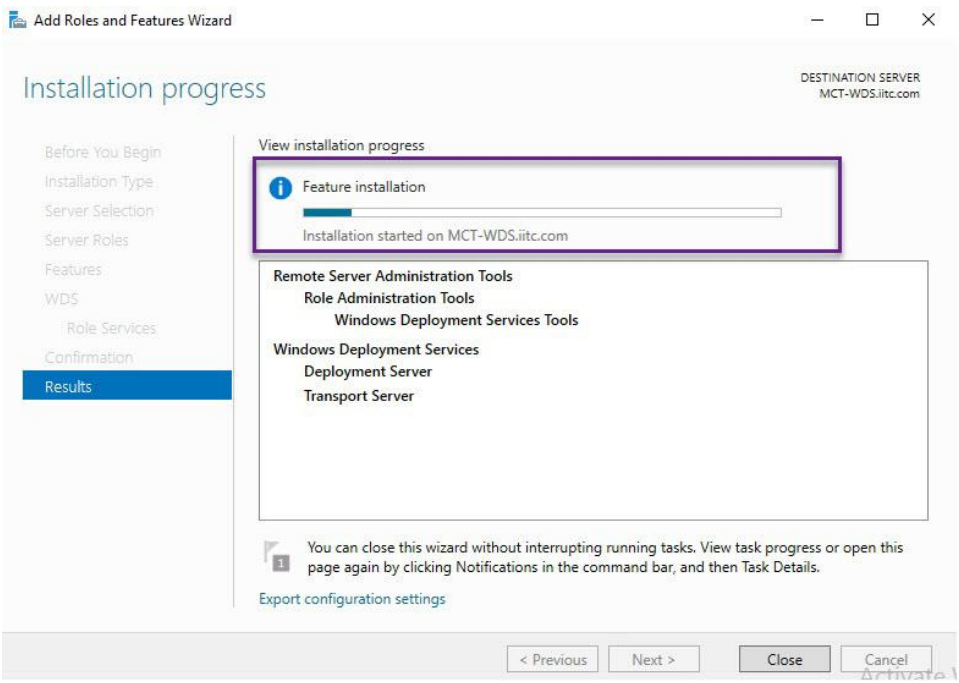


Windows Deployment Services (WDS)

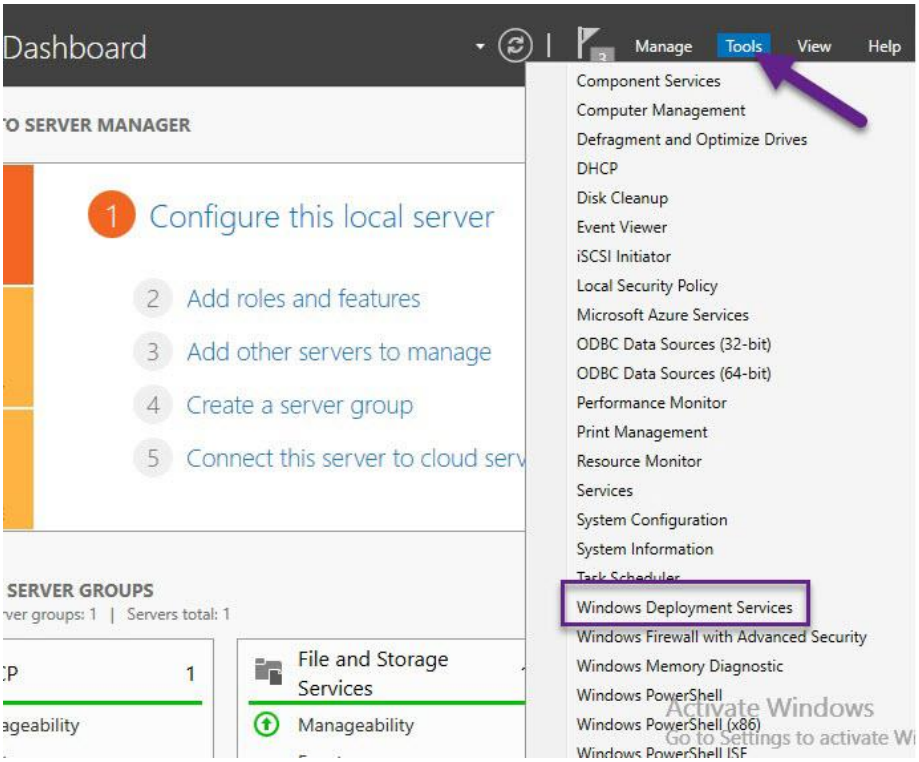
Install WDS Feature

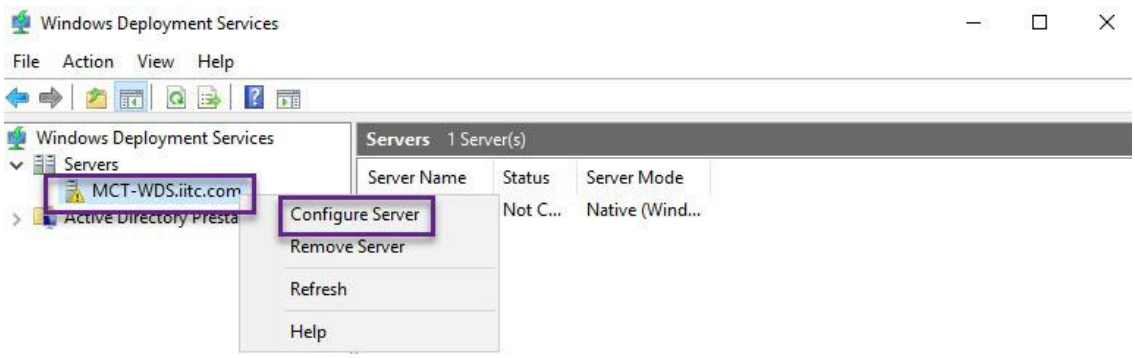


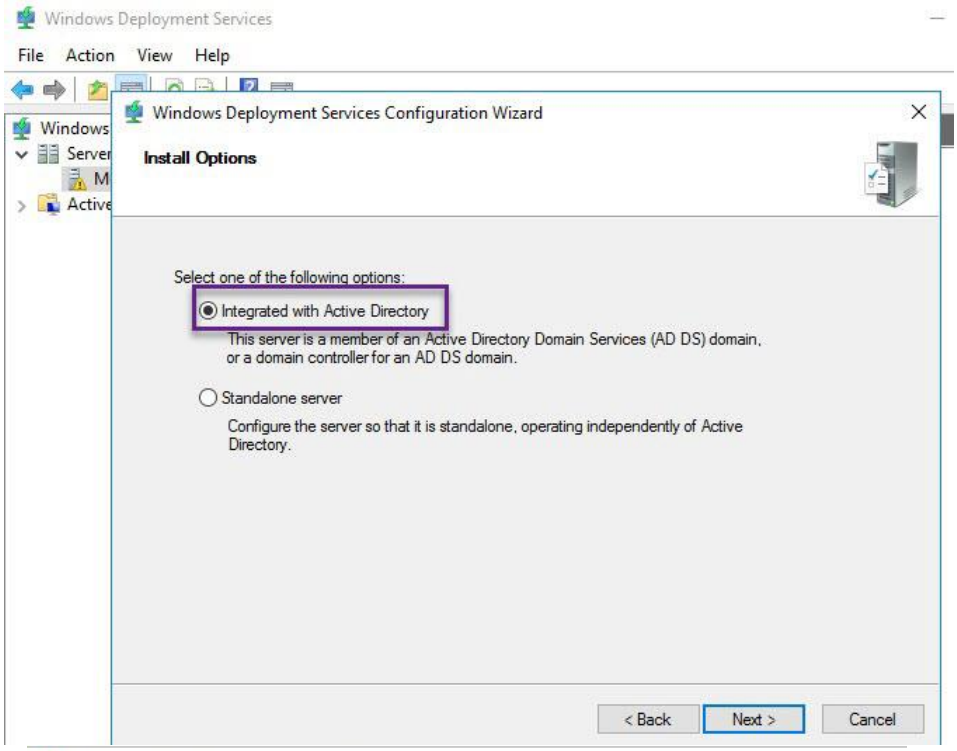


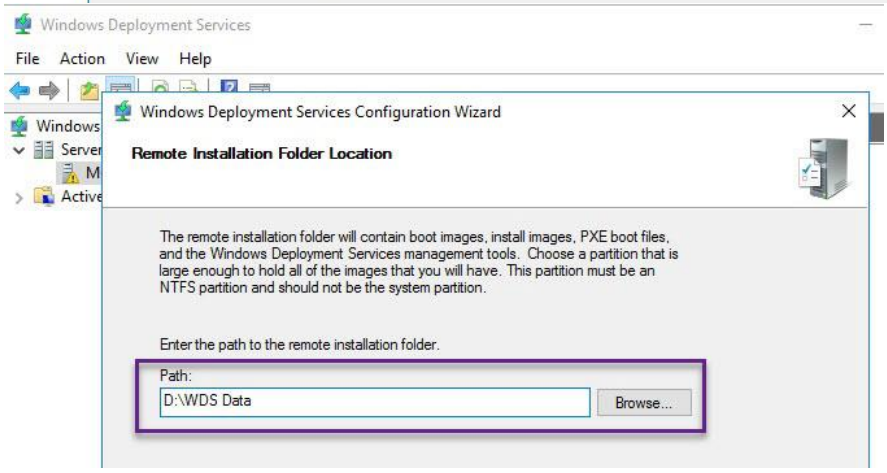


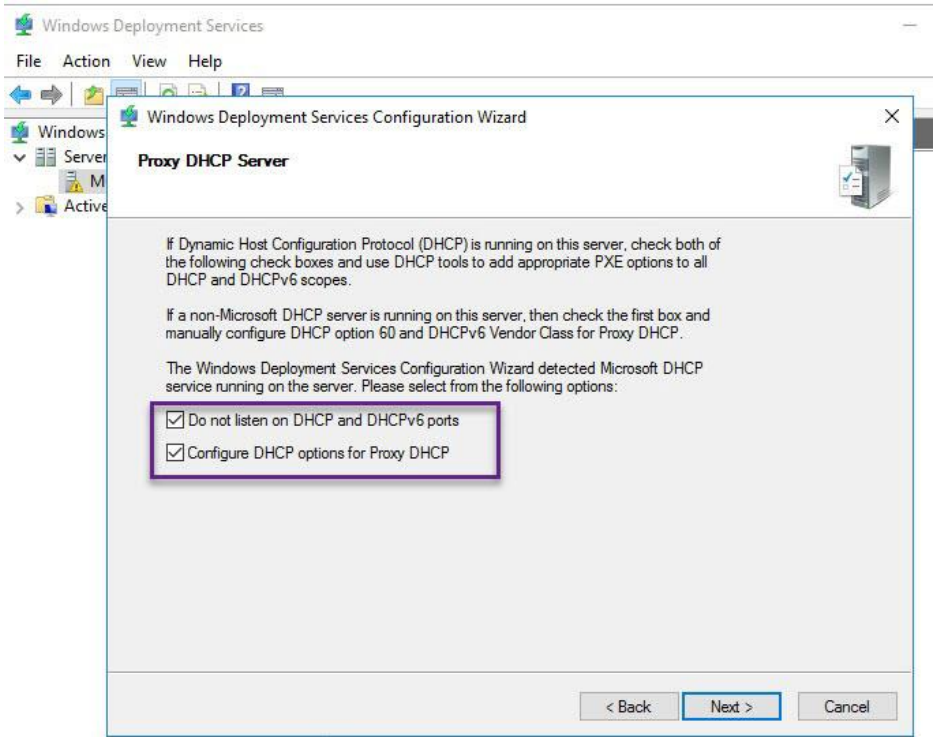
Configure WDS Service

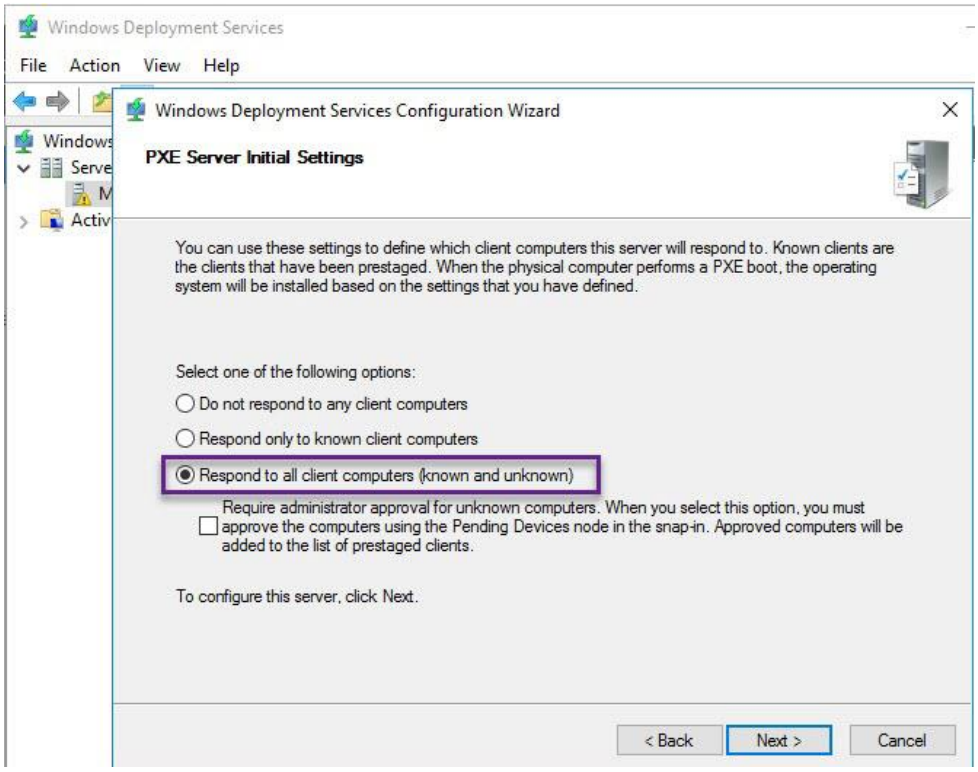


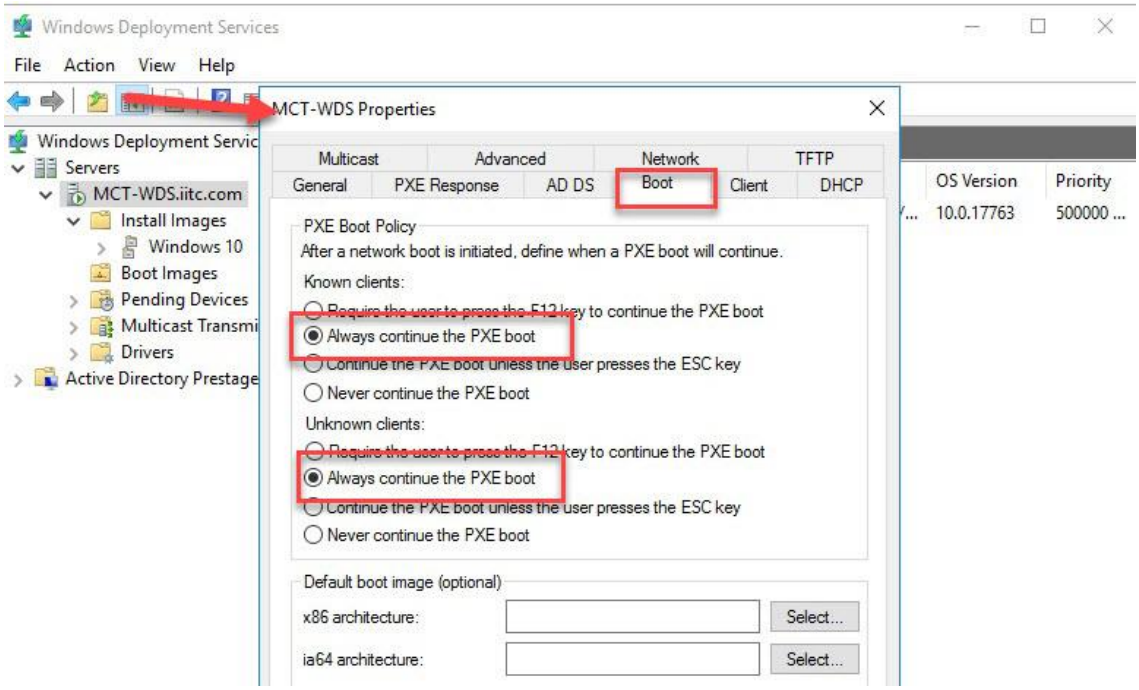

Windows Deployment Services
File Action View Help
Windows Deployment Services
Servers
MCT-WDS.iitc.com
Active Directory Presta
Servers 1 Server(s)
Server Name
Status
Server Mode
Not C...
Native (Wind...
Configure Server
Remove Server
Refresh
Help


Windows Deployment Services
File Action View Help
Windows Deployment Services Configuration Wizard
Install Options
Select one of the following options:
Integrated with Active Directory
This server is a member of an Active Directory Domain Services (AD DS) domain, or a domain controller for an AD DS domain.
Standalone server
Configure the server so that it is standalone, operating independently of Active Directory.
< Back
Next >
Cancel

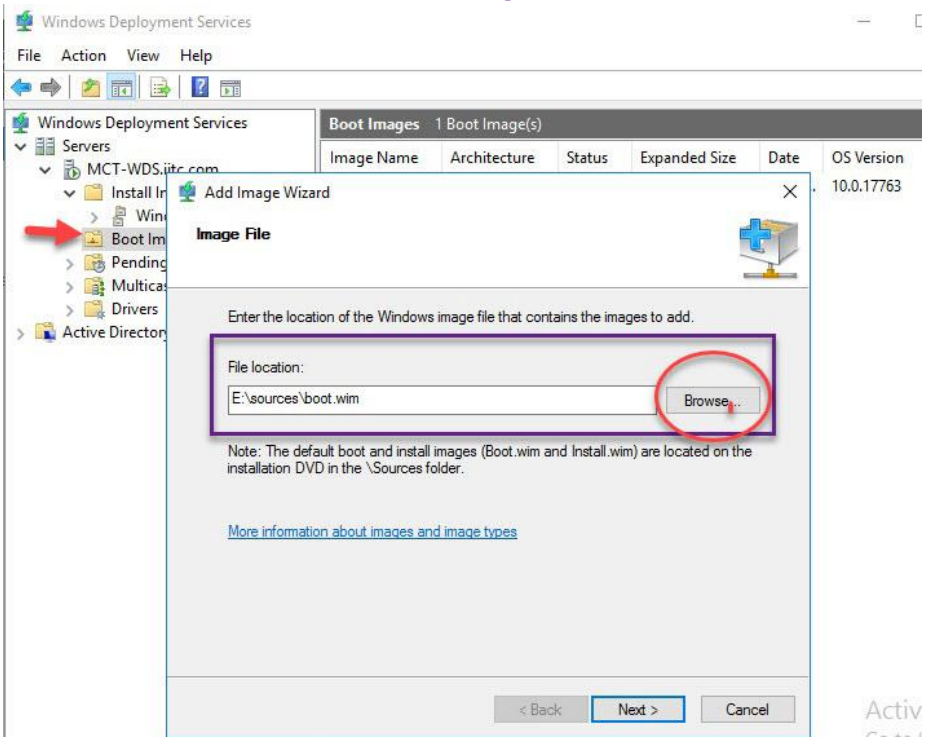

Windows Deployment Services
File Action View Help
Windows Deployment Services Configuration Wizard
Remote Installation Folder Location
The remote installation folder will contain boot images, install images, PXE boot files, and the Windows Deployment Services management tools. Choose a partition that is large enough to hold all of the images that you will have. This partition must be an NTFS partition and should not be the system partition.
Enter the path to the remote installation folder.
Path:
D:\WDS Data
Browse...

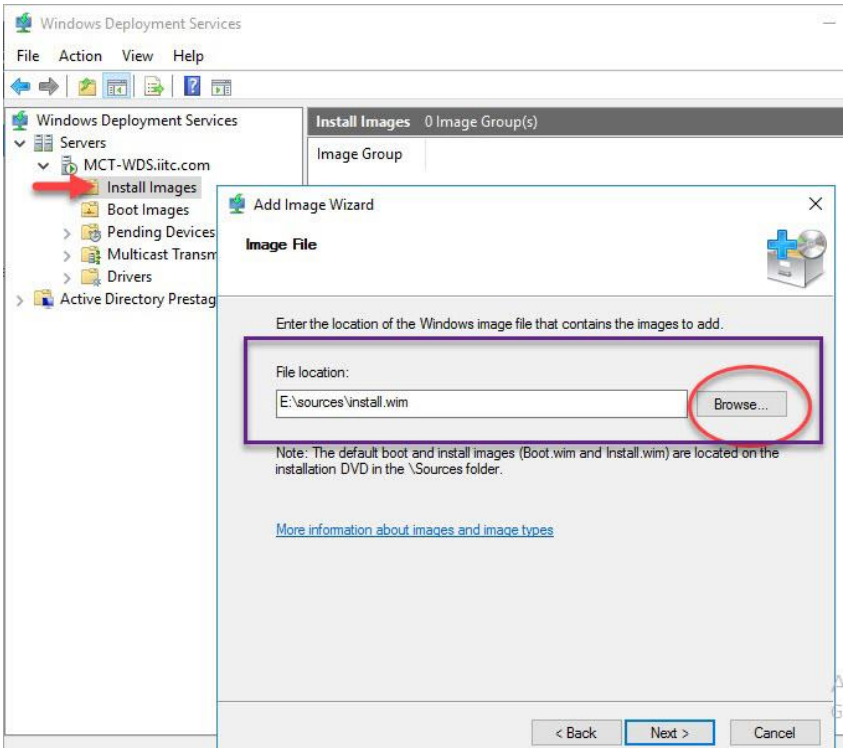

Windows Deployment Services
File Action View Help
Windows Deployment Services Configuration Wizard
Proxy DHCP Server
If Dynamic Host Configuration Protocol (DHCP) is running on this server, check both of the following check boxes and use DHCP tools to add appropriate PXE options to all DHCP and DHCPv6 scopes.
If a non-Microsoft DHCP server is running on this server, then check the first box and manually configure DHCP option 60 and DHCPv6 Vendor Class for Proxy DHCP.
The Windows Deployment Services Configuration Wizard detected Microsoft DHCP service running on the server. Please select from the following options:
Do not listen on DHCP and DHCPv6 ports
Configure DHCP options for Proxy DHCP
< Back
Next >
Cancel

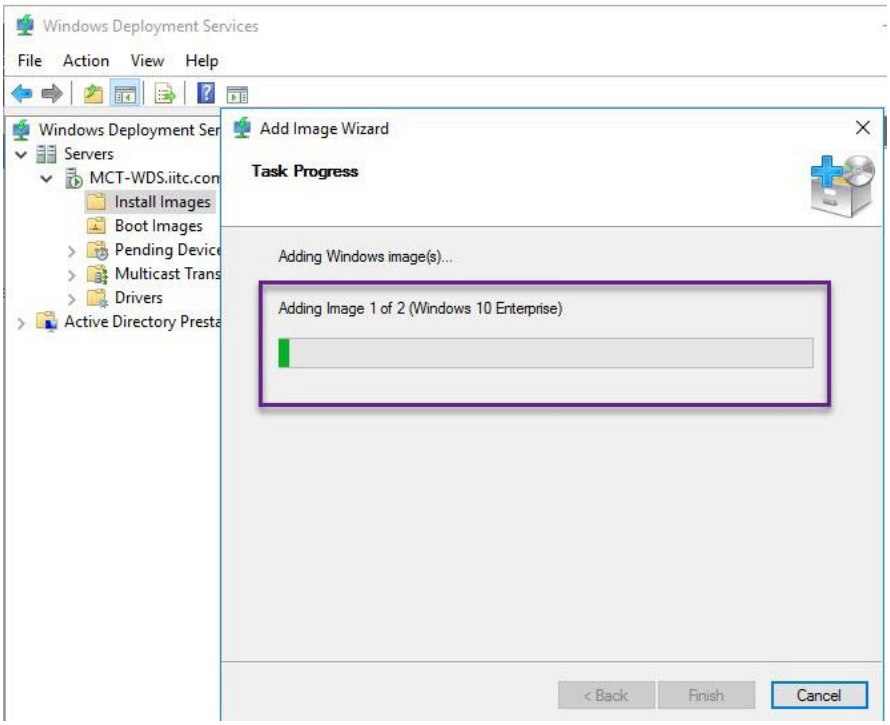

Windows Deployment Services
File Action View Help
Windows Deployment Services Configuration Wizard
PXE Server Initial Settings
You can use these settings to define which client computers this server will respond to. Known clients are the clients that have been prestaged. When the physical computer performs a PXE boot, the operating system will be installed based on the settings that you have defined.
Select one of the following options:
Do not respond to any client computers
Respond only to known client computers
Respond to all client computers (known and unknown)
Require administrator approval for unknown computers. When you select this option, you must approve the computers using the Pending Devices node in the snap-in. Approved computers will be added to the list of prestaged clients.
To configure this server, click Next.
< Back
Next >
Cancel



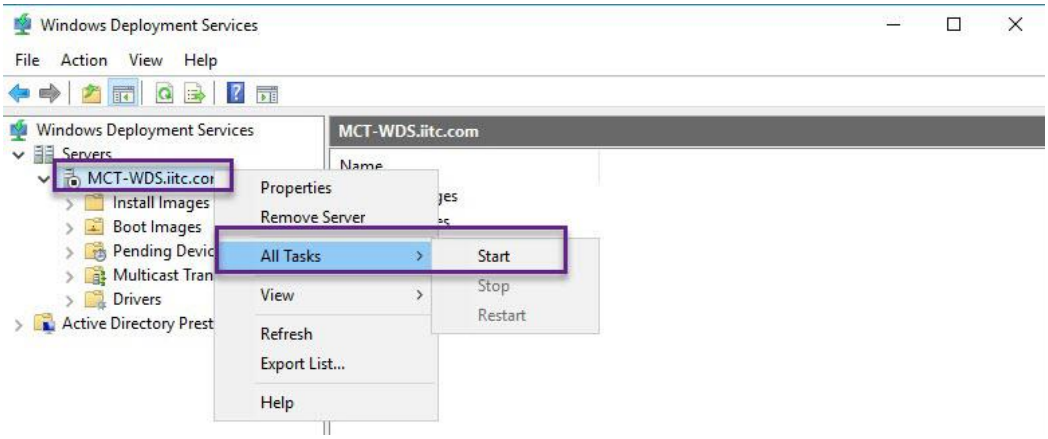
Using Windows DVD source add boot and install images to WDS




Windows Deployment Services
File Action View Help
Windows Deployment Services
Servers
MCT-WDS.iitc.com
Install Images
Boot Images
Pending Devices
Multicast Transm
Drivers
Active Directory Prestag
Install Images 0 Image Group(s)
Image Group
Add Image Wizard
Image File
Enter the location of the Windows image file that contains the images to add.
File location:
E:\sources\install.wim
Browse...
Note: The default boot and install images (Boot.wim and Install.wim) are located on the installation DVD in the \Sources folder.
More information about images and image types
< Back
Next >
Cancel

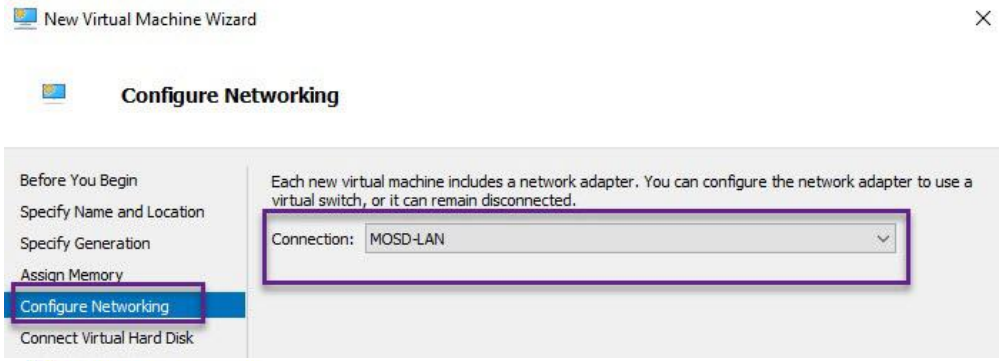

Windows Deployment Services
File Action View Help
Windows Deployment Ser
Servers
MCT-WDS.iitc.com
Install Images
Boot Images
Pending Device
Multicast Trans
Drivers
Active Directory Presta
Add Image Wizard
Task Progress
Adding Windows image(s)...
Adding Image 1 of 2 (Windows 10 Enterprise)
< Back
Finish
Cancel

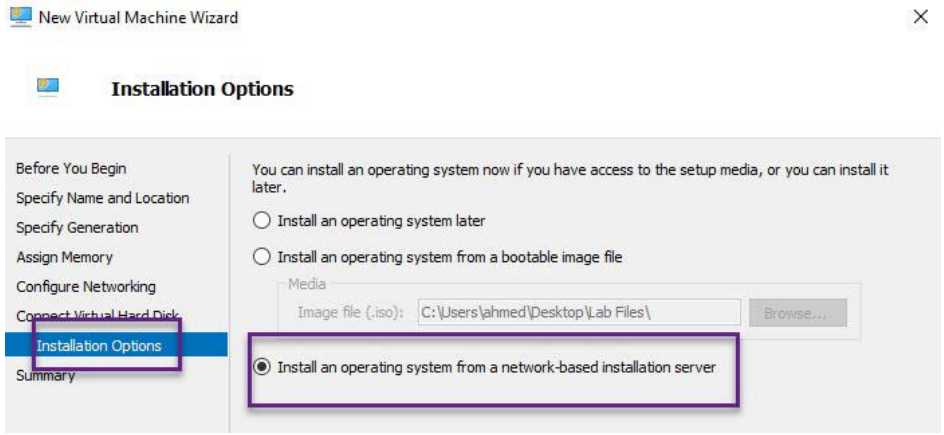
Now start WDS service



Testing

Please proceed with the creation of a virtual machine using the standard configuration, ensuring that the VM's network is linked to the same WDS and DHCP switch and set up for network boot.



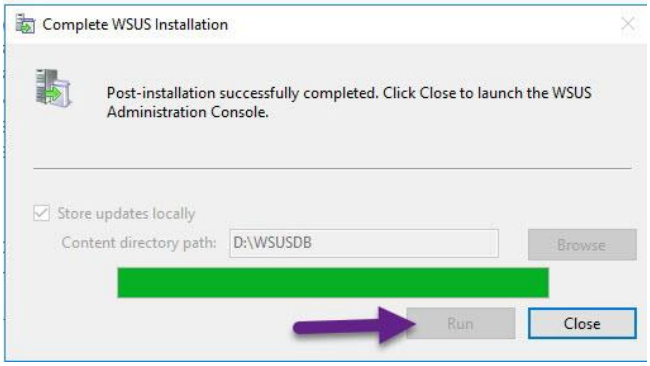


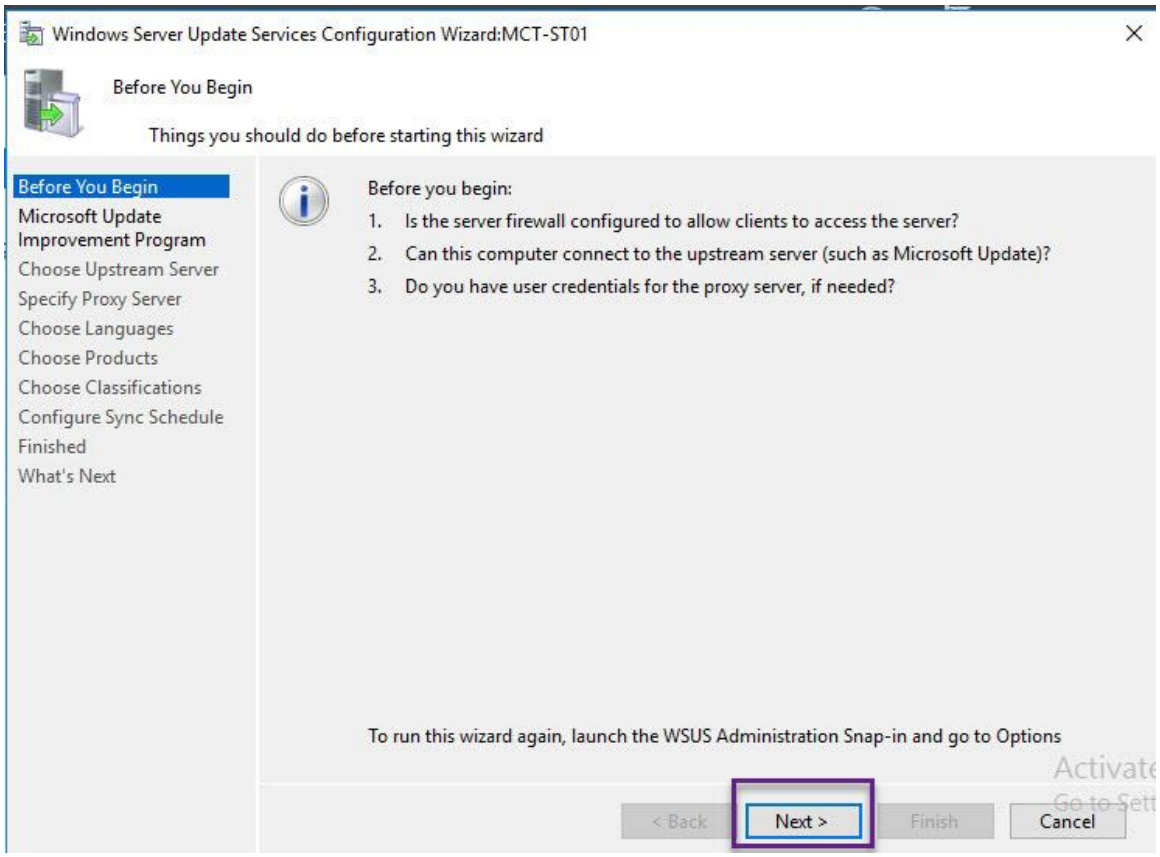
Now initiate the VM and begin the installation process.

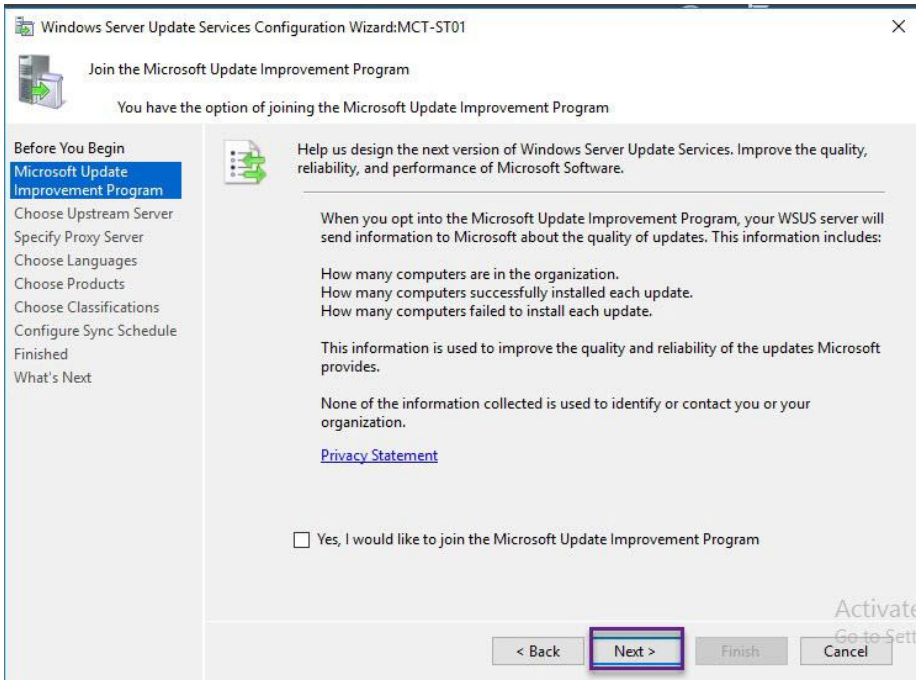
Windows Server Update Services (WSUS)

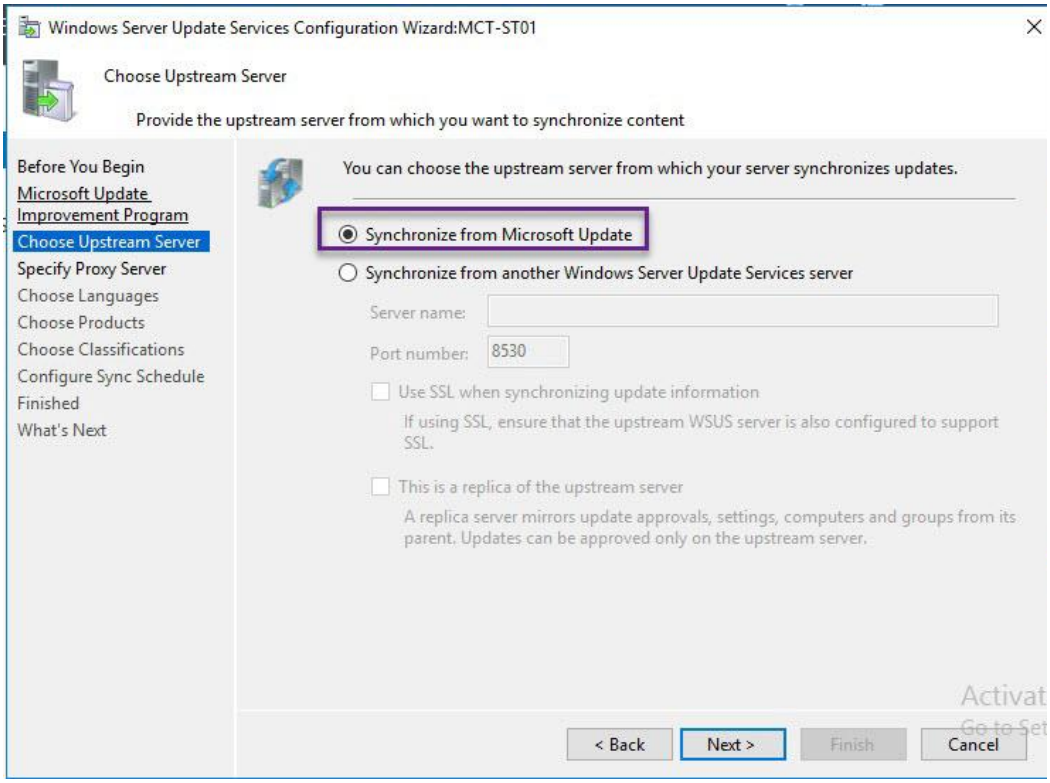
Configure WSUS Service

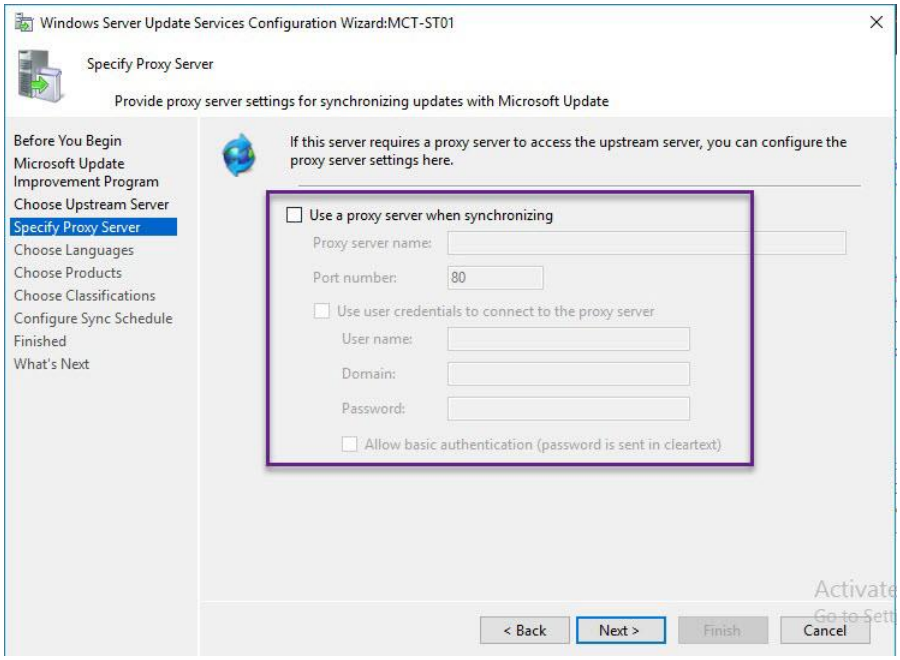
Once the role installation is complete, proceed with the following steps for configuration.

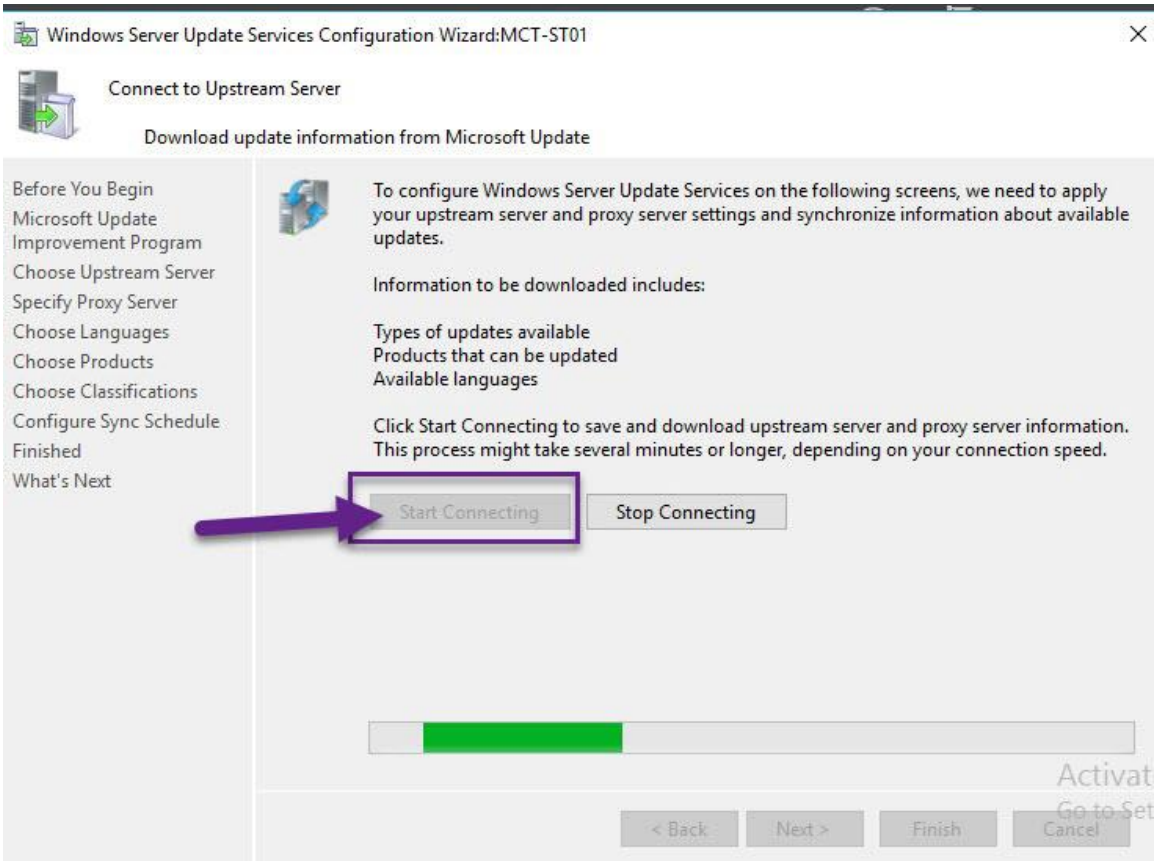


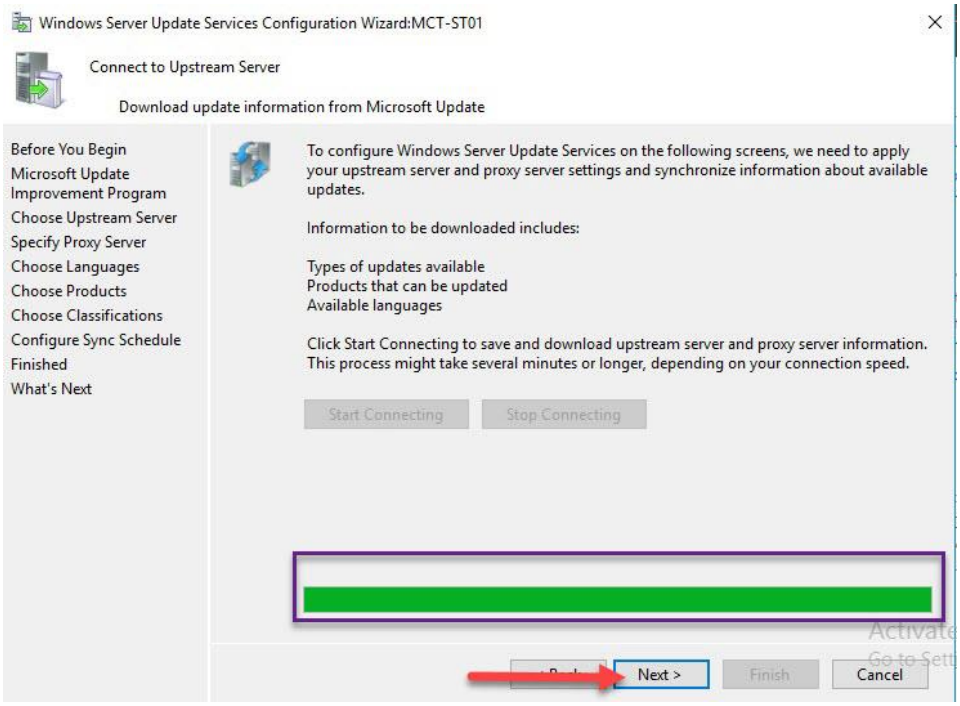



Windows Server Update Services Configuration Wizard:MCT-ST01
Join the Microsoft Update Improvement Program
You have the option of joining the Microsoft Update Improvement Program
Before You Begin
Microsoft Update Improvement Program
Choose Upstream Server
Specify Proxy Server
Choose Languages
Choose Products
Choose Classifications
Configure Sync Schedule
Finished
What's Next
Help us design the next version of Windows Server Update Services. Improve the quality, reliability, and performance of Microsoft Software.
When you opt into the Microsoft Update Improvement Program, your WSUS server will send information to Microsoft about the quality of updates. This information includes:
How many computers are in the organization.
How many computers successfully installed each update.
How many computers failed to install each update.
This information is used to improve the quality and reliability of the updates Microsoft provides.
None of the information collected is used to identify or contact you or your organization.
Privacy Statement
Yes, I would like to join the Microsoft Update Improvement Program
< Back
Next >
Finish
Cancel

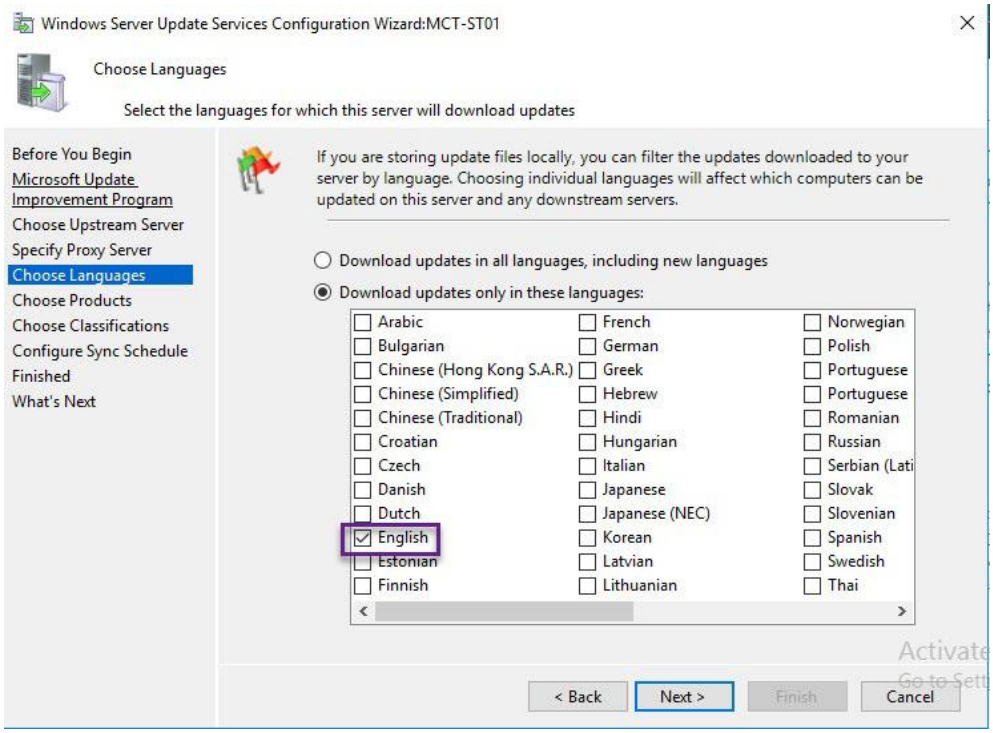

Windows Server Update Services Configuration Wizard:MCT-ST01
Choose Upstream Server
Provide the upstream server from which you want to synchronize content
Before You Begin
Microsoft Update Improvement Program
Choose Upstream Server
Specify Proxy Server
Choose Languages
Choose Products
Choose Classifications
Configure Sync Schedule
Finished
What's Next
You can choose the upstream server from which your server synchronizes updates.
Synchronize from Microsoft Update
Synchronize from another Windows Server Update Services server
Server name:
Port number:
8530
Use SSL when synchronizing update information
If using SSL, ensure that the upstream WSUS server is also configured to support SSL.
This is a replica of the upstream server
A replica server mirrors update approvals, settings, computers and groups from its parent. Updates can be approved only on the upstream server.
< Back
Next >
Finish
Cancel


Windows Server Update Services Configuration Wizard:MCT-ST01
Specify Proxy Server
Provide proxy server settings for synchronizing updates with Microsoft Update
Before You Begin
Microsoft Update Improvement Program
Choose Upstream Server
Specify Proxy Server
Choose Languages
Choose Products
Choose Classifications
Configure Sync Schedule
Finished
What's Next
If this server requires a proxy server to access the upstream server, you can configure the proxy server settings here.
Use a proxy server when synchronizing
Proxy server name:
Port number:
80
Use user credentials to connect to the proxy server
User name:
Domain:
Password:
Allow basic authentication (password is sent in cleartext)
< Back
Next >
Finish
Cancel

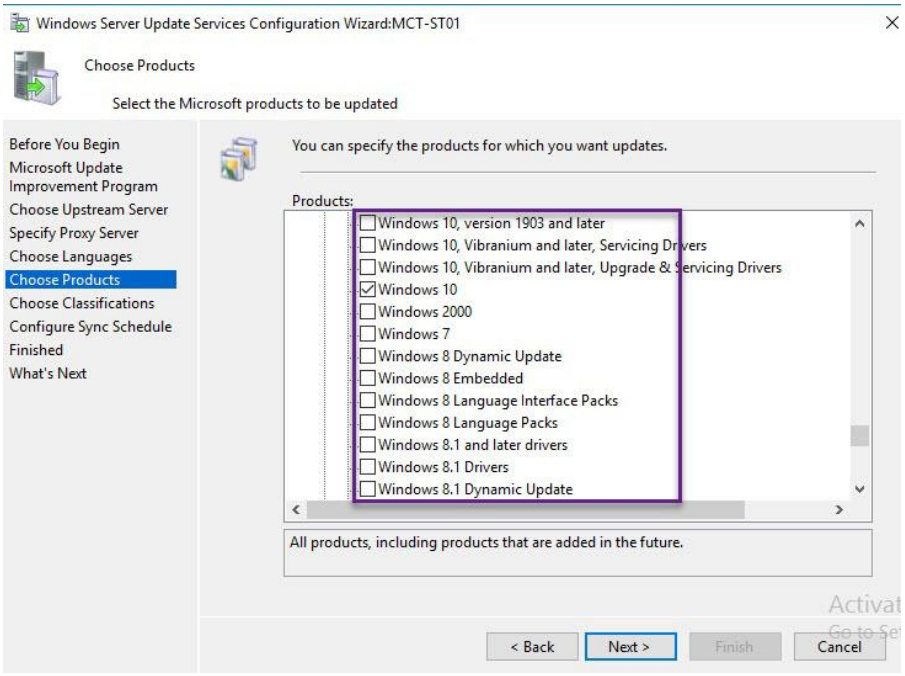

Windows Server Update Services Configuration Wizard:MCT-ST01
Connect to Upstream Server
Download update information from Microsoft Update
Before You Begin
Microsoft Update Improvement Program
Choose Upstream Server
Specify Proxy Server
Choose Languages
Choose Products
Choose Classifications
Configure Sync Schedule
Finished
What's Next
To configure Windows Server Update Services on the following screens, we need to apply your upstream server and proxy server settings and synchronize information about available updates.
Information to be downloaded includes:
Types of updates available
Products that can be updated
Available languages
Click Start Connecting to save and download upstream server and proxy server information. This process might take several minutes or longer, depending on your connection speed.
Start Connecting
Stop Connecting
< Back
Next >
Finish
Cancel



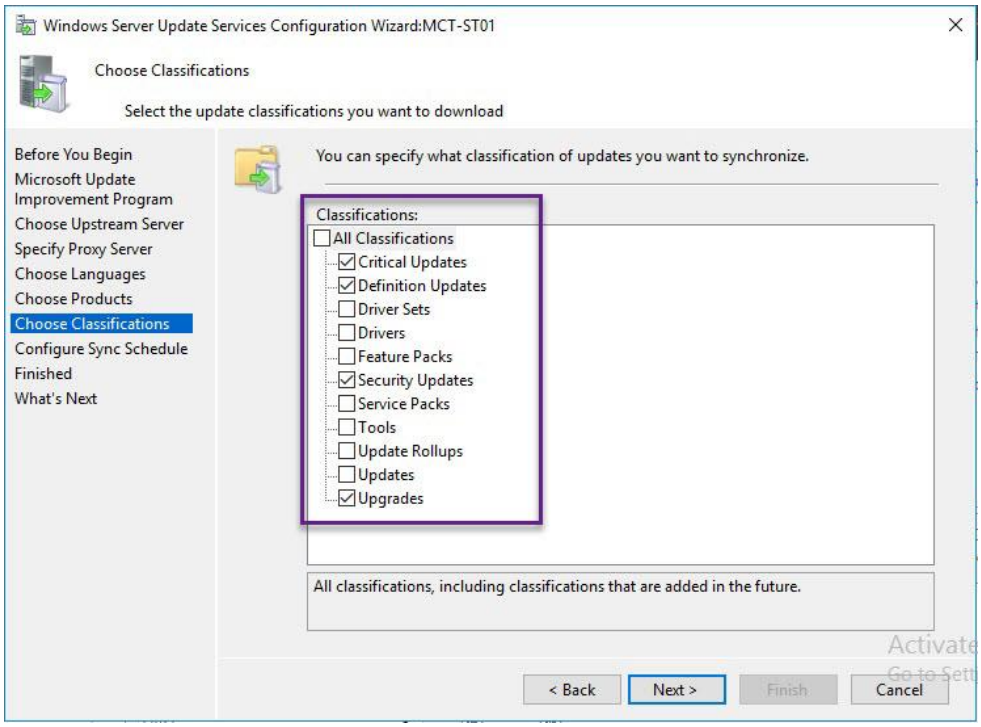
Select Update Language



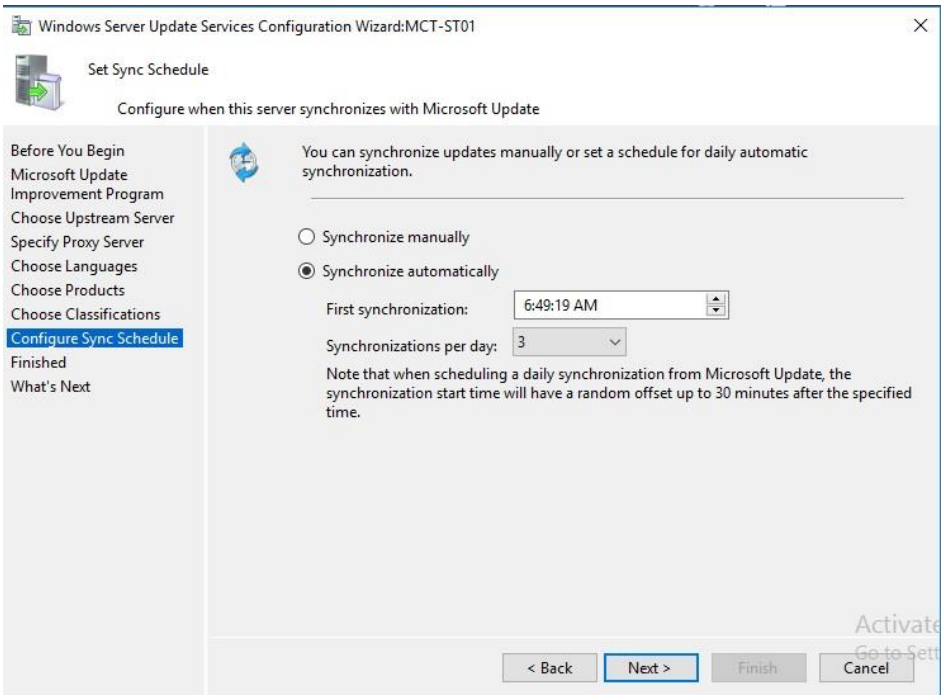
Select your products

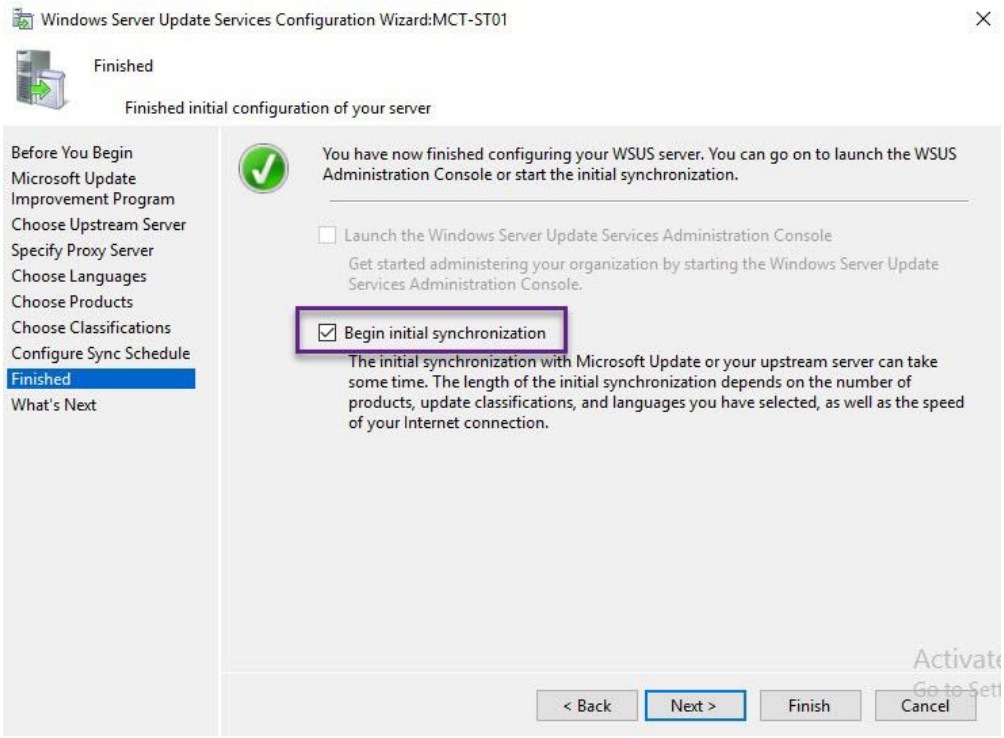


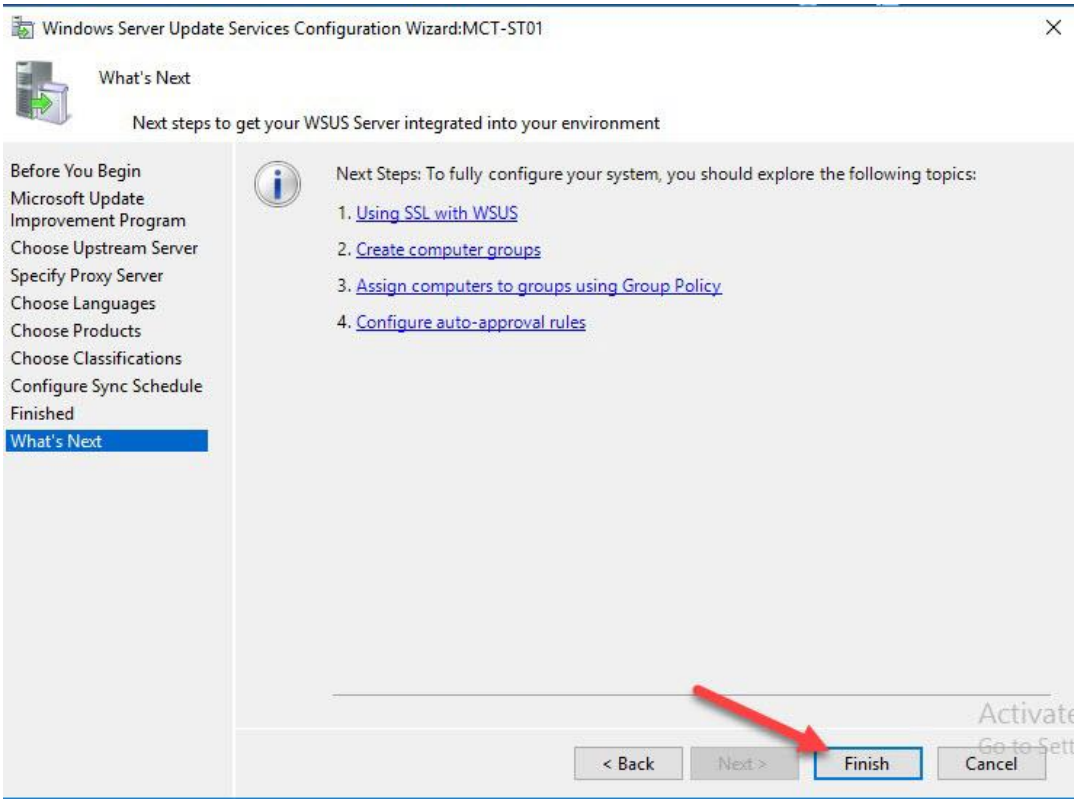
Select update category



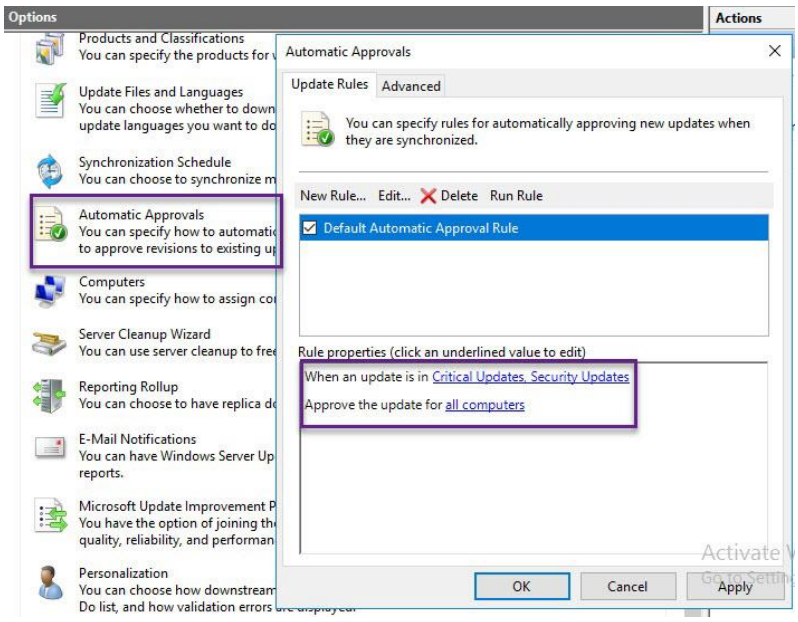
Choose a sync time with Microsoft update servers and initiate the first synchronization.



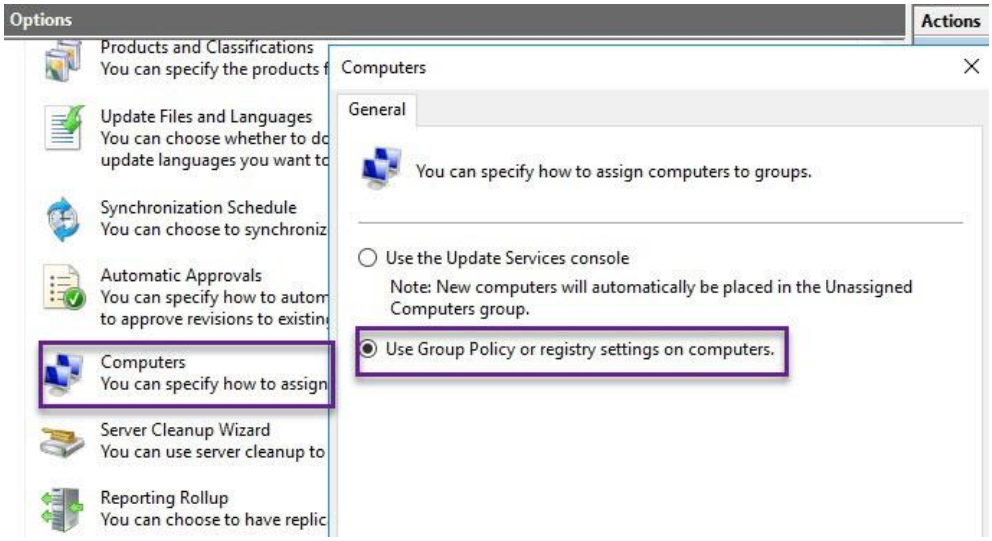


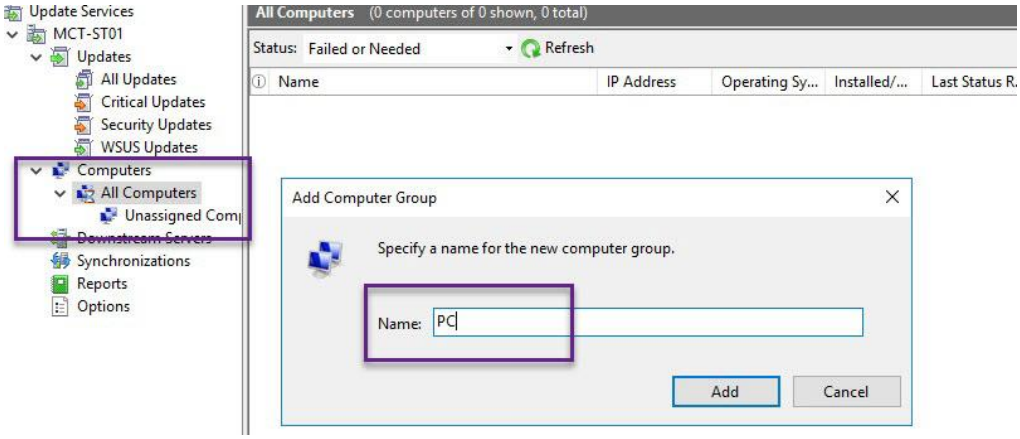


Enable automatic approval

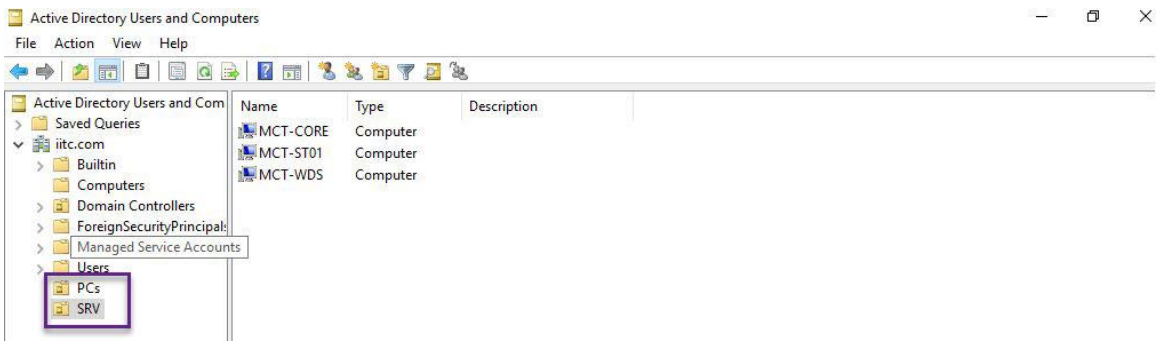


Set two groups one for PCs and another for Servers

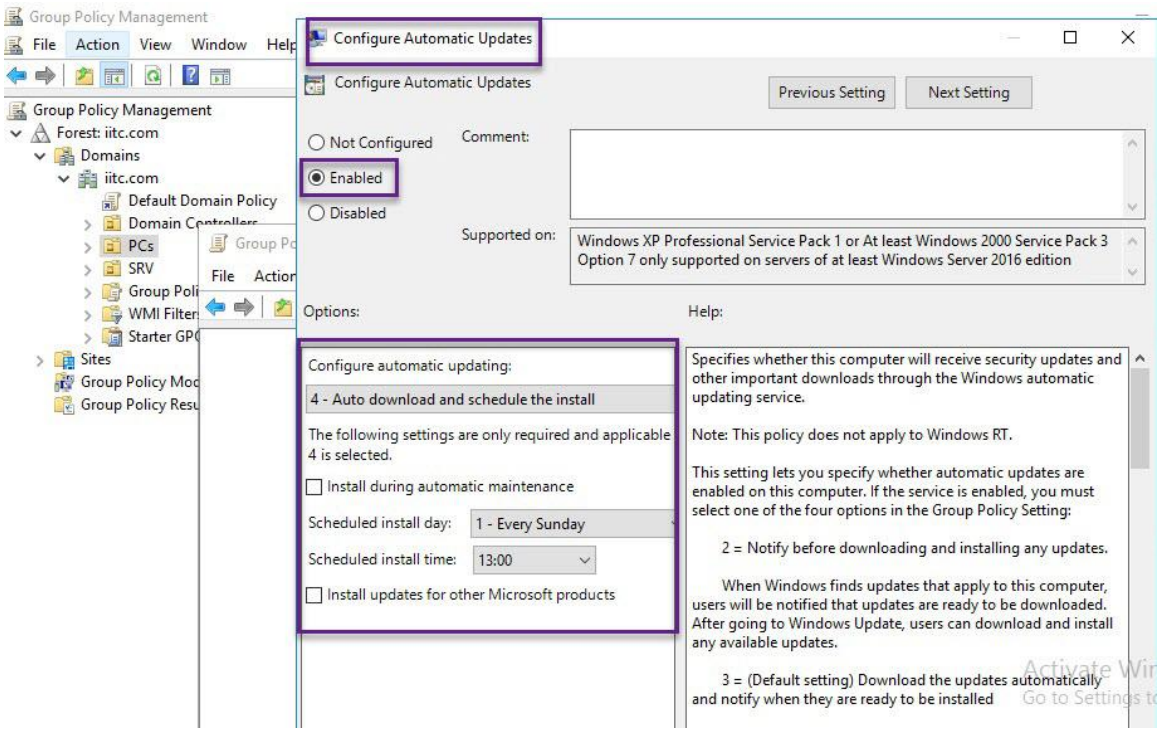


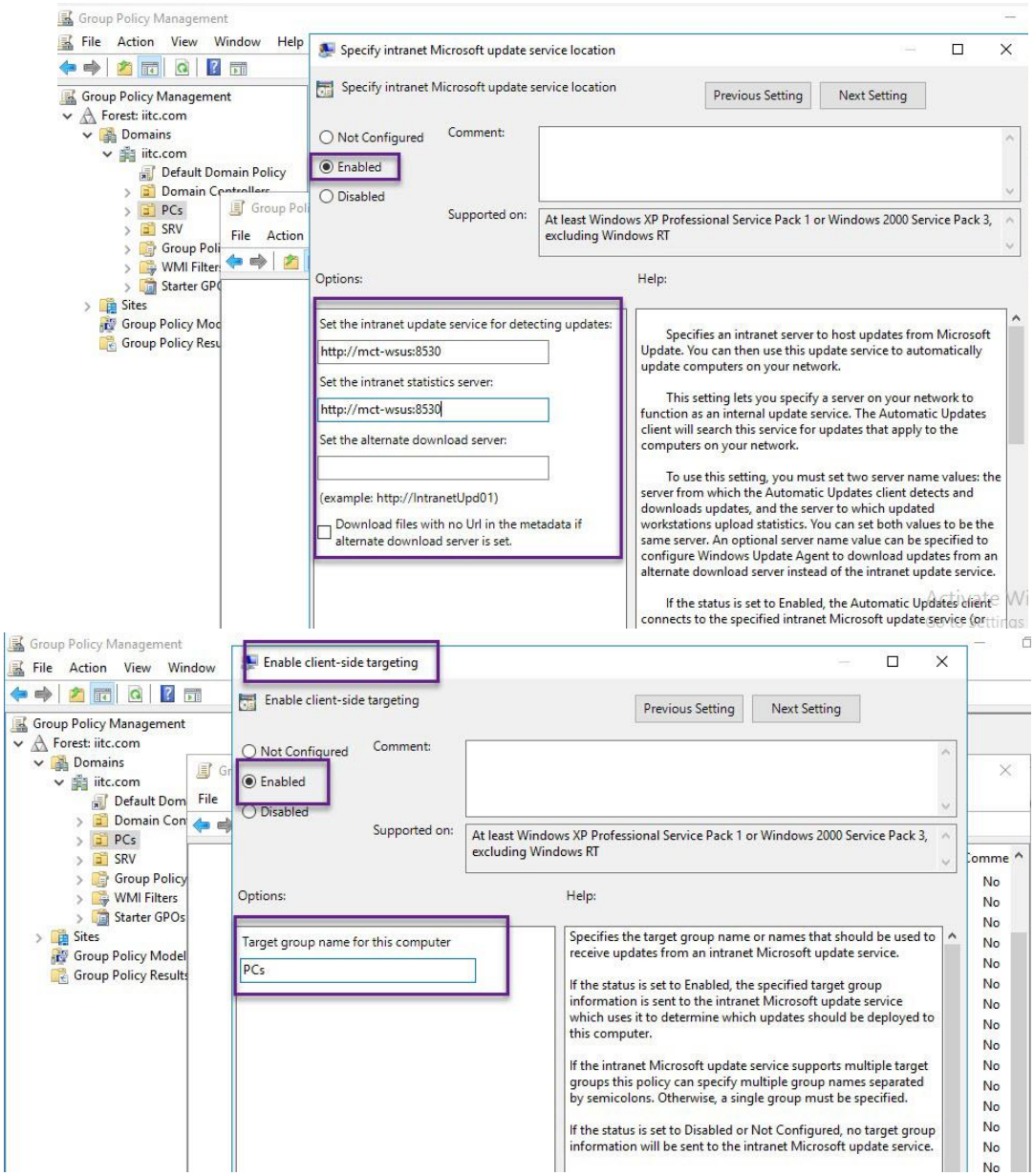


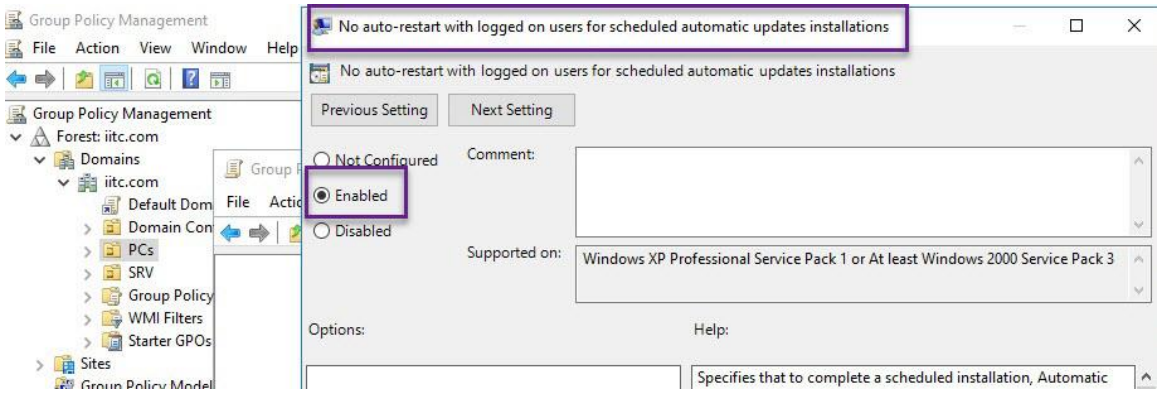
Create two organizational units (OUs) in Active Directory, one for personal computers and another for servers (SRV), to implement distinct policies for PCs and servers.

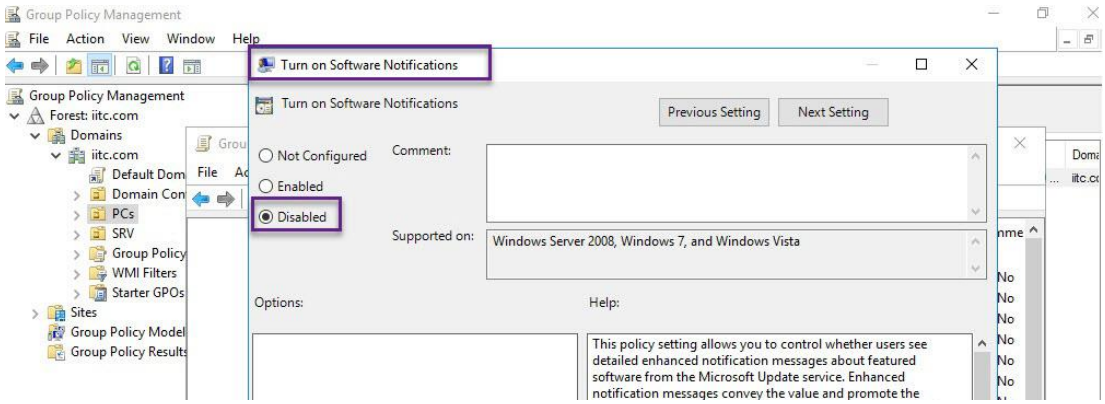


Create two group policy objects, one for personal computers and another for servers, with the specified update settings at the computer level.




Group Policy Management
File Action View Window Help
Specify intranet Microsoft update service location
Specify intranet Microsoft update service location
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Windows XP Professional Service Pack 1 or Windows 2000 Service Pack 3, excluding Windows RT
Options:
Help:
Set the intranet update service for detecting updates:
http://mct-wsus:8530
Set the intranet statistics server:
http://mct-wsus:8530
Set the alternate download server:
(example: http://IntranetUpd01)
Download files with no Url in the metadata if alternate download server is set.
Specifies an intranet server to host updates from Microsoft Update. You can then use this update service to automatically update computers on your network.
This setting lets you specify a server on your network to function as an internal update service. The Automatic Updates client will search this service for updates that apply to the computers on your network.
To use this setting, you must set two server name values: the server from which the Automatic Updates client detects and downloads updates, and the server to which updated workstations upload statistics. You can set both values to be the same server. An optional server name value can be specified to configure Windows Update Agent to download updates from an alternate download server instead of the intranet update service.
If the status is set to Enabled, the Automatic Updates client connects to the specified intranet Microsoft update service (or
Group Policy Management
Forest: iitc.com
Domains
iitc.com
Default Domain Policy
PCs
SRV
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Enable client-side targeting
Enable client-side targeting
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Windows XP Professional Service Pack 1 or Windows 2000 Service Pack 3, excluding Windows RT
Options:
Help:
Target group name for this computer
PCs
Specifies the target group name or names that should be used to receive updates from an intranet Microsoft update service.
If the status is set to Enabled, the specified target group information is sent to the intranet Microsoft update service which uses it to determine which updates should be deployed to this computer.
If the intranet Microsoft update service supports multiple target groups this policy can specify multiple group names separated by semicolons. Otherwise, a single group must be specified.
If the status is set to Disabled or Not Configured, no target group information will be sent to the intranet Microsoft update service.





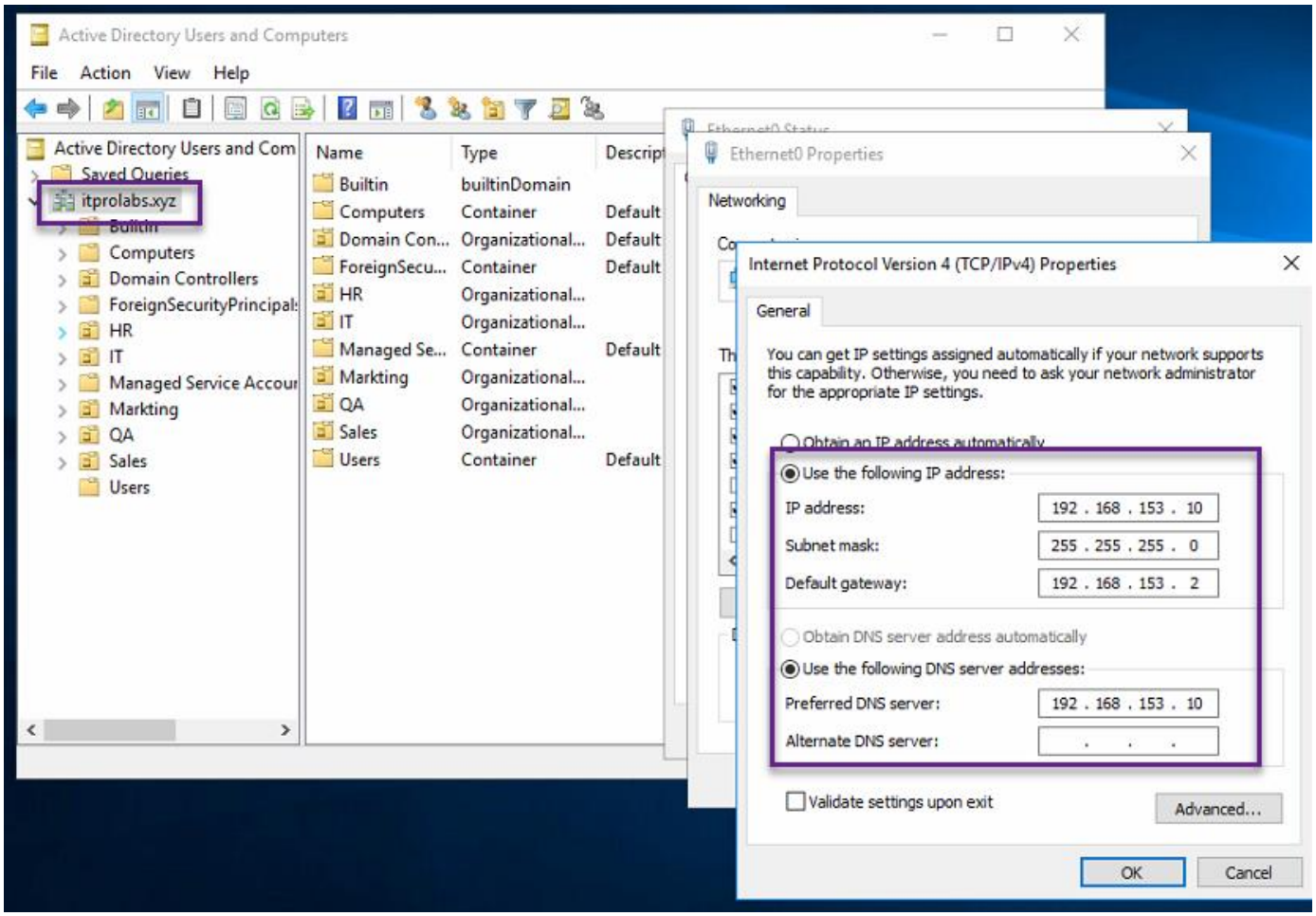
To apply the policy, either execute gpupdate /force or reboot the computers.

L2TP/IPsec VPN

A Virtual Private Network (VPN) creates a protected network channel that enables you to link to your private network from different internet locations, providing access to internal resources as per the access rights granted to you.

Existing Active directory environment

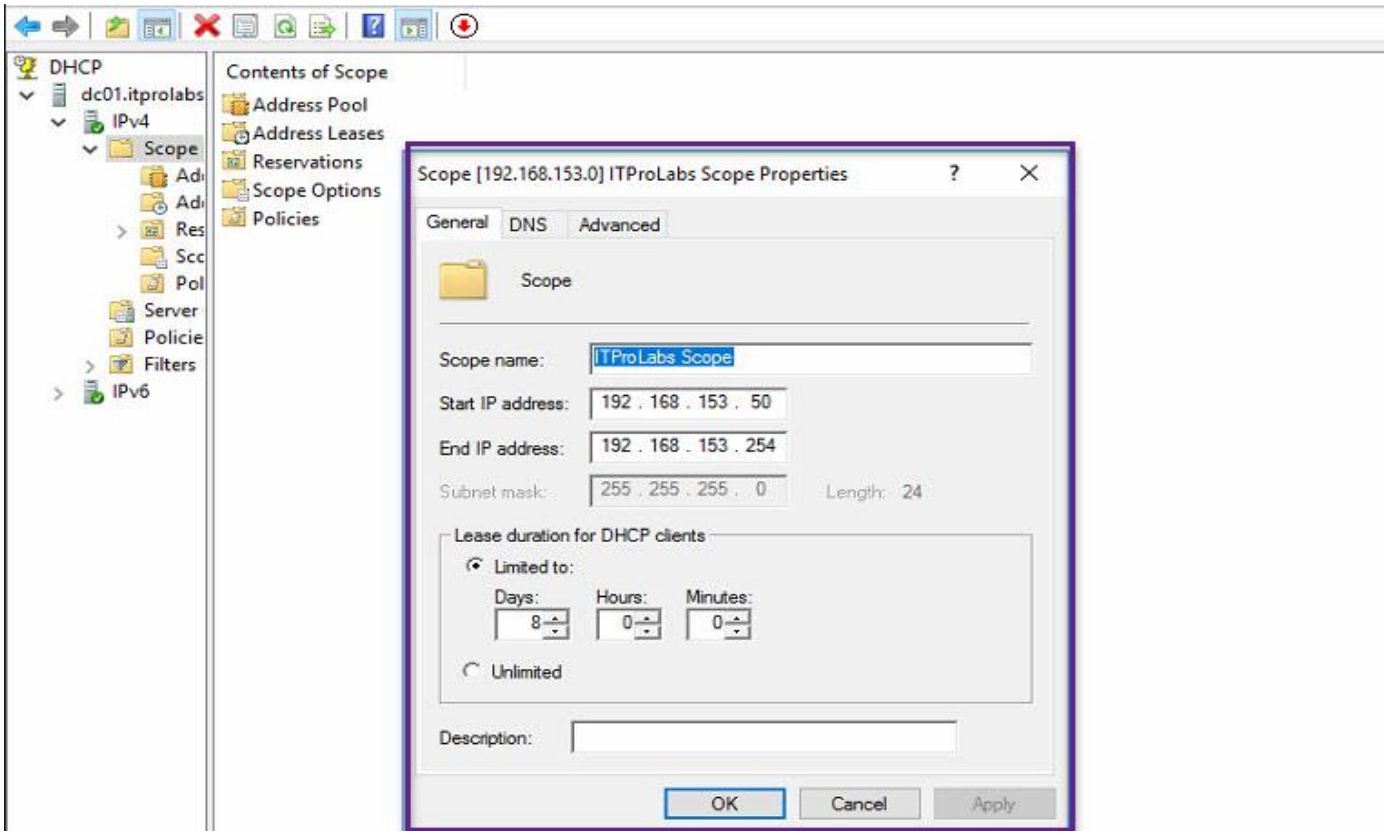
OS: Windows server 2016
Domain Name: ITPROLABS.XYZ
Domain IP: 192.168.153.10/24
IP Scheme: 192.168.153.0/24



Existing DHCP Server Configuration:

VPN clients will reach out to the DHCP server to get our internal TCP/IP settings in order to access internal resources, as outlined in the following DHCP server configuration:

Server IP: 192.168.153.10/24
Scope range: 192.168.153.50 – 192.168.153.254
DG: 192.168.153.2
DNS: 192.168.153.10

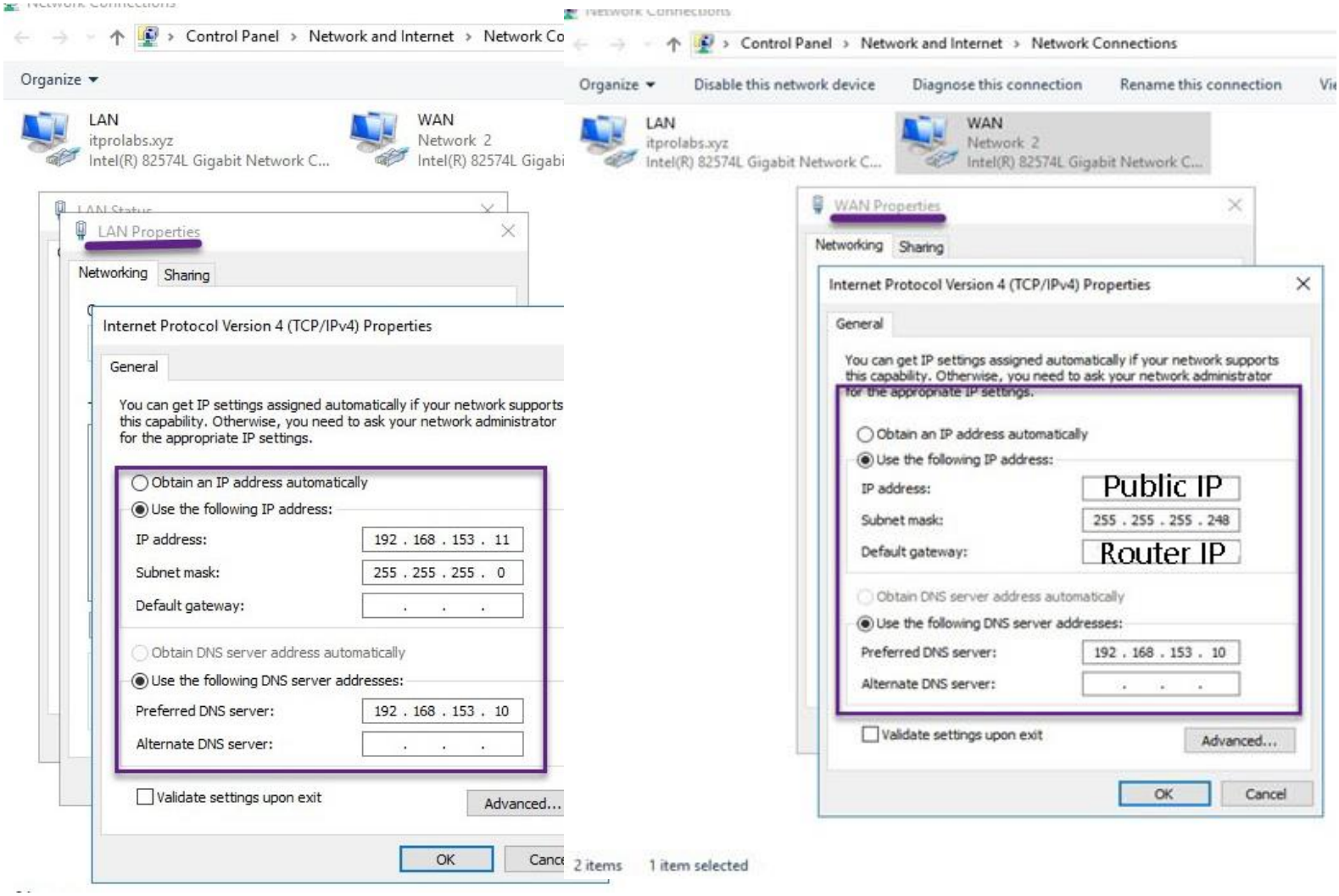


VPN Server Setup and Configurations

Server Name: **VPN**
LAN IP: 192.168.153.11/24
WAN IP: public IP address

Network configuration:

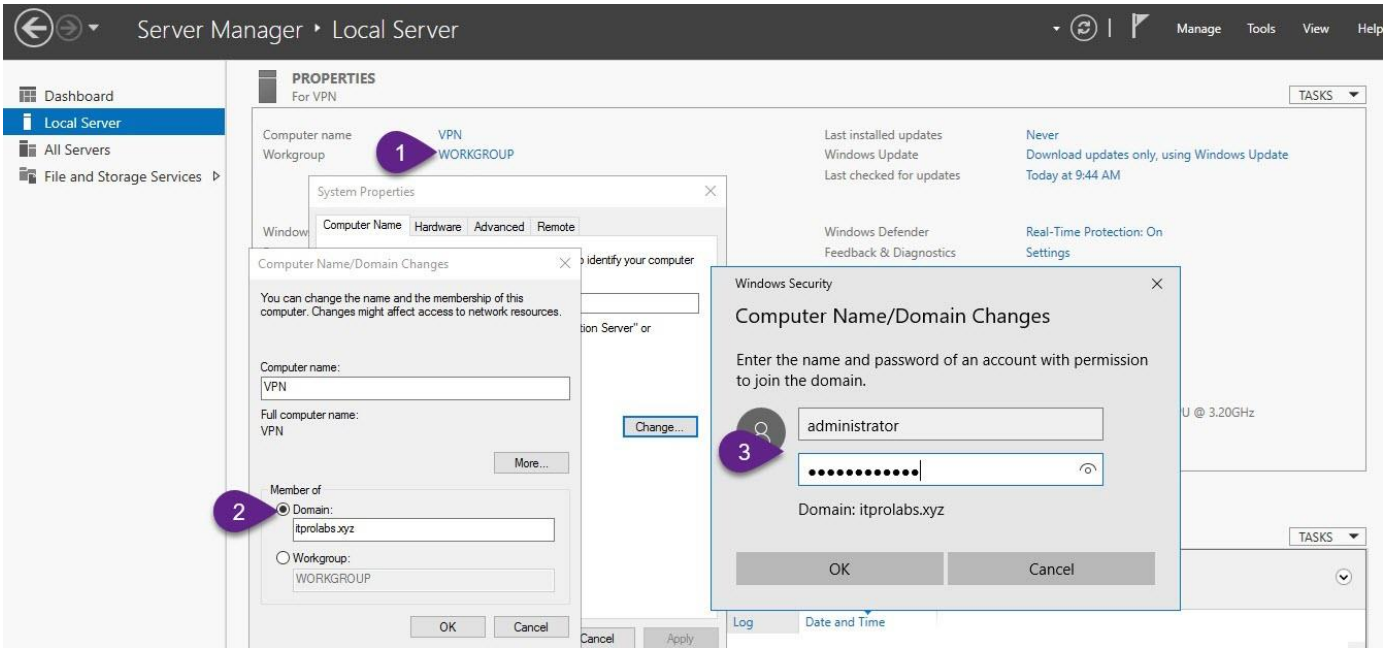
Our setup includes two network interfaces: one is dedicated to LAN connections within our domain scope, while the other handles WAN operations, specifically accepting VPN client connection requests from the internet.



VPN Configuration Steps:

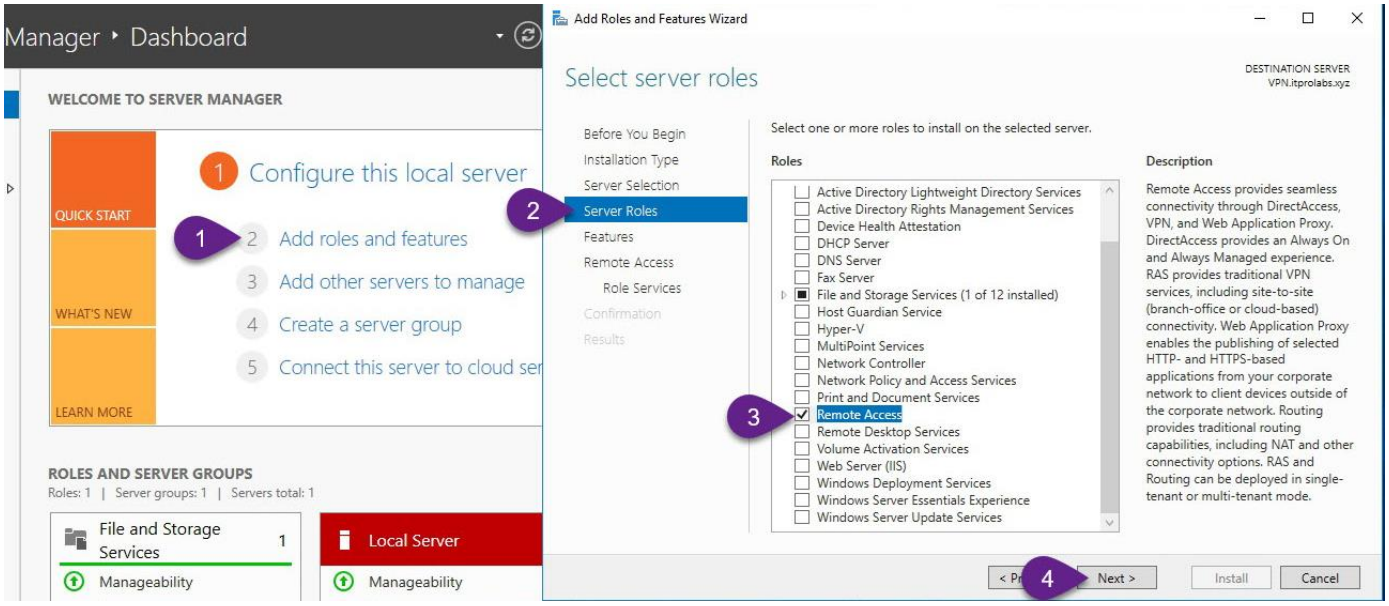
Step 1: Join VPN Server to ITPROLABS.XYZ domain

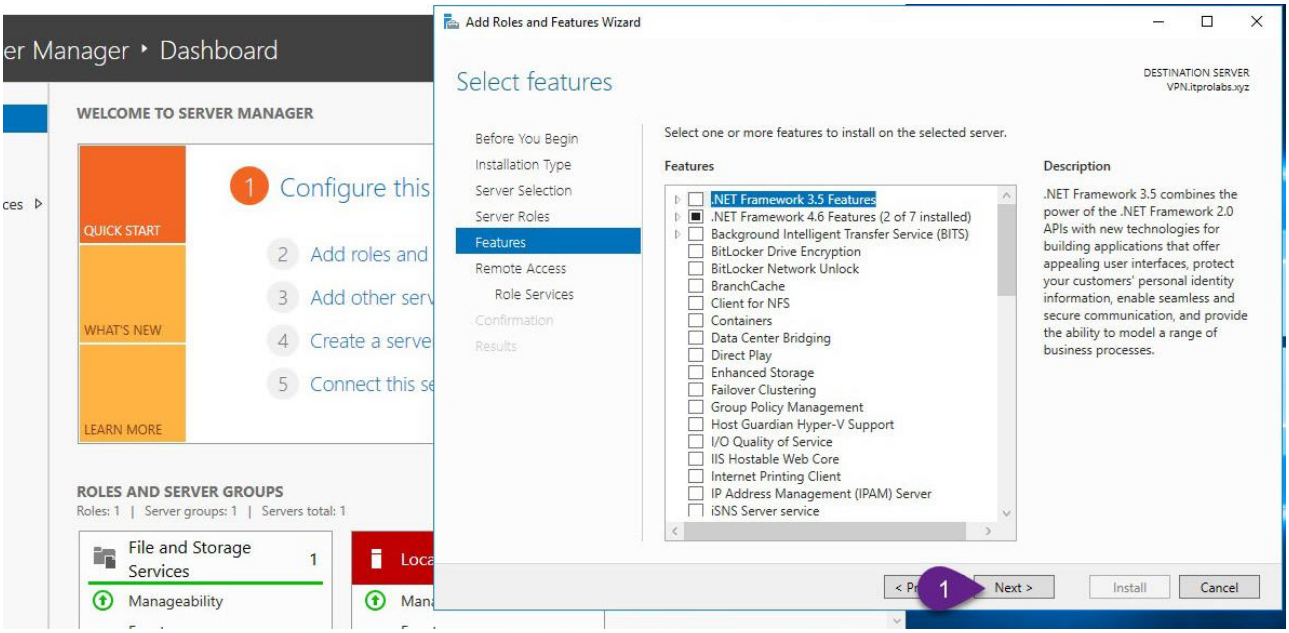
Initially, connect to our VPN server linked to the ITPROLABS.XYZ domain in order to authenticate VPN client connections using active directory.

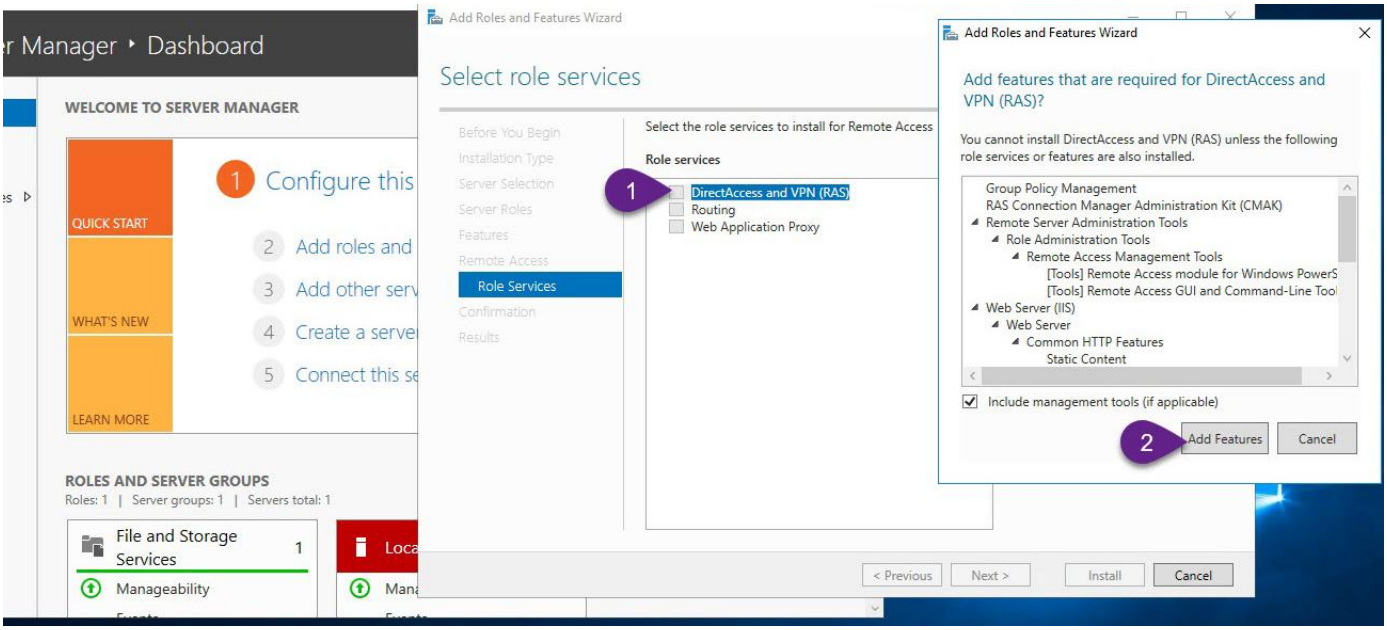


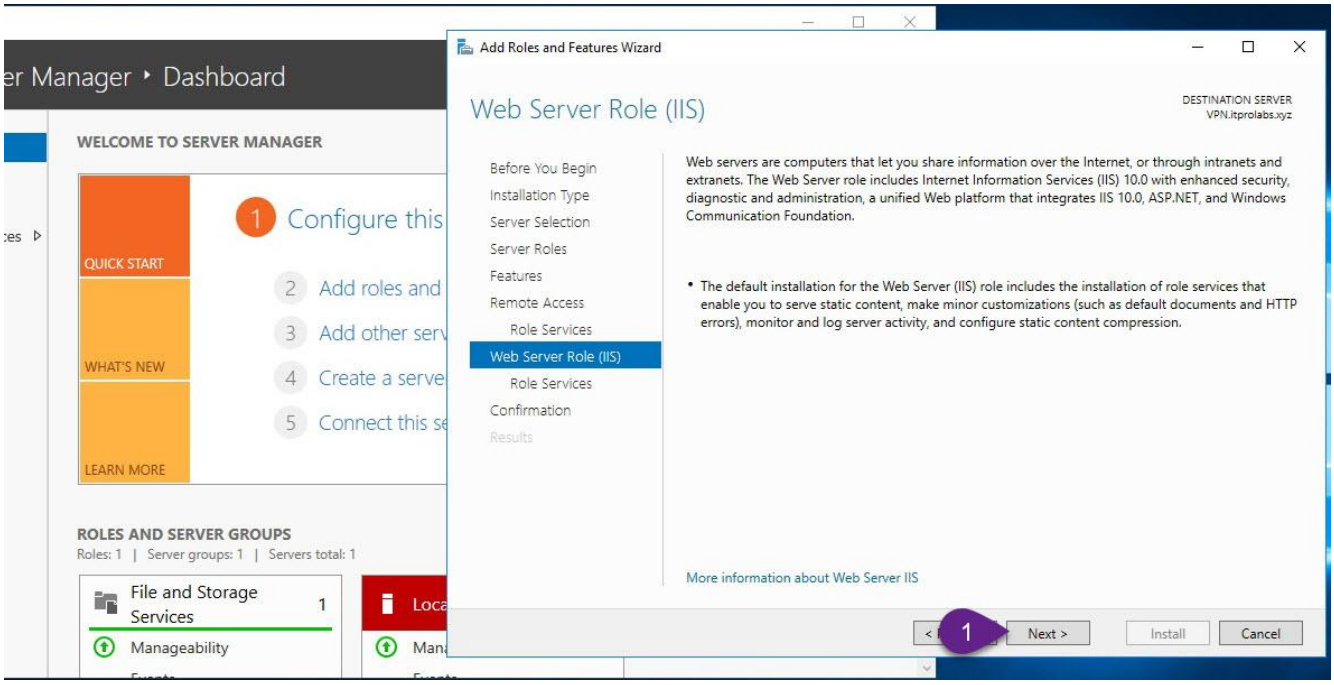
Step 2: Add Remote Access role

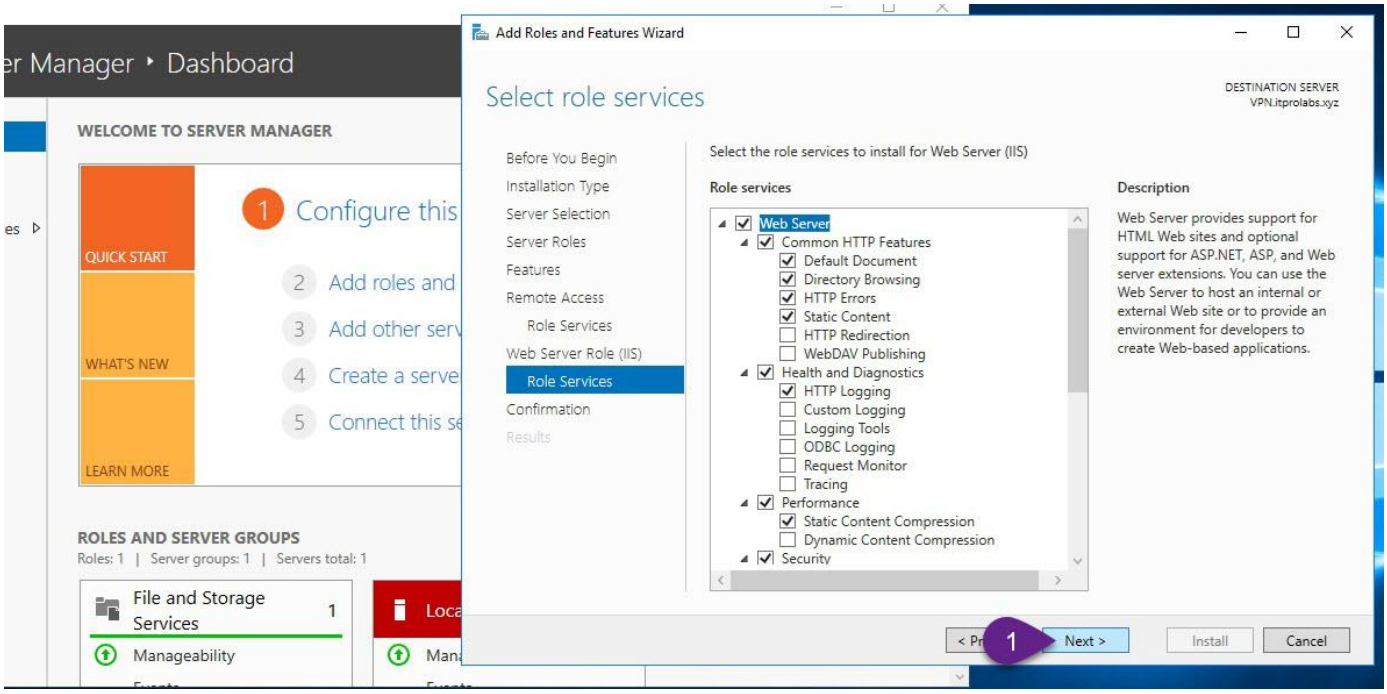
On the VPN server, use the Server Manager to install the remote access role as depicted in the following illustrations.

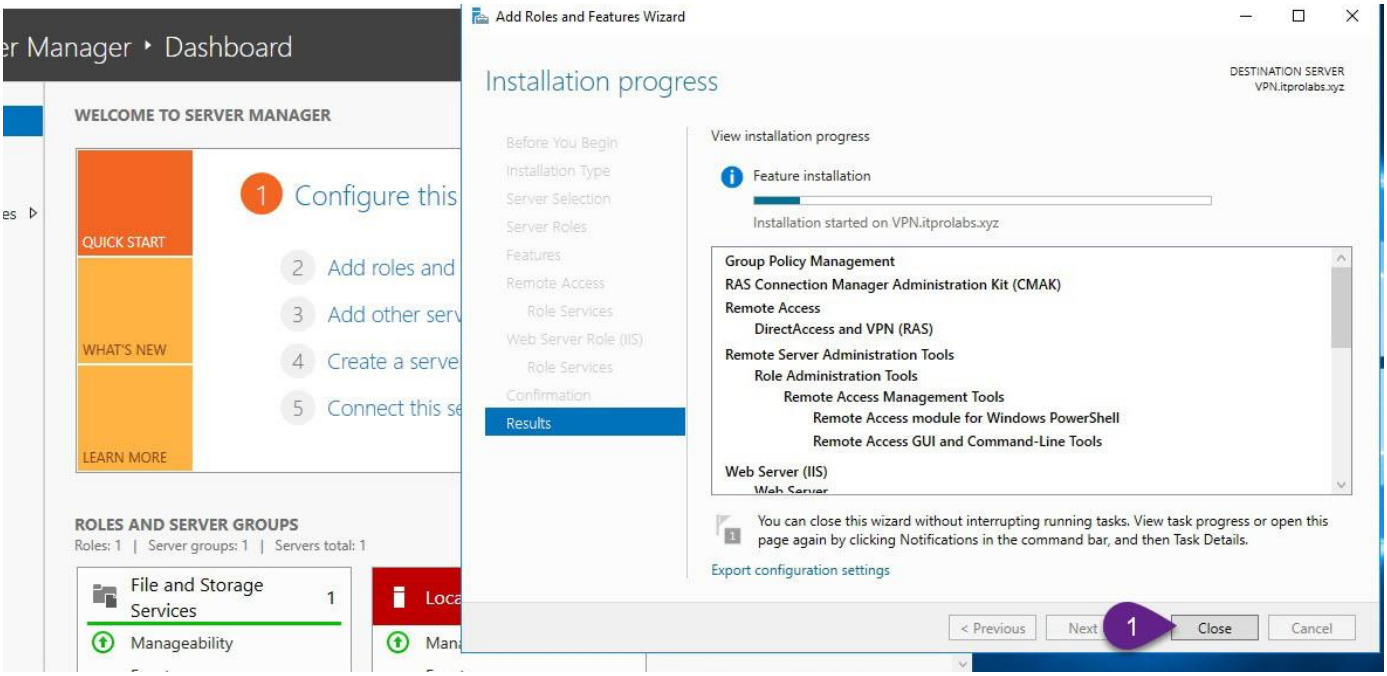


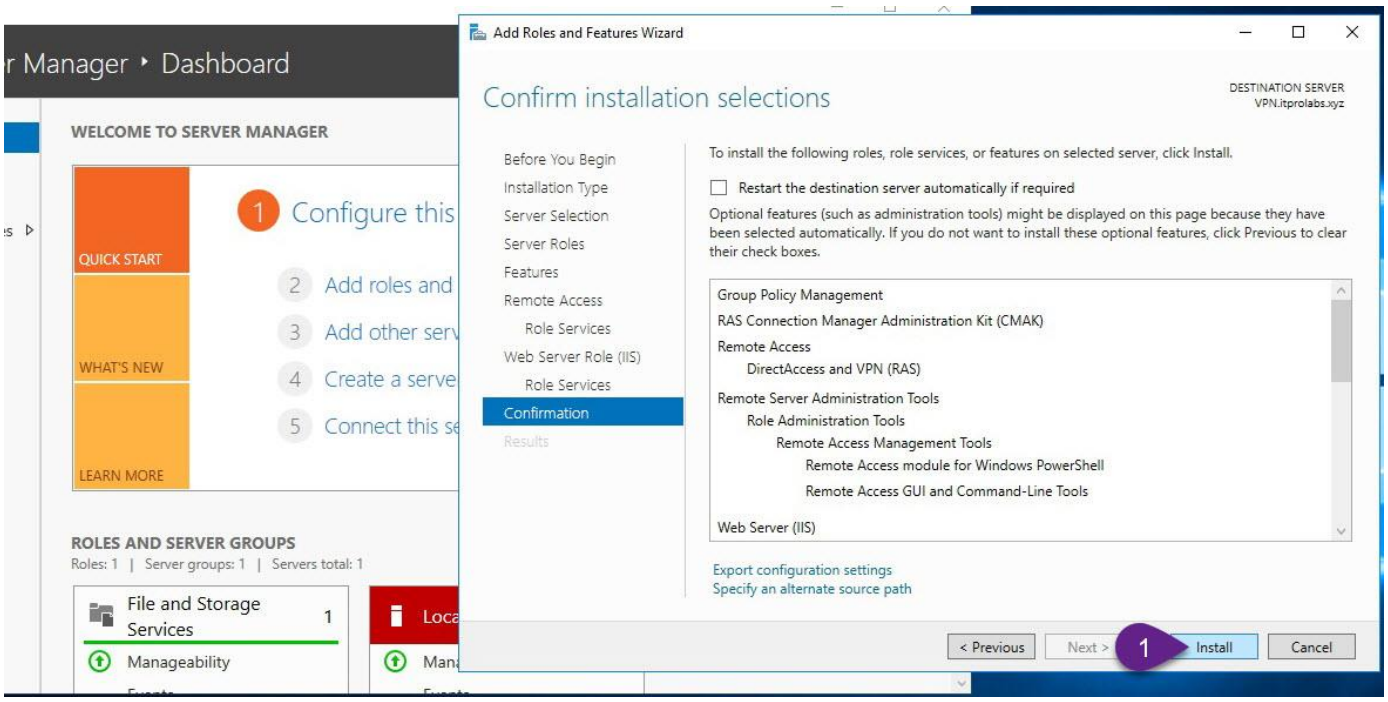

er Manager ‣ Dashboard
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this
2 Add roles and
3 Add other serv
4 Create a serve
5 Connect this se
ROLES AND SERVER GROUPS
Roles: 1 | Server groups: 1 | Servers total: 1
File and Storage Services 1
Manageability
Add Roles and Features Wizard
Select features
DESTINATION SERVER
VPN.itprolabs.xyz
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Remote Access
Role Services
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
Group Policy Management
Host Guardian Hyper-V Support
I/O Quality of Service
IIS Hostable Web Core
Internet Printing Client
IP Address Management (IPAM) Server
iSNS Server service
Description
.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.
1
Next >
Install
Cancel


r Manager ‣ Dashboard
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this
2 Add roles and
3 Add other serv
4 Create a serve
5 Connect this se
ROLES AND SERVER GROUPS
Roles: 1 | Server groups: 1 | Servers total: 1
File and Storage Services 1
Manageability
Add Roles and Features Wizard
Select role services
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Remote Access
Role Services
Confirmation
Results
Select the role services to install for Remote Access
Role services
1
DirectAccess and VPN (RAS)
Routing
Web Application Proxy
< Previous
Next >
Install
Cancel
Add Roles and Features Wizard
Add features that are required for DirectAccess and VPN (RAS)?
You cannot install DirectAccess and VPN (RAS) unless the following role services or features are also installed.
Group Policy Management
RAS Connection Manager Administration Kit (CMAK)
Remote Server Administration Tools
Role Administration Tools
Remote Access Management Tools
[Tools] Remote Access module for Windows PowerS
[Tools] Remote Access GUI and Command-Line Too
Web Server (IIS)
Web Server
Common HTTP Features
Static Content
Include management tools (if applicable)
2
Add Features
Cancel


Server Manager • Dashboard
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this
2 Add roles and
3 Add other serv
4 Create a serve
5 Connect this se
ROLES AND SERVER GROUPS
Roles: 1 | Server groups: 1 | Servers total: 1
File and Storage Services 1
Manageability
Add Roles and Features Wizard
Web Server Role (IIS)
DESTINATION SERVER
VPN.itprolabs.xyz
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Remote Access
Role Services
Web Server Role (IIS)
Role Services
Confirmation
Results
Web servers are computers that let you share information over the Internet, or through intranets and extranets. The Web Server role includes Internet Information Services (IIS) 10.0 with enhanced security, diagnostic and administration, a unified Web platform that integrates IIS 10.0, ASP.NET, and Windows Communication Foundation.
• The default installation for the Web Server (IIS) role includes the installation of role services that enable you to serve static content, make minor customizations (such as default documents and HTTP errors), monitor and log server activity, and configure static content compression.
More information about Web Server IIS
1
Next >
Install
Cancel

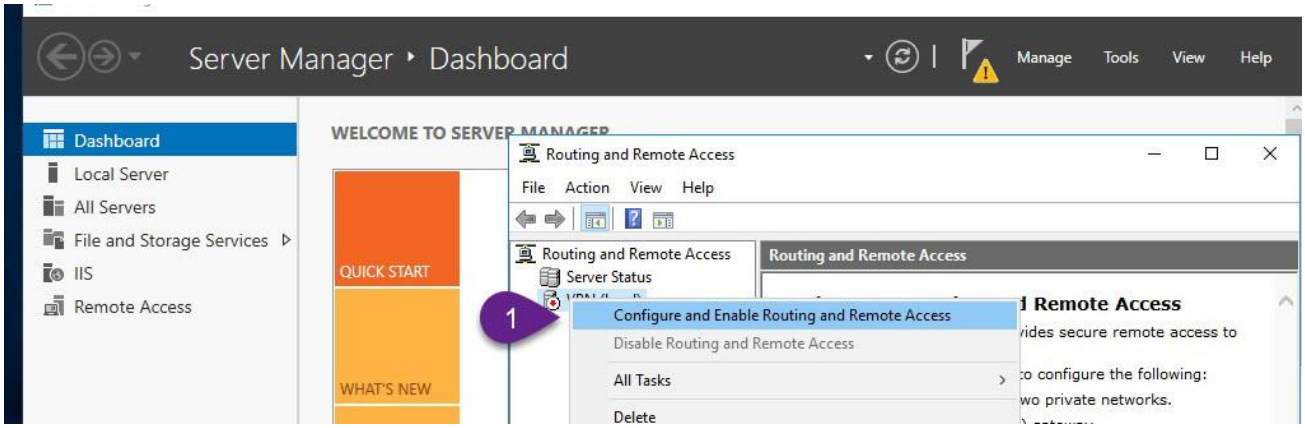

Server Manager • Dashboard
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this
2 Add roles and
3 Add other serv
4 Create a serve
5 Connect this se
ROLES AND SERVER GROUPS
Roles: 1 | Server groups: 1 | Servers total: 1
File and Storage Services 1
Manageability
Add Roles and Features Wizard
Select role services
DESTINATION SERVER
VPN.itprolabs.xyz
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Remote Access
Role Services
Web Server Role (IIS)
Role Services
Confirmation
Results
Select the role services to install for Web Server (IIS)
Role services
Web Server
Common HTTP Features
Default Document
Directory Browsing
HTTP Errors
Static Content
HTTP Redirection
WebDAV Publishing
Health and Diagnostics
HTTP Logging
Custom Logging
Logging Tools
ODBC Logging
Request Monitor
Tracing
Performance
Static Content Compression
Dynamic Content Compression
Security
Description
Web Server provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web-based applications.
1
Next >
Install
Cancel

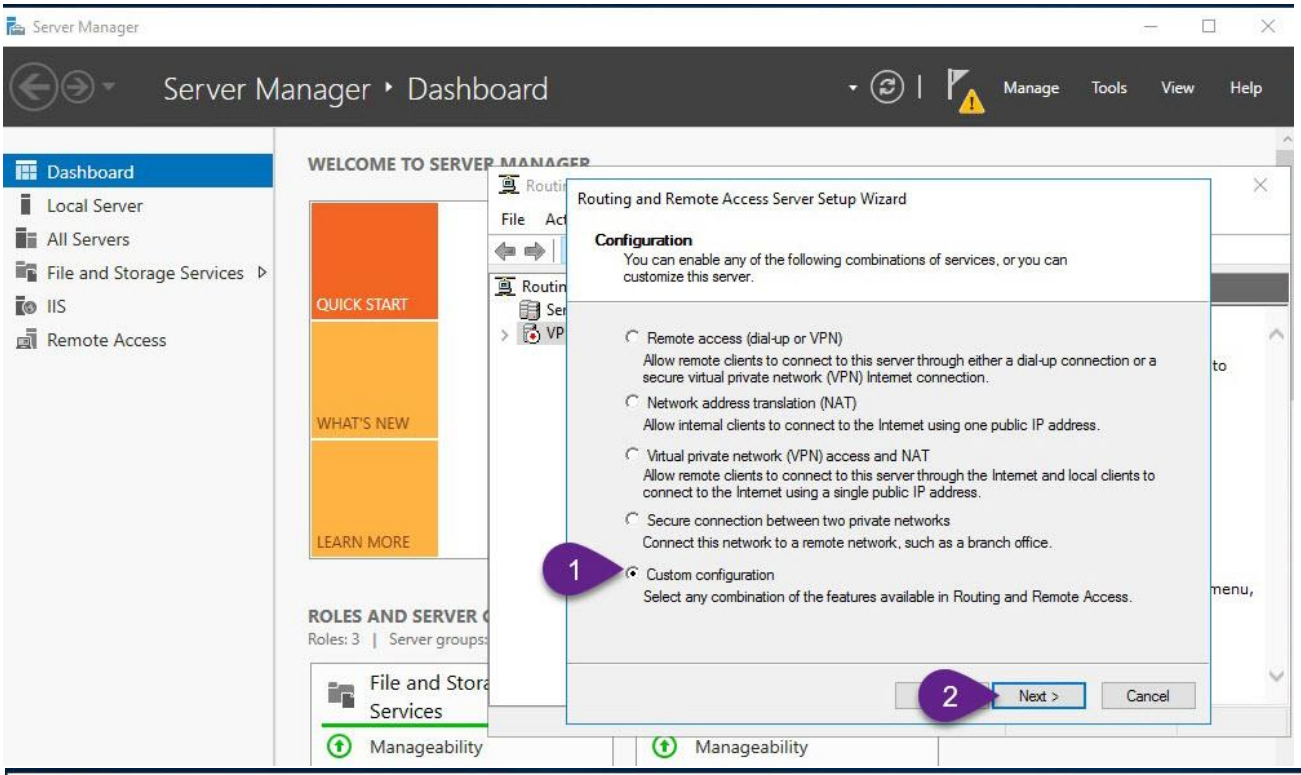

Manager ▸ Dashboard
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this
2 Add roles and
3 Add other serv
4 Create a serve
5 Connect this se
ROLES AND SERVER GROUPS
Roles: 1 | Server groups: 1 | Servers total: 1
File and Storage Services 1
Manageability
Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
VPN.itprolabs.xyz
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Remote Access
Role Services
Web Server Role (IIS)
Role Services
Confirmation
Results
View installation progress
Feature installation
Installation started on VPN.itprolabs.xyz
Group Policy Management
RAS Connection Manager Administration Kit (CMAK)
Remote Access
DirectAccess and VPN (RAS)
Remote Server Administration Tools
Role Administration Tools
Remote Access Management Tools
Remote Access module for Windows PowerShell
Remote Access GUI and Command-Line Tools
Web Server (IIS)
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
1
Close
Cancel

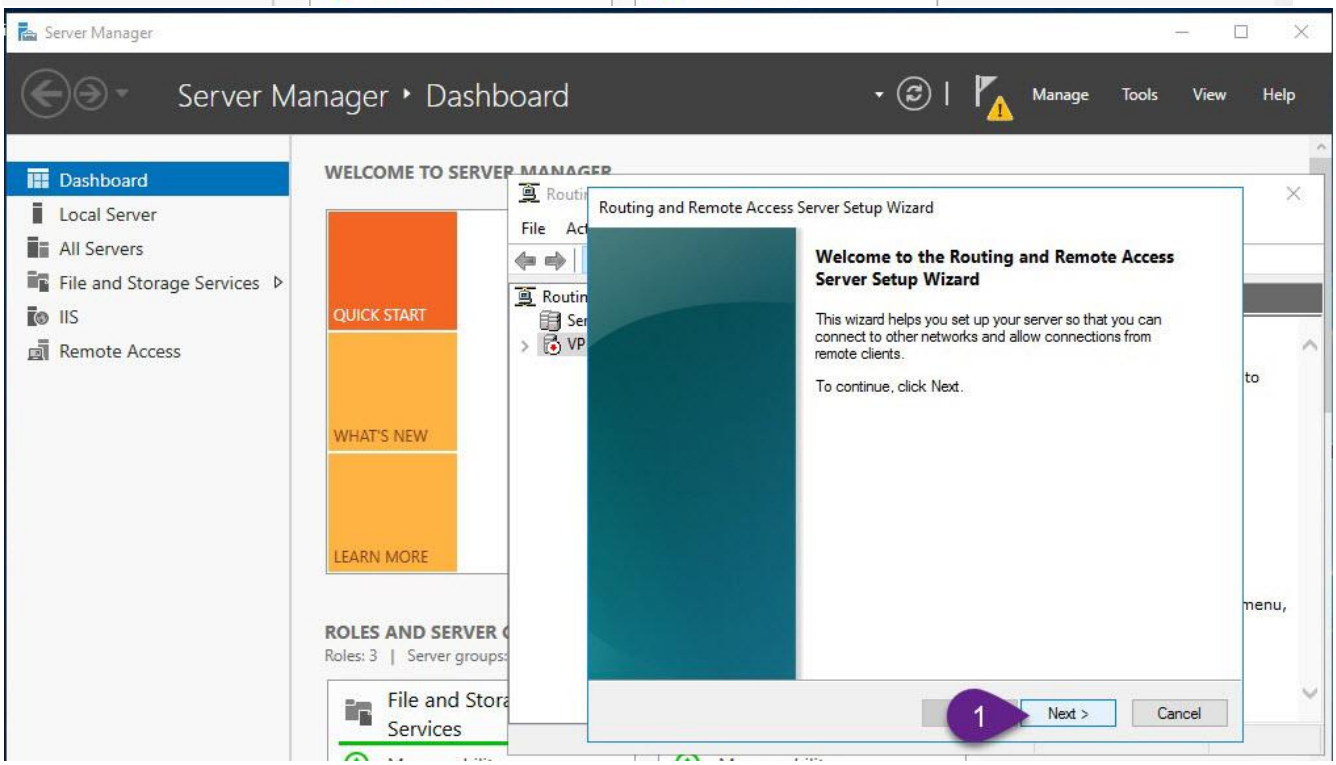

Manager ▸ Dashboard
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this
2 Add roles and
3 Add other serv
4 Create a serve
5 Connect this se
ROLES AND SERVER GROUPS
Roles: 1 | Server groups: 1 | Servers total: 1
File and Storage Services 1
Manageability
Add Roles and Features Wizard
Confirm installation selections
DESTINATION SERVER
VPN.itprolabs.xyz
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Remote Access
Role Services
Web Server Role (IIS)
Role Services
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.
Group Policy Management
RAS Connection Manager Administration Kit (CMAK)
Remote Access
DirectAccess and VPN (RAS)
Remote Server Administration Tools
Role Administration Tools
Remote Access Management Tools
Remote Access module for Windows PowerShell
Remote Access GUI and Command-Line Tools
Web Server (IIS)
Export configuration settings
Specify an alternate source path
< Previous
Next >
1
Install
Cancel

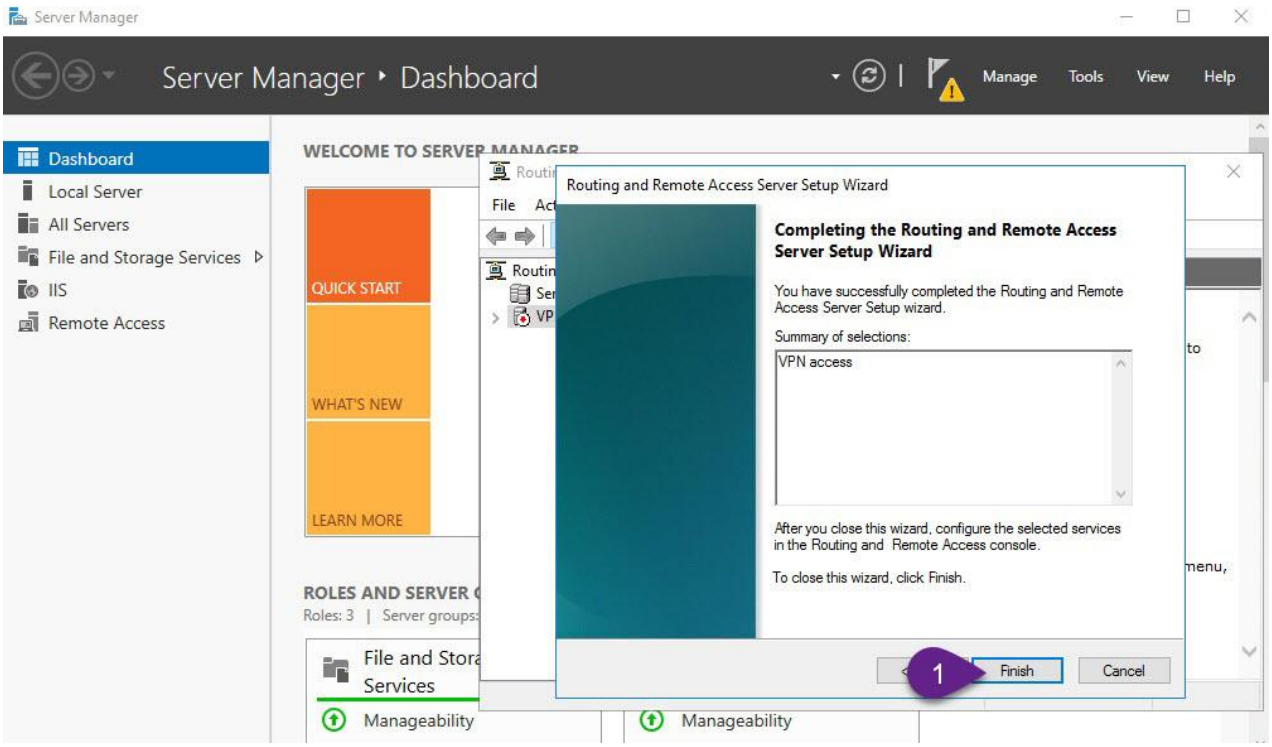
Step 3: Enable and configure routing and remote access (Enable VPN Service)

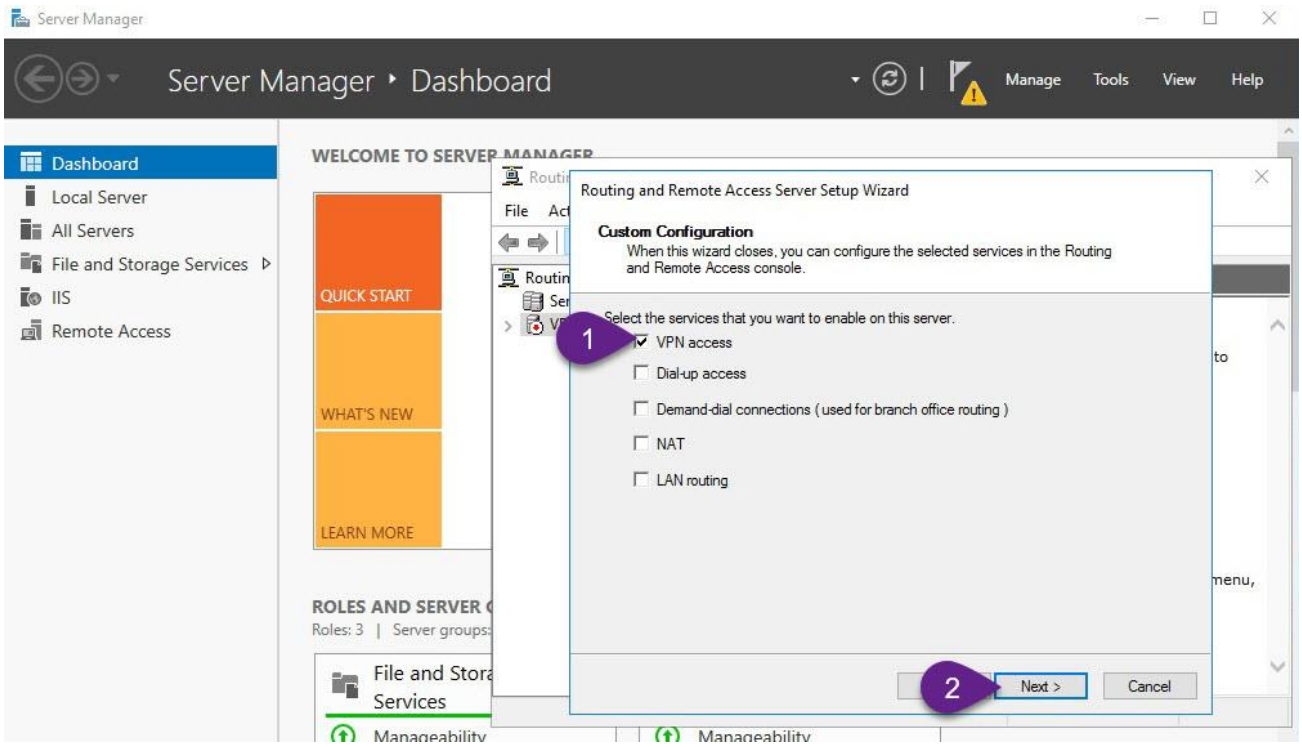
1. On **VPN**, from Server Manager, open Routing and Remote Access.
2. Right-click **VPN** (local), and then click Configure and Enable Routing and Remote Access and follow the instructions as explained in the figures below

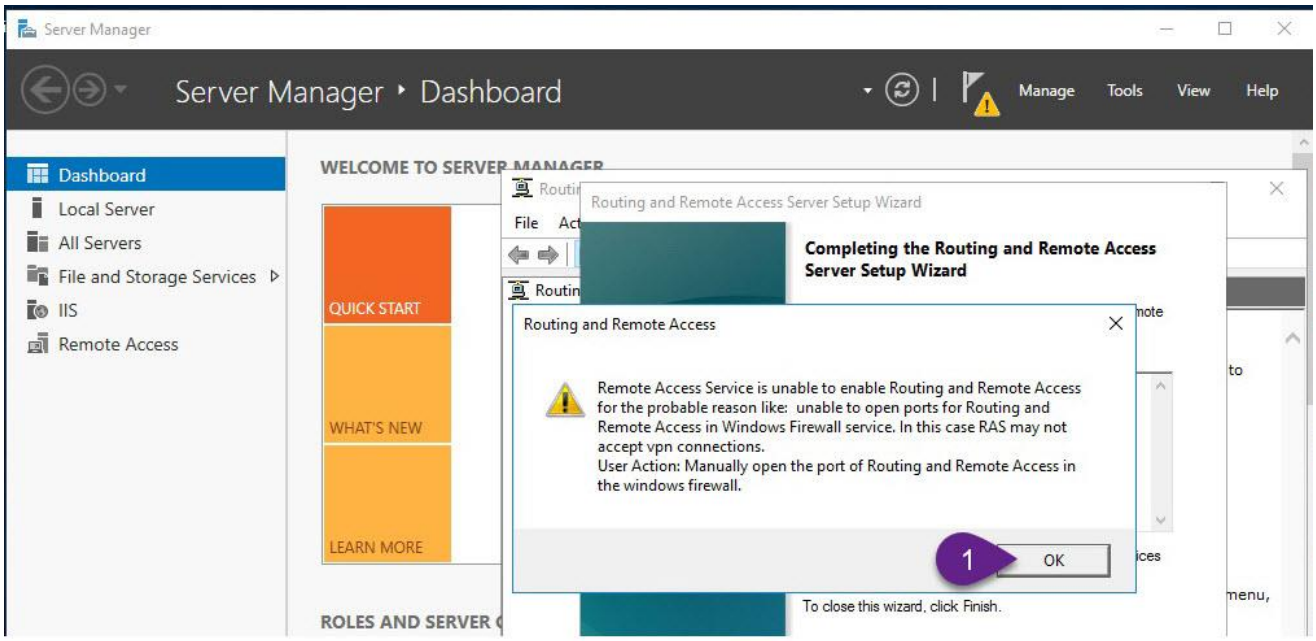


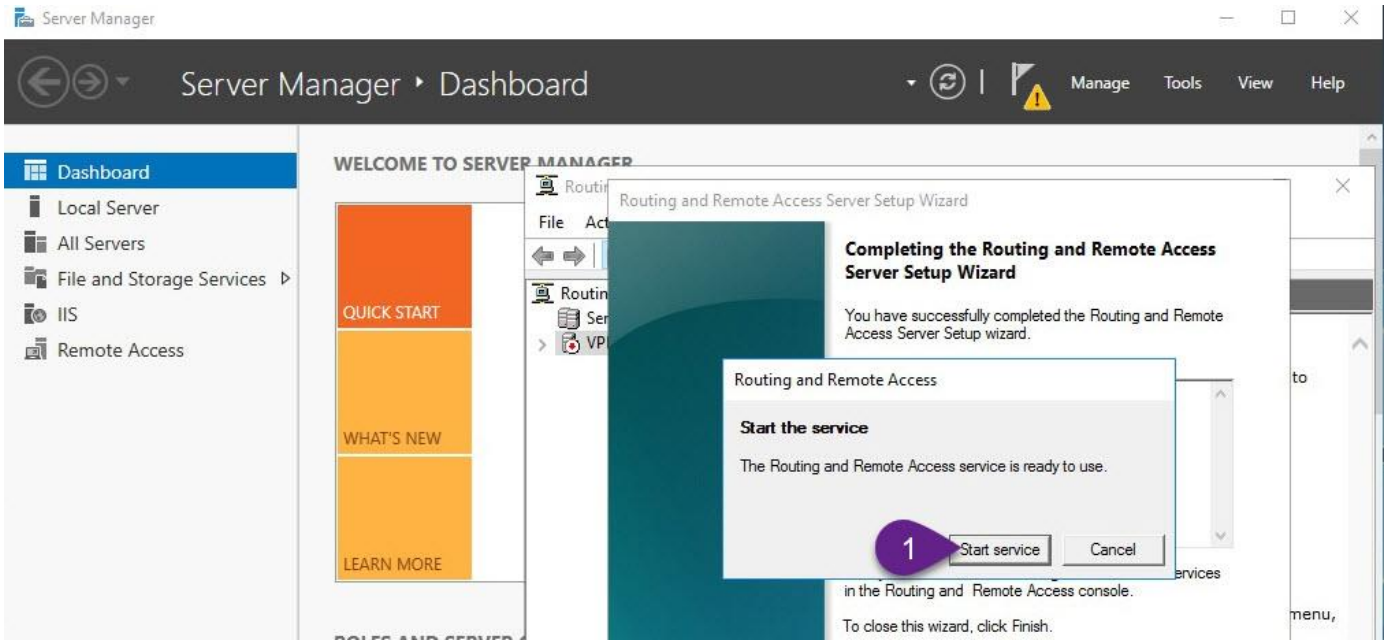

Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
IIS
Remote Access
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
ROLES AND SERVER
Roles: 3 | Server groups:
File and Stora
Services
Manageability
Manageability
Routing and Remote Access Server Setup Wizard
Configuration
You can enable any of the following combinations of services, or you can customize this server.
Remote access (dial-up or VPN)
Allow remote clients to connect to this server through either a dial-up connection or a secure virtual private network (VPN) Internet connection.
Network address translation (NAT)
Allow internal clients to connect to the Internet using one public IP address.
Virtual private network (VPN) access and NAT
Allow remote clients to connect to this server through the Internet and local clients to connect to the Internet using a single public IP address.
Secure connection between two private networks
Connect this network to a remote network, such as a branch office.
Custom configuration
Select any combination of the features available in Routing and Remote Access.
1
2
Next >
Cancel


Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
IIS
Remote Access
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
ROLES AND SERVER
Roles: 3 | Server groups:
File and Stora
Services
Routing and Remote Access Server Setup Wizard
Welcome to the Routing and Remote Access Server Setup Wizard
This wizard helps you set up your server so that you can connect to other networks and allow connections from remote clients.
To continue, click Next.
1
Next >
Cancel


Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
IIS
Remote Access
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
ROLES AND SERVER
Roles: 3 | Server groups:
File and Stora
Services
Manageability
Routing and Remote Access Server Setup Wizard
Completing the Routing and Remote Access Server Setup Wizard
You have successfully completed the Routing and Remote Access Server Setup wizard.
Summary of selections:
VPN access
After you close this wizard, configure the selected services in the Routing and Remote Access console.
To close this wizard, click Finish.
1
Finish
Cancel

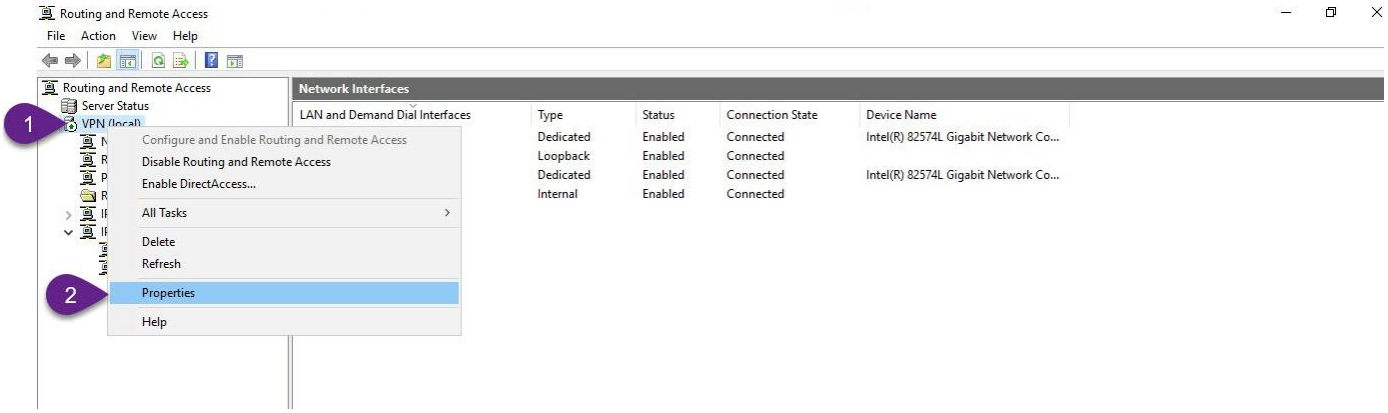

Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
IIS
Remote Access
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
ROLES AND SERVER
Roles: 3 | Server groups:
File and Stora
Services
Manageability
Routing and Remote Access Server Setup Wizard
Custom Configuration
When this wizard closes, you can configure the selected services in the Routing and Remote Access console.
Select the services that you want to enable on this server.
1
VPN access
Dial-up access
Demand-dial connections (used for branch office routing)
NAT
LAN routing
2
Next >
Cancel

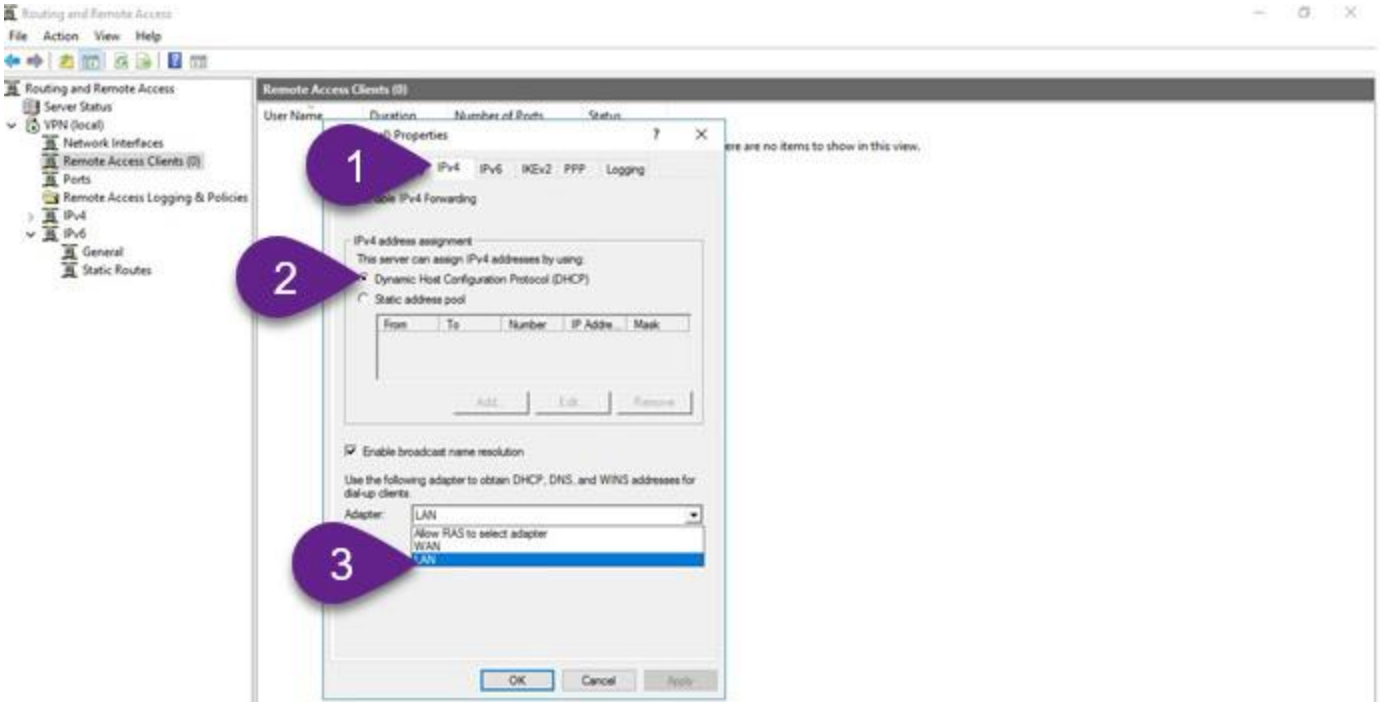

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
IIS
Remote Access
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
ROLES AND SERVER
Routing and Remote Access Server Setup Wizard
Completing the Routing and Remote Access Server Setup Wizard
Routing and Remote Access
Remote Access Service is unable to enable Routing and Remote Access for the probable reason like: unable to open ports for Routing and Remote Access in Windows Firewall service. In this case RAS may not accept vpn connections.
User Action: Manually open the port of Routing and Remote Access in the windows firewall.
1
OK
To close this wizard, click Finish.


Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
IIS
Remote Access
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
Routing and Remote Access Server Setup Wizard
Completing the Routing and Remote Access Server Setup Wizard
You have successfully completed the Routing and Remote Access Server Setup wizard.
Routing and Remote Access
Start the service
The Routing and Remote Access service is ready to use.
1
Start service
Cancel
in the Routing and Remote Access console.
To close this wizard, click Finish.

Step 4: Allow VPN clients to obtain TCP/IP configuration from DHCP and use internal DNS

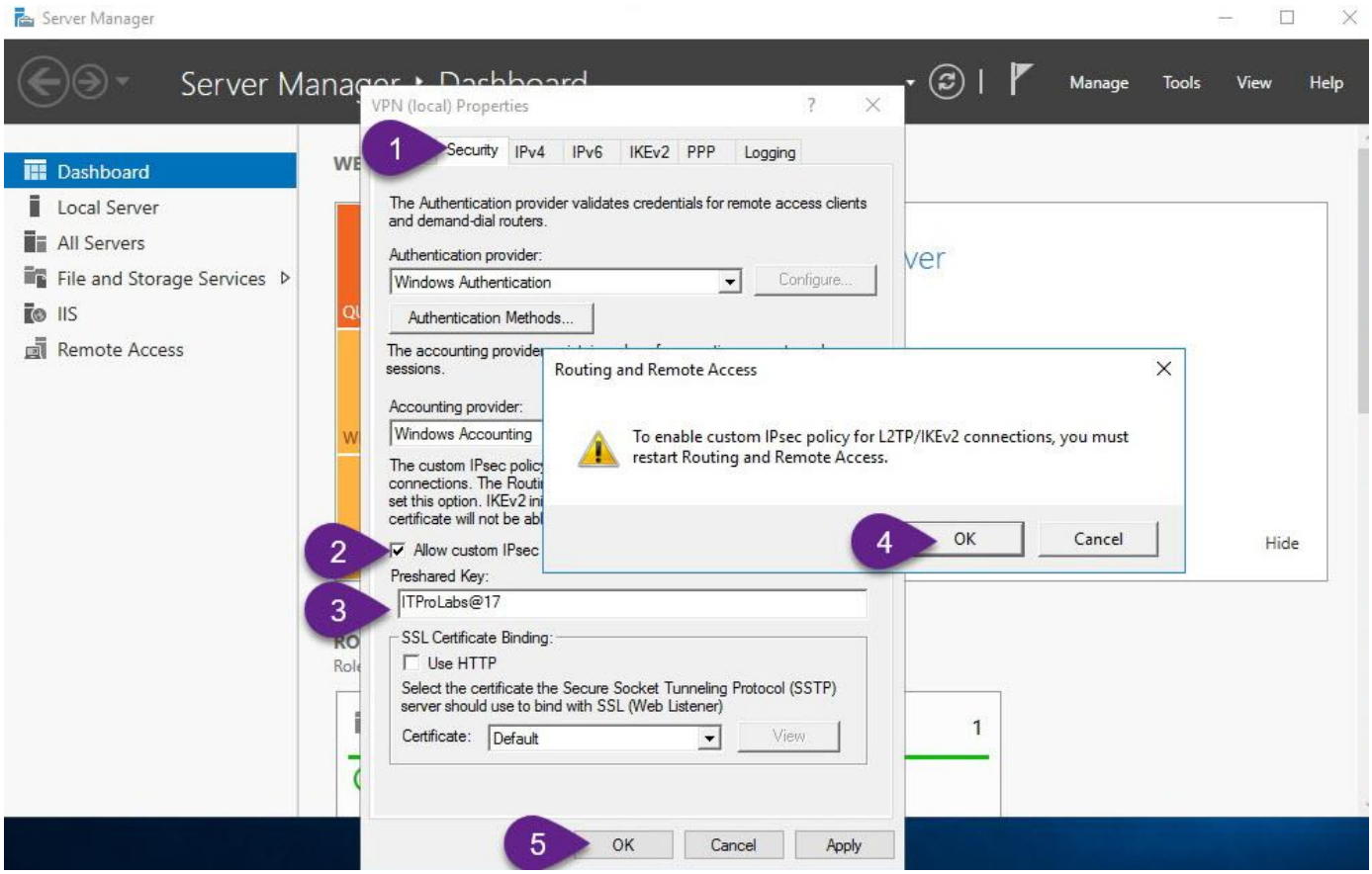
This section will enable VPN clients to receive TCP/IP settings from DHCP. Moreover, it is advantageous for VPN users to utilize the internal DNS server, which simplifies the process of locating and utilizing internal network resources.





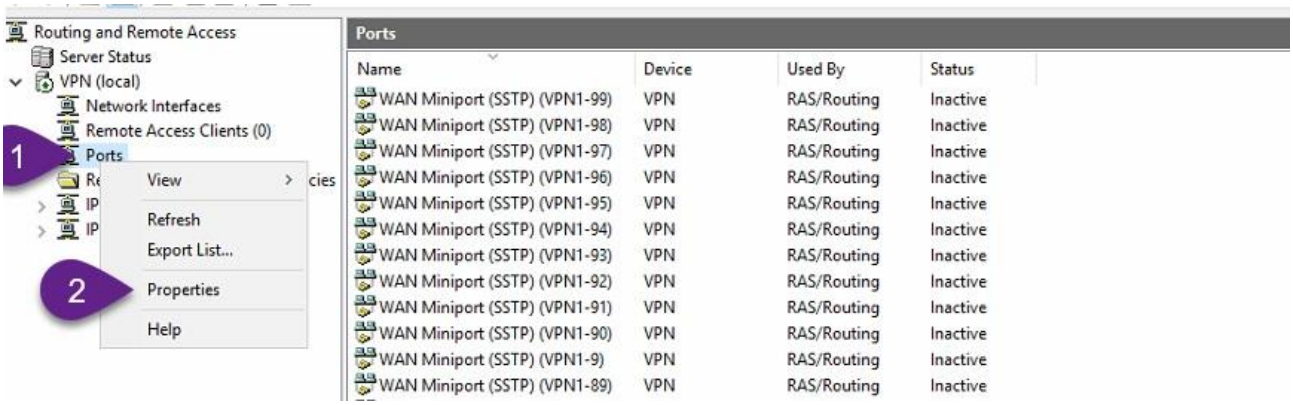
Step 5: Set up a preshared key for the IPSec connection

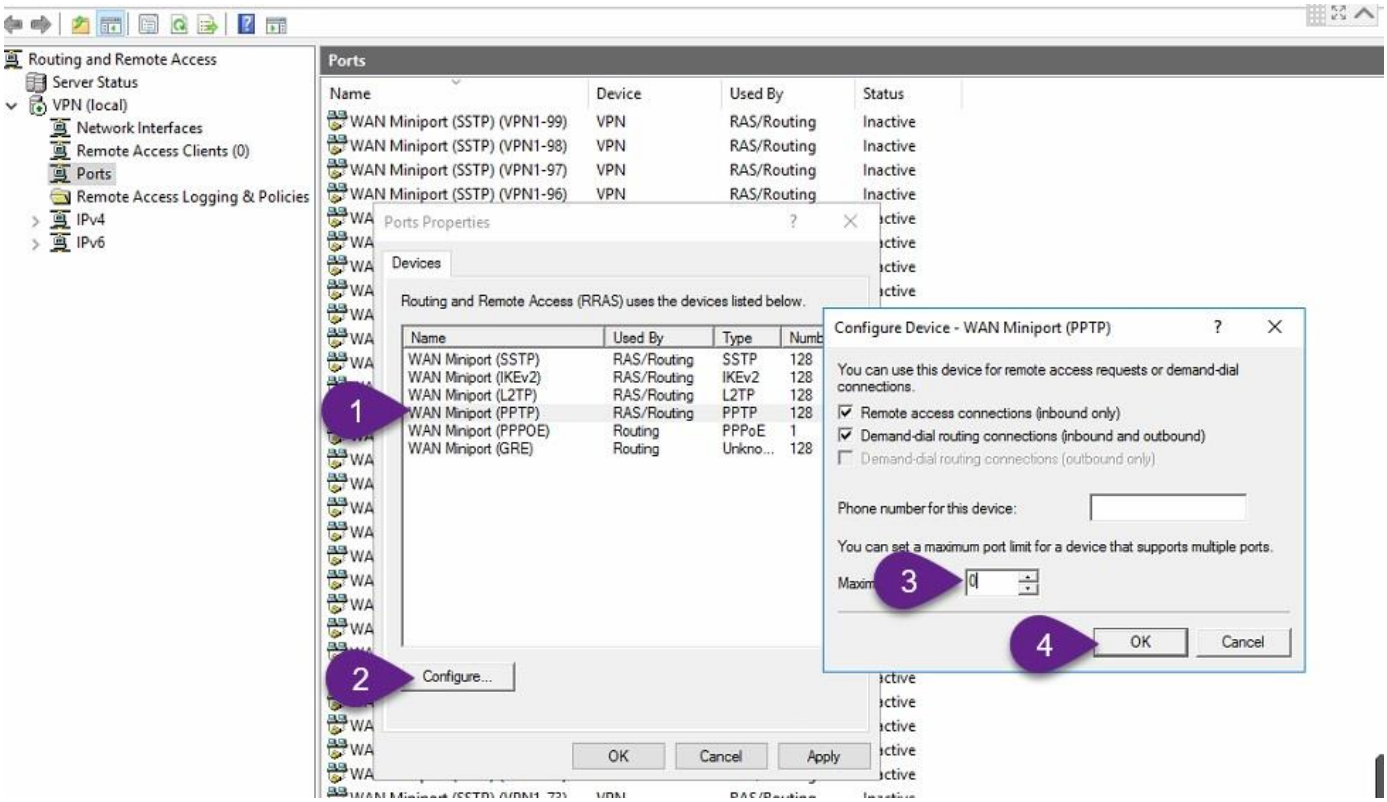
Set up a preshared key on the VPN server to be utilized for IPSec connections.



Disable PPTP connections

The VPN Server is initially configured to allow up to 128 simultaneous connections for PPTP, SSTP, and L2TP. This limit can be either raised or lowered according to your needs, and you can even disable it by setting the concurrent connection count down to zero, as detailed in the following figures.

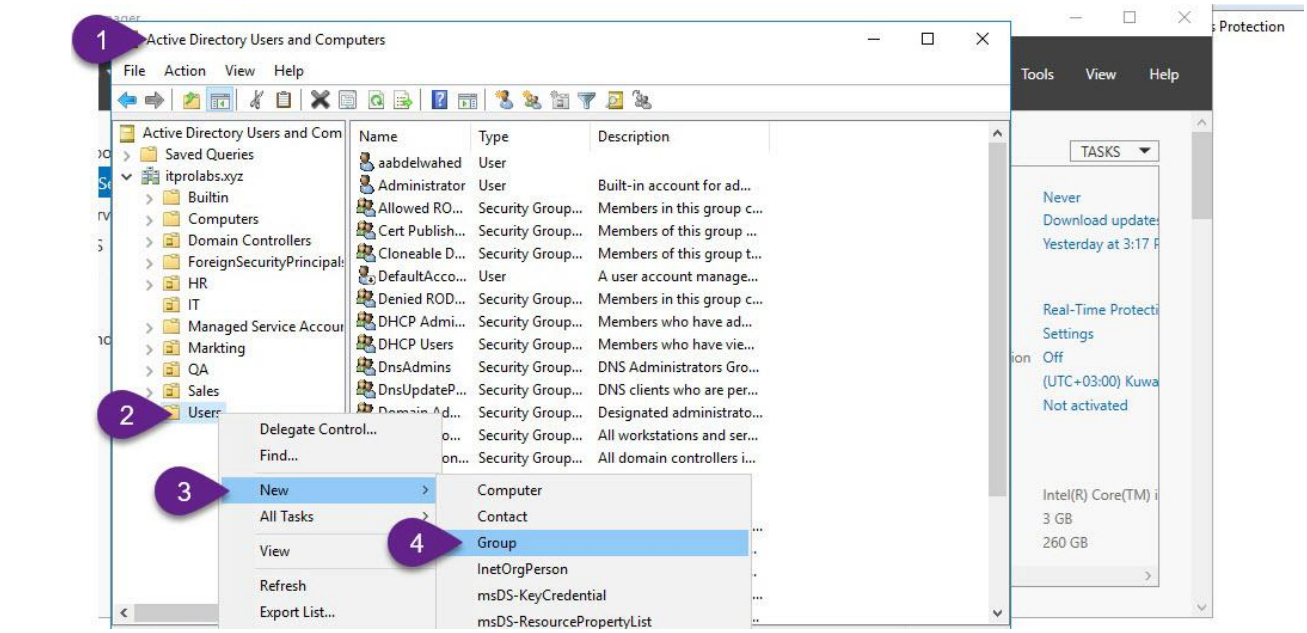


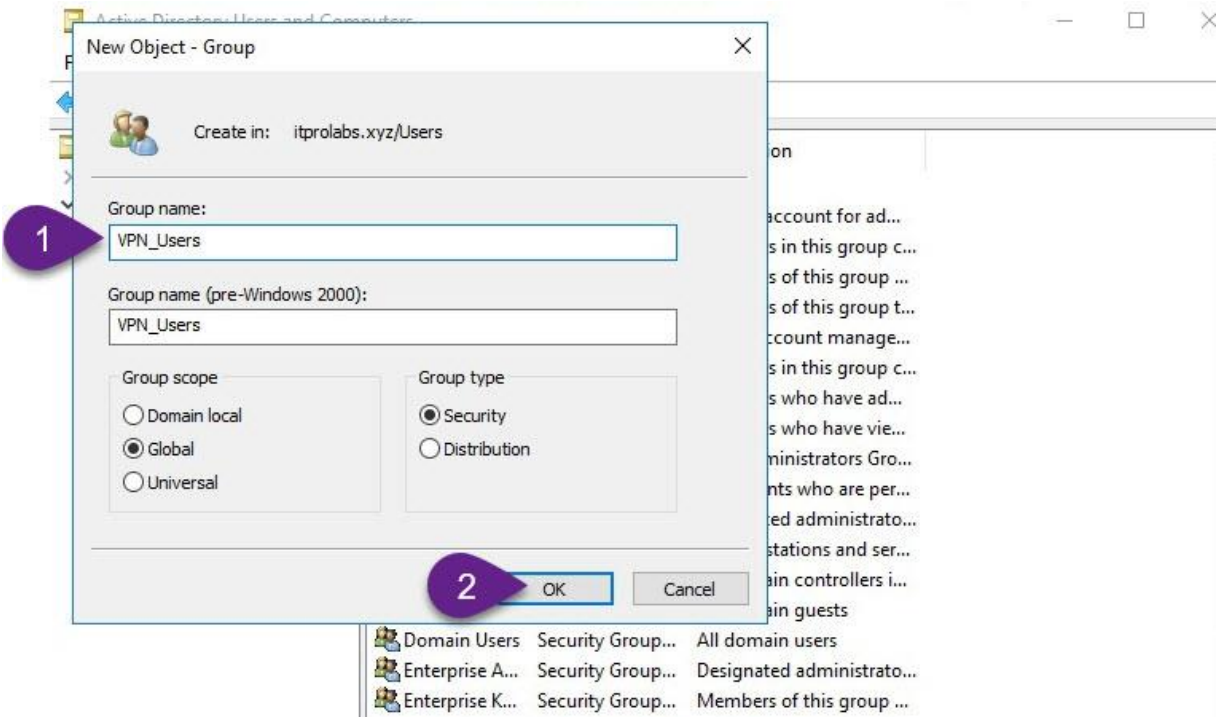

Routing and Remote Access
Server Status
VPN (local)
Network Interfaces
Remote Access Clients (0)
Ports
Remote Access Logging & Policies
IPv4
IPv6
Ports
Name
Device
Used By
Status
WAN Miniport (SSTP) (VPN1-99) VPN RAS/Routing Inactive
WAN Miniport (SSTP) (VPN1-98) VPN RAS/Routing Inactive
WAN Miniport (SSTP) (VPN1-97) VPN RAS/Routing Inactive
WAN Miniport (SSTP) (VPN1-96) VPN RAS/Routing Inactive
Ports Properties
Devices
Routing and Remote Access (RRAS) uses the devices listed below.
Name
Used By
Type
WAN Miniport (SSTP) RAS/Routing SSTP 128
WAN Miniport (IKEv2) RAS/Routing IKEv2 128
WAN Miniport (L2TP) RAS/Routing L2TP 128
WAN Miniport (PPTP) RAS/Routing PPTP 128
WAN Miniport (PPPOE) Routing PPPoE 1
WAN Miniport (GRE) Routing Unkno... 128
1
2
Configure...
OK
Cancel
Apply
Configure Device - WAN Miniport (PPTP)
You can use this device for remote access requests or demand-dial connections.
Remote access connections (inbound only)
Demand-dial routing connections (inbound and outbound)
Demand-dial routing connections (outbound only)
Phone number for this device:
You can set a maximum port limit for a device that supports multiple ports.
3
4
OK
Cancel

Allowing internet users to connect through VPN

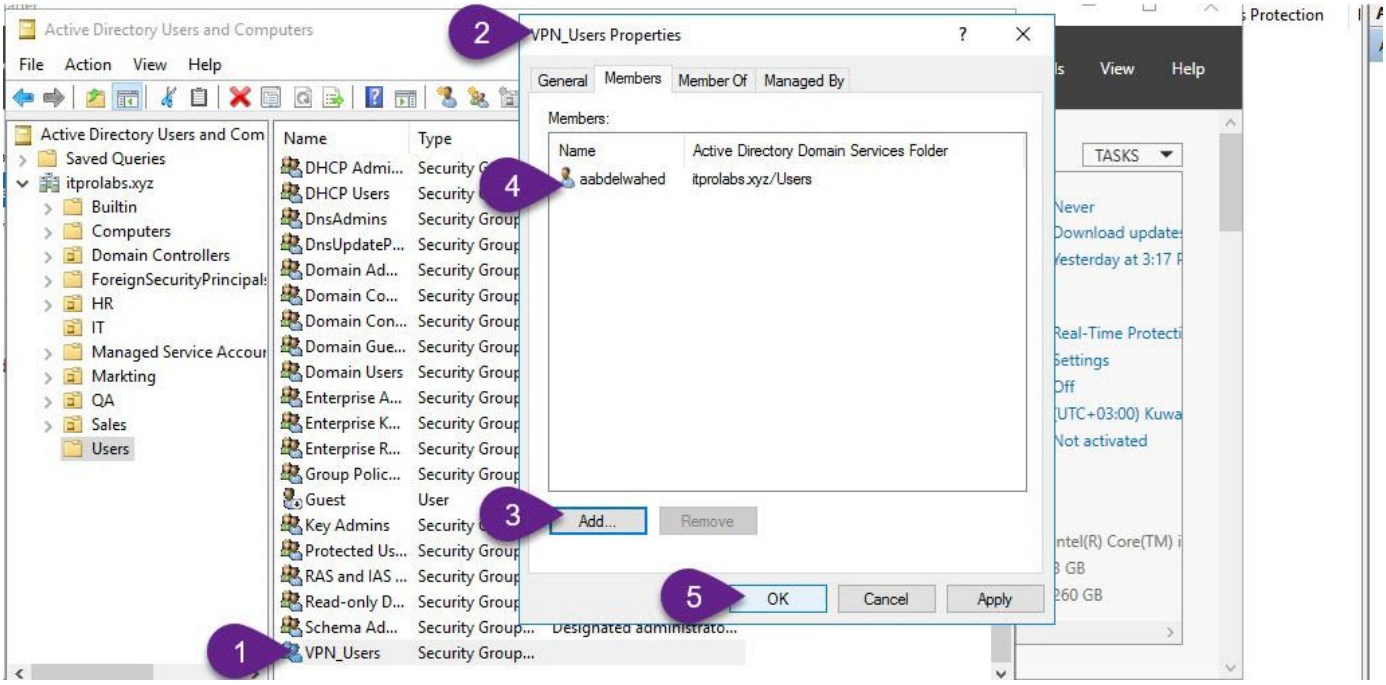
Step 1: Active Directory Configuration

To permit only specific users to access VPN, create an Active Directory group called 'VPN_Users' using the Active Directory Users and Computers tool. Add a user, such as 'aabdelwahed', for testing purposes. These settings apply to the ITPROLABS.XYZ domain on the DC01 server.



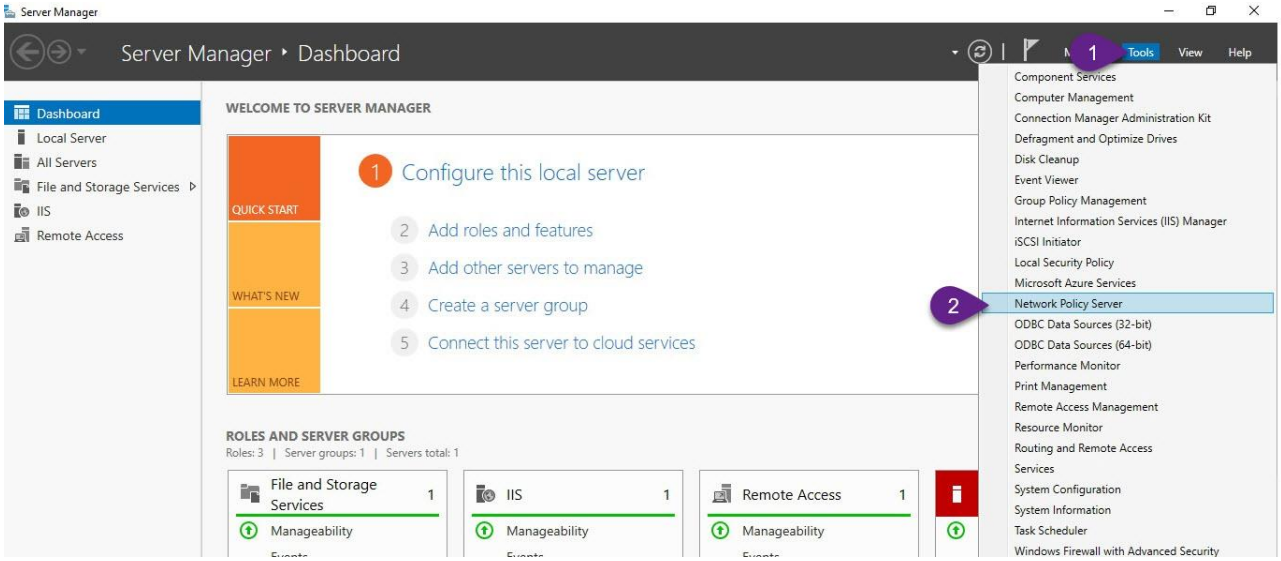


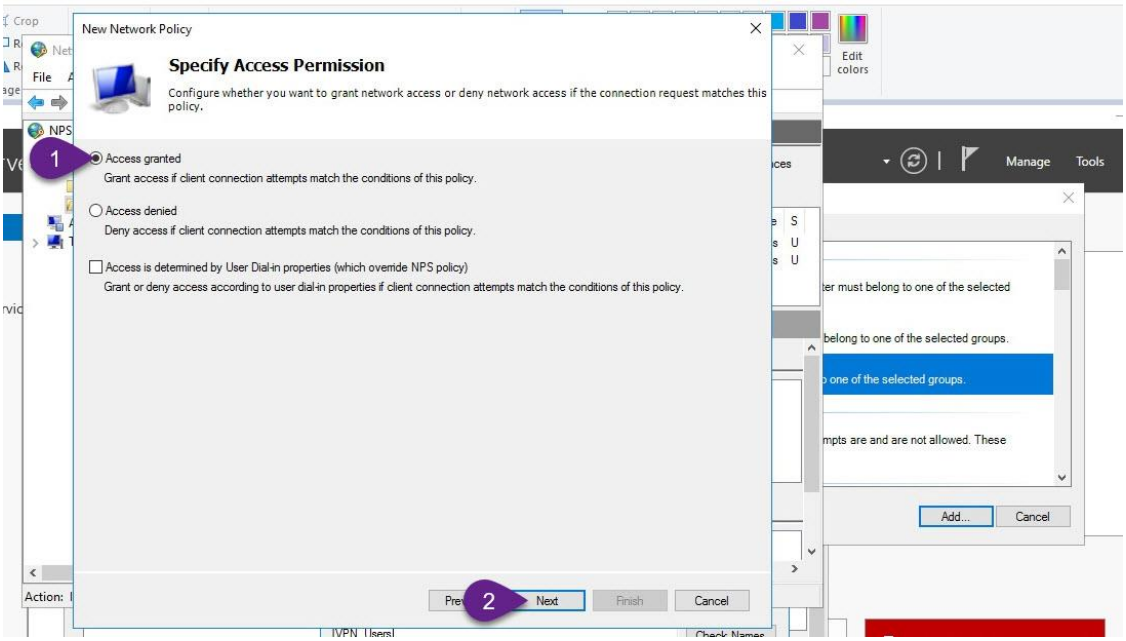
You are now able to include members in this group whom you wish to grant VPN access privileges.



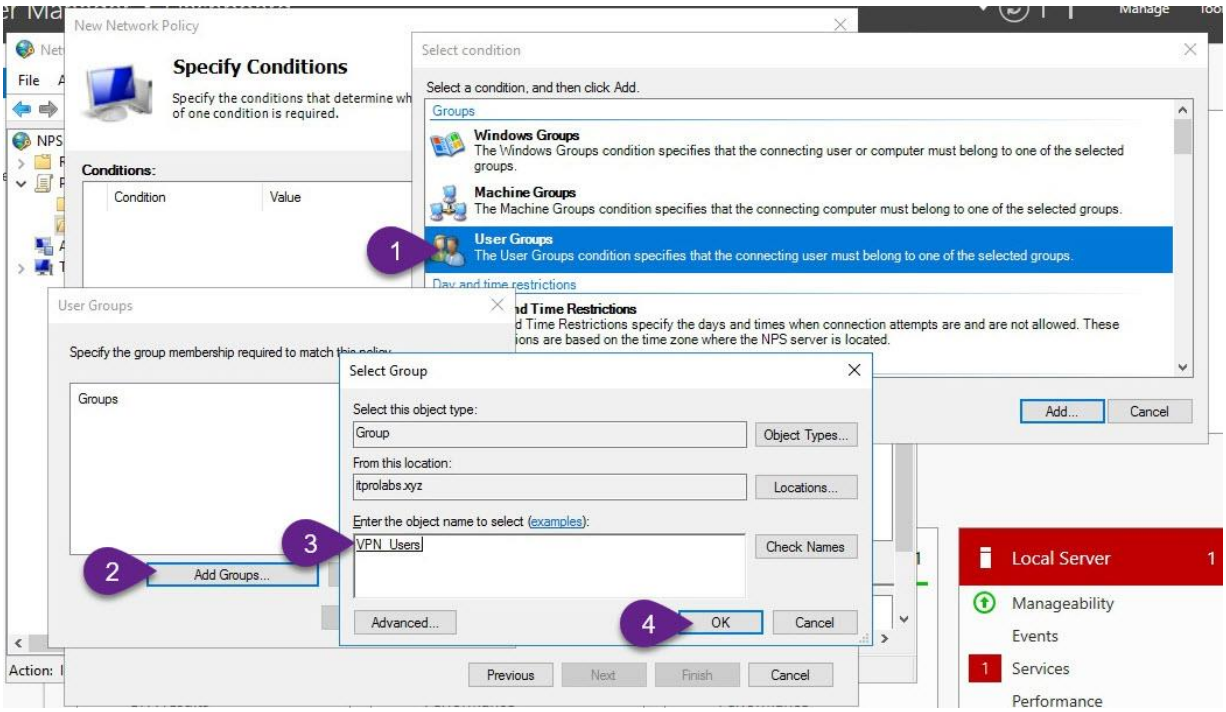
Step 2: Configure the Remote Access policies (NPS)

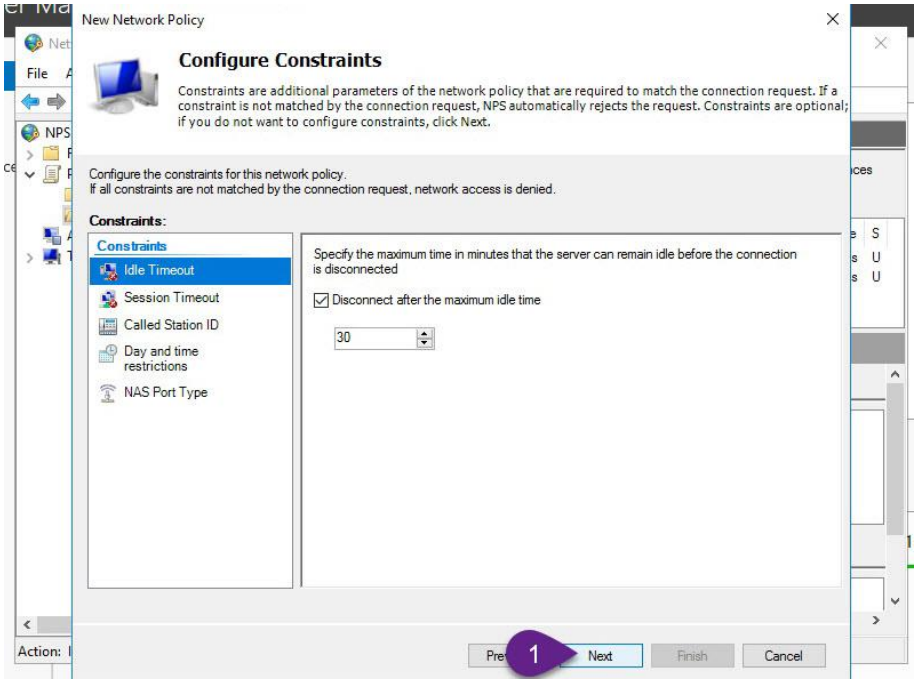
To enable users for VPN access, they must receive permission via the Network Policy Server or individually through 'dial-in' access in the Active Directory Users and Computers wizard. Using Network Policy Server (NPS), we going to allow VPN_Users group to access using VPN.



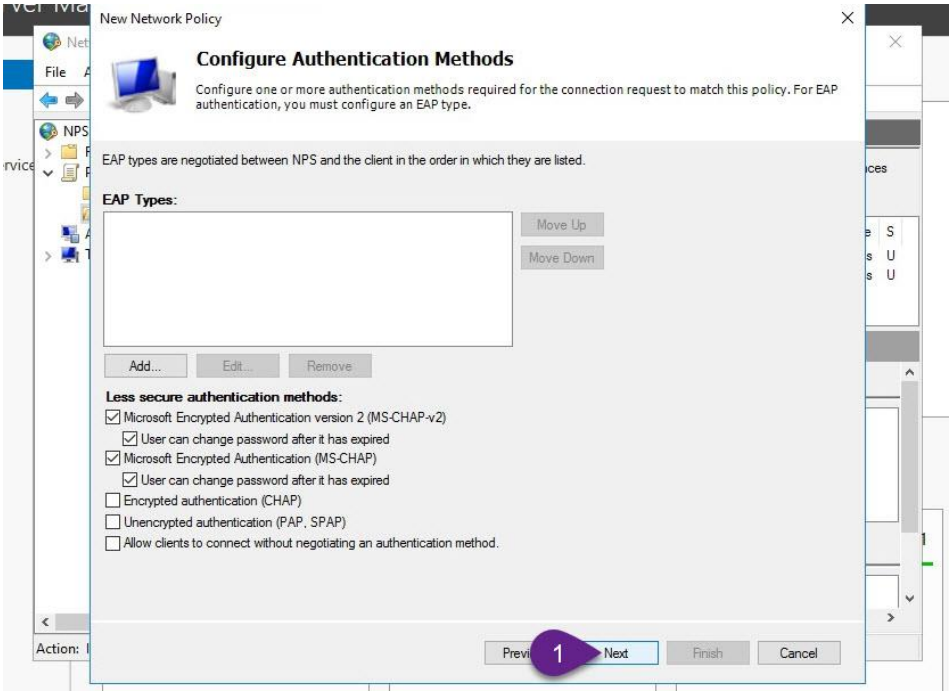


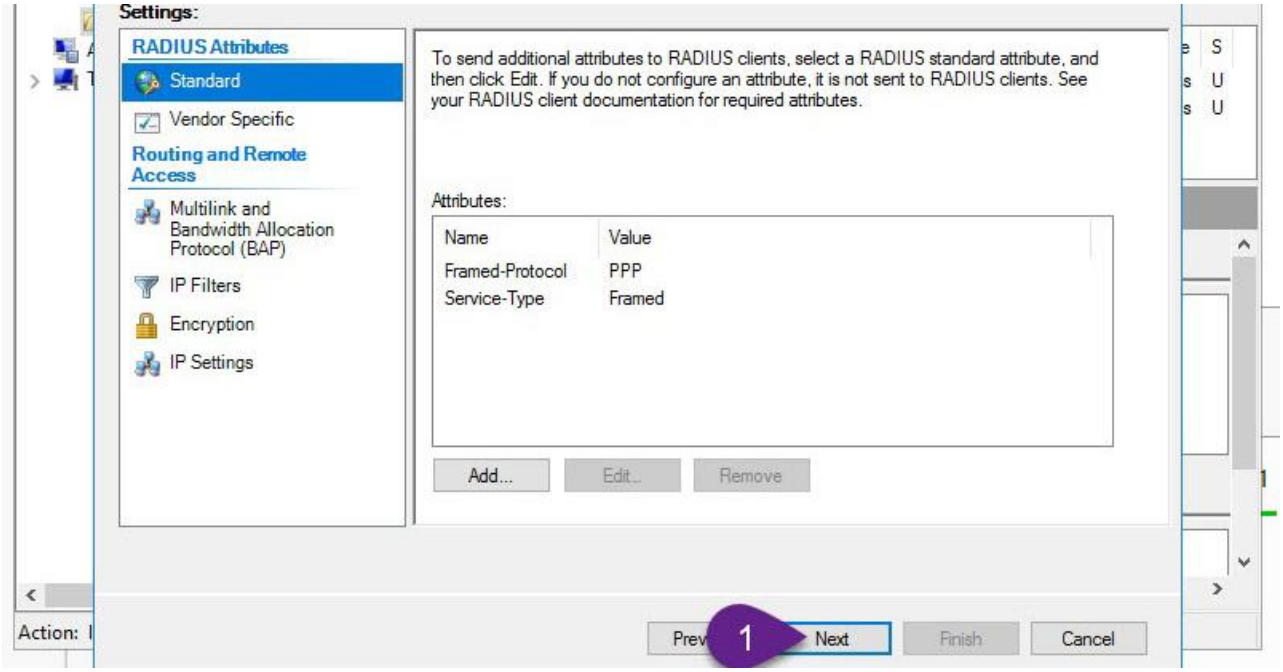
Include the users and groups you wish to authorize for VPN access.

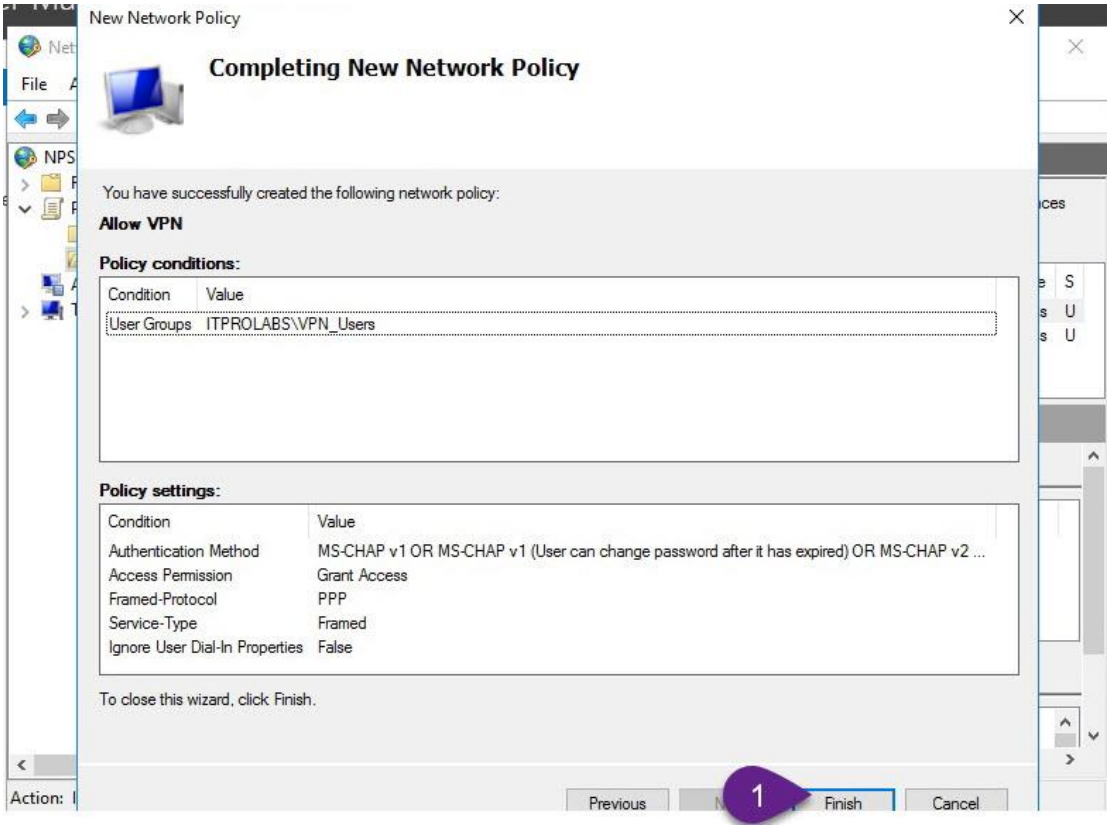




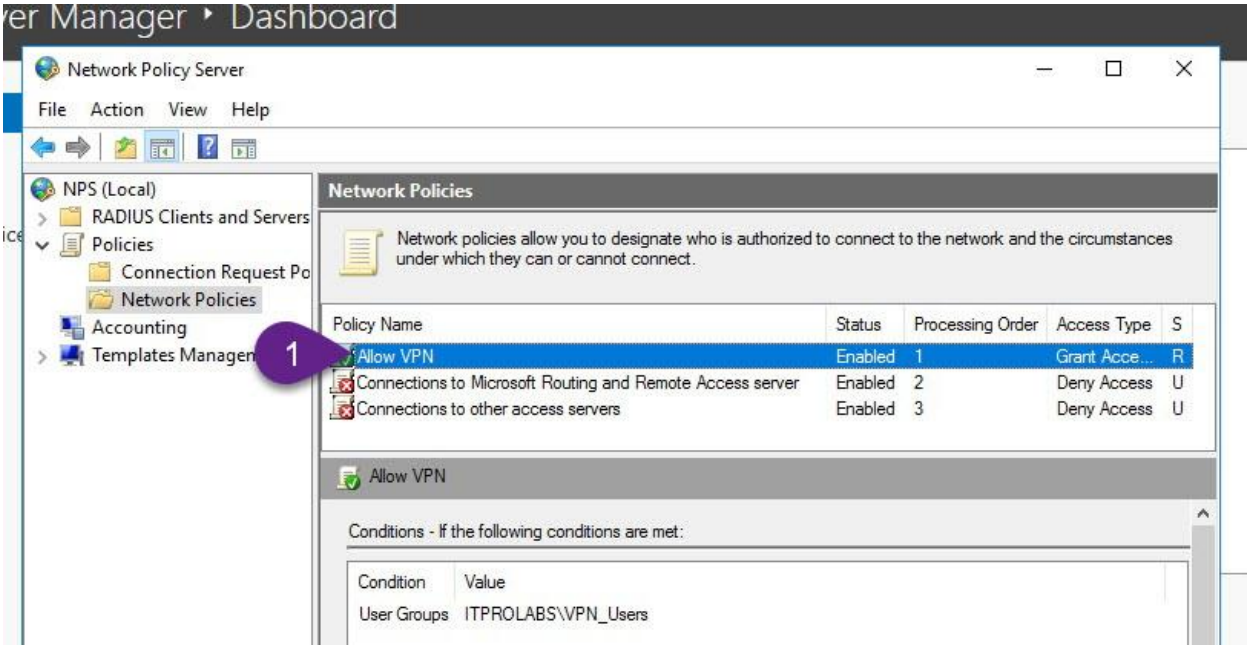
Using this wizard, we can implement policies and restrictions for VPN clients, such as setting a limit on session duration.




Settings:
RADIUS Attributes
Standard
Vendor Specific
Routing and Remote Access
Multilink and Bandwidth Allocation Protocol (BAP)
IP Filters
Encryption
IP Settings
To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.
Attributes:
Name
Value
Framed-Protocol
PPP
Service-Type
Framed
Add...
Edit...
Remove
Action:
Prev
1
Next
Finish
Cancel


New Network Policy
Completing New Network Policy
You have successfully created the following network policy:
Allow VPN
Policy conditions:
Condition
Value
User Groups
ITPROLABS\VPN_Users
Policy settings:
Condition
Value
Authentication Method
MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has expired) OR MS-CHAP v2 ...
Access Permission
Grant Access
Framed-Protocol
PPP
Service-Type
Framed
Ignore User Dial-In Properties
False
To close this wizard, click Finish.
Action:
Previous
1
Finish
Cancel

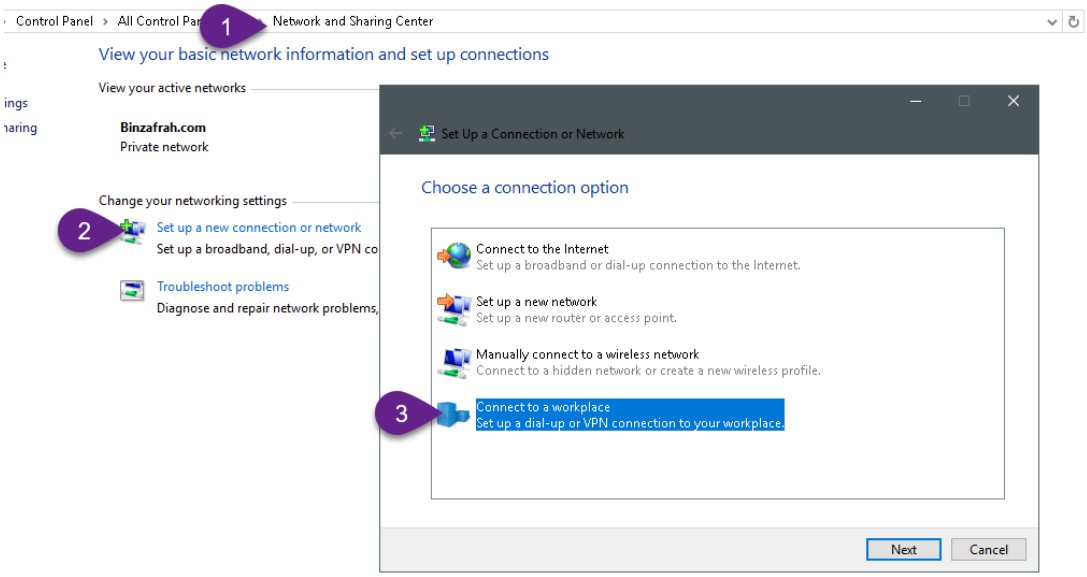
Ensure the policy order you establish is number 1.

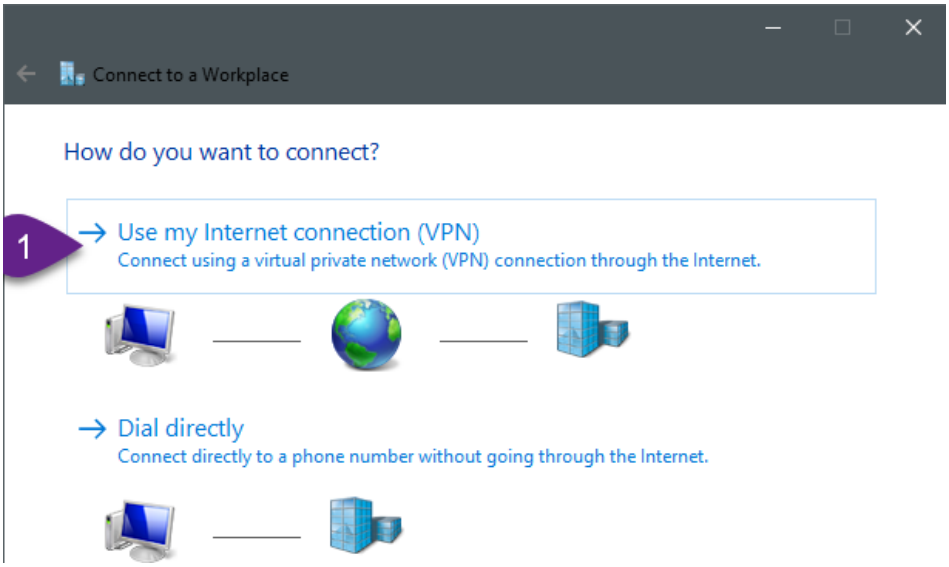


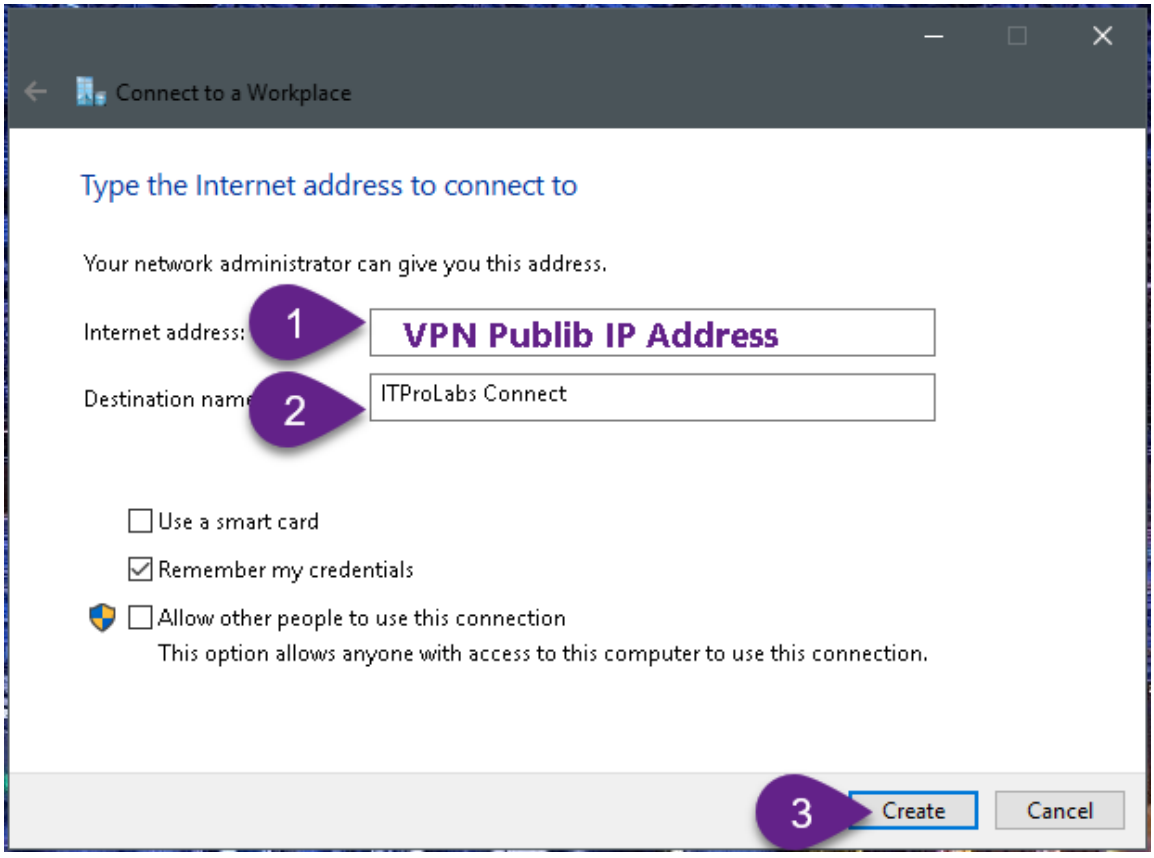
Testing

Create VPN connection from windows 10 Client.

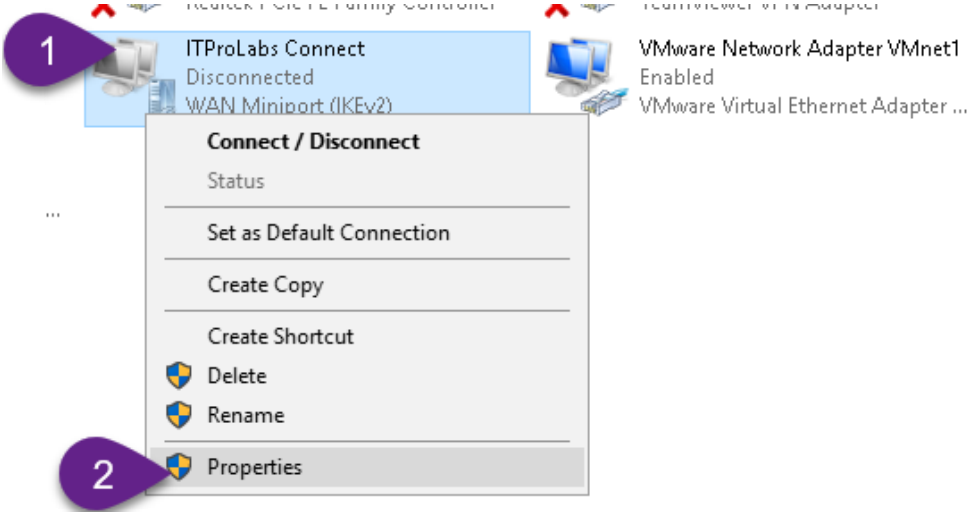
First, set up a VPN connection using the VPN Server's public IP address (as detailed in the figures below).

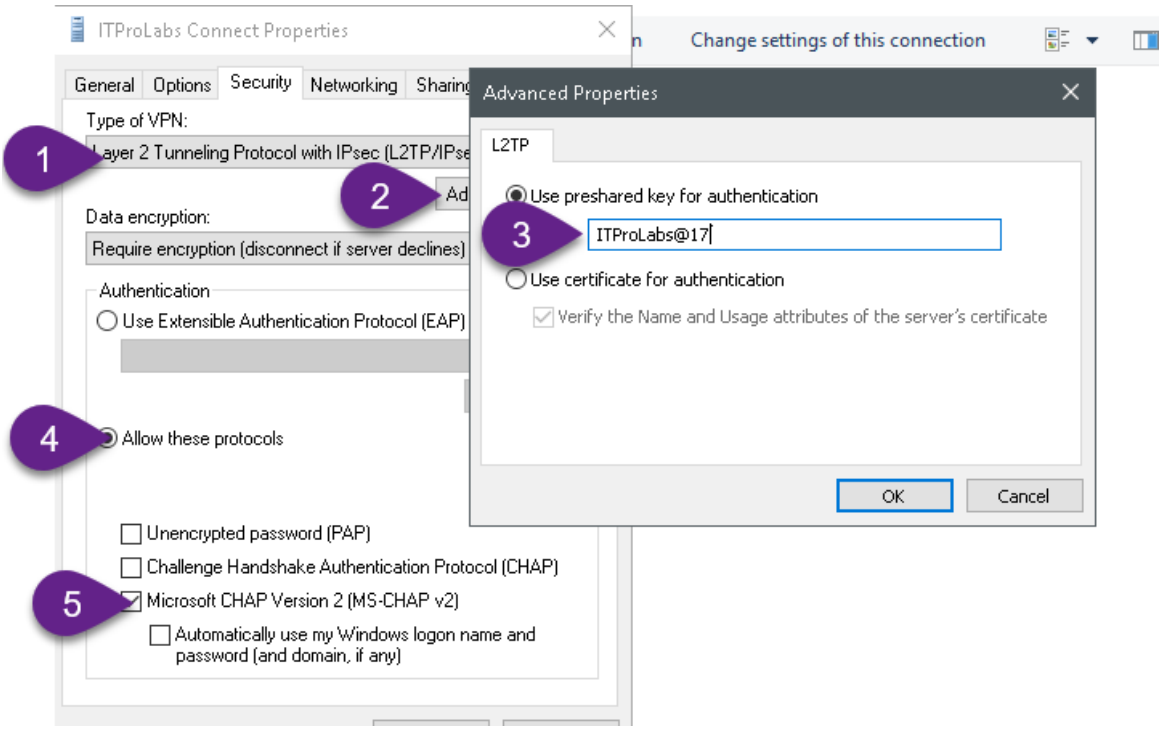



Connect to a Workplace
How do you want to connect?
1
Use my Internet connection (VPN)
Connect using a virtual private network (VPN) connection through the Internet.
Dial directly
Connect directly to a phone number without going through the Internet.


Connect to a Workplace
Type the Internet address to connect to
Your network administrator can give you this address.
Internet address:
1
VPN Publib IP Address
Destination name
2
ITProLabs Connect
Use a smart card
Remember my credentials
Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.
3
Create
Cancel

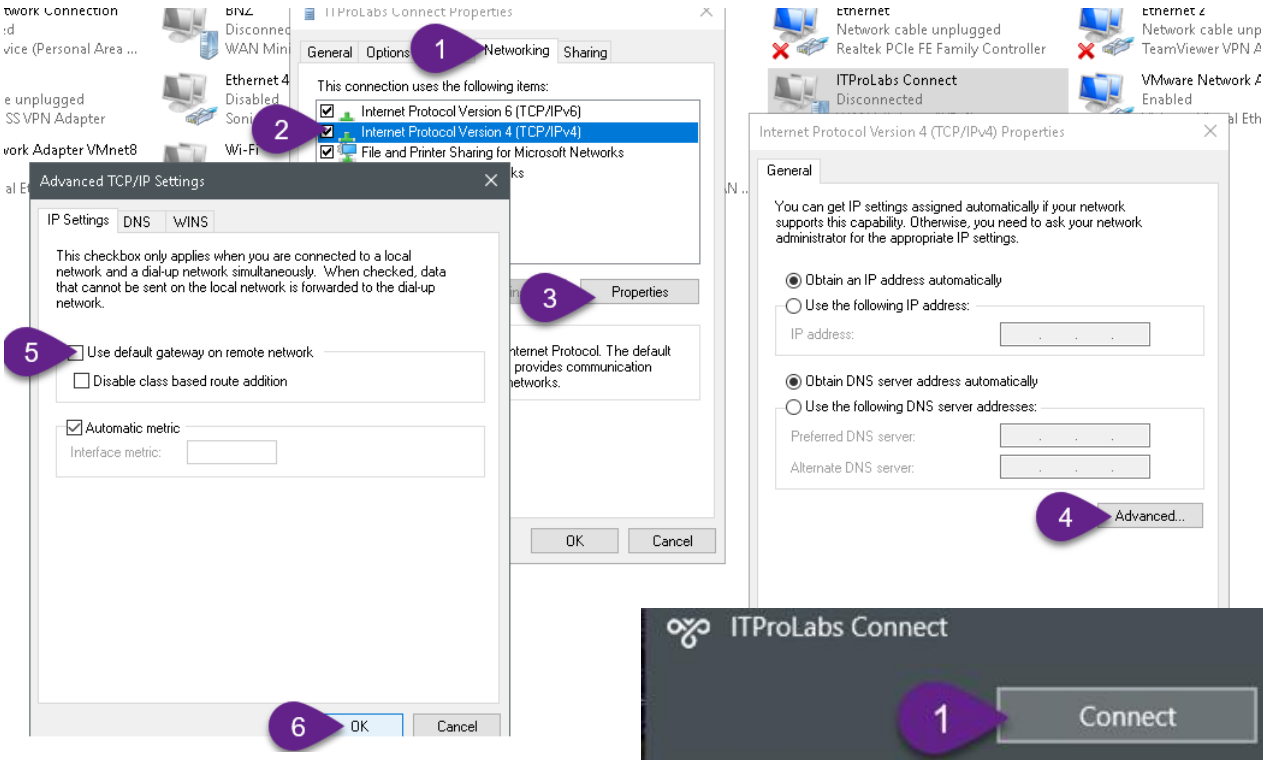
Now, set up our connection to utilize L2TP (as illustrated in the following diagrams)





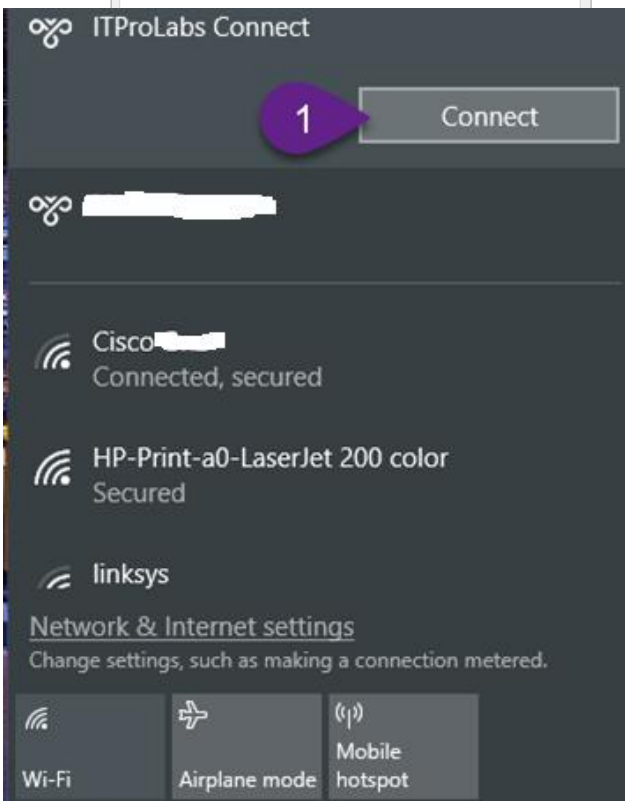
Allow internet connectivity with VPN

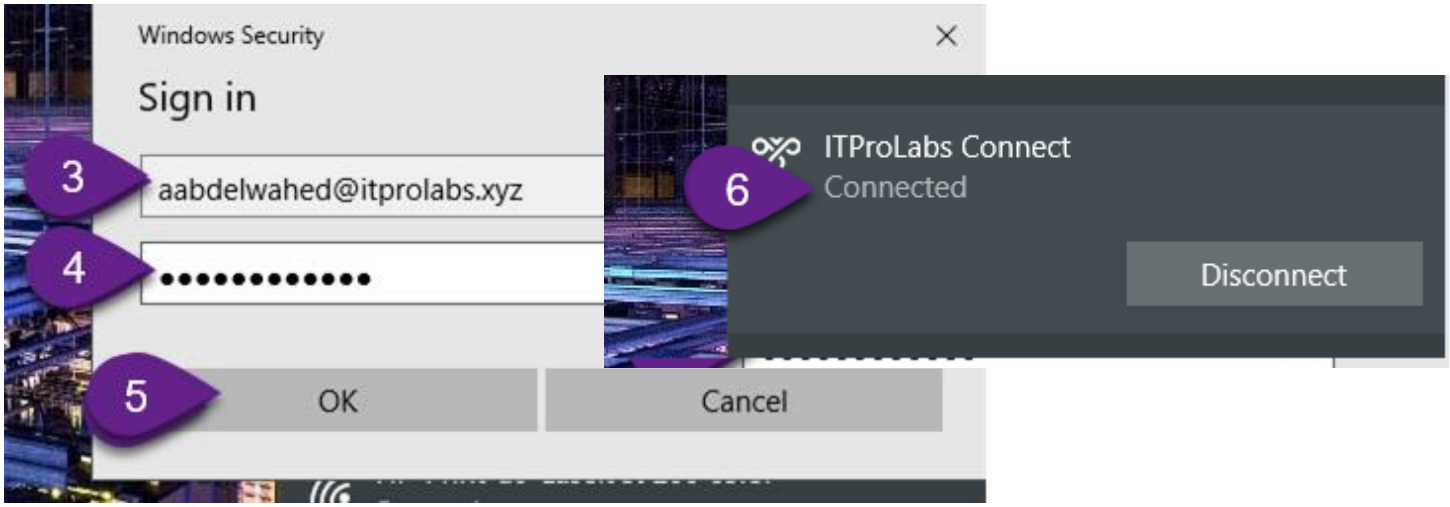
Typically, clients connected to a VPN cannot access the internet; this problem can be resolved as described in the figures that follow.



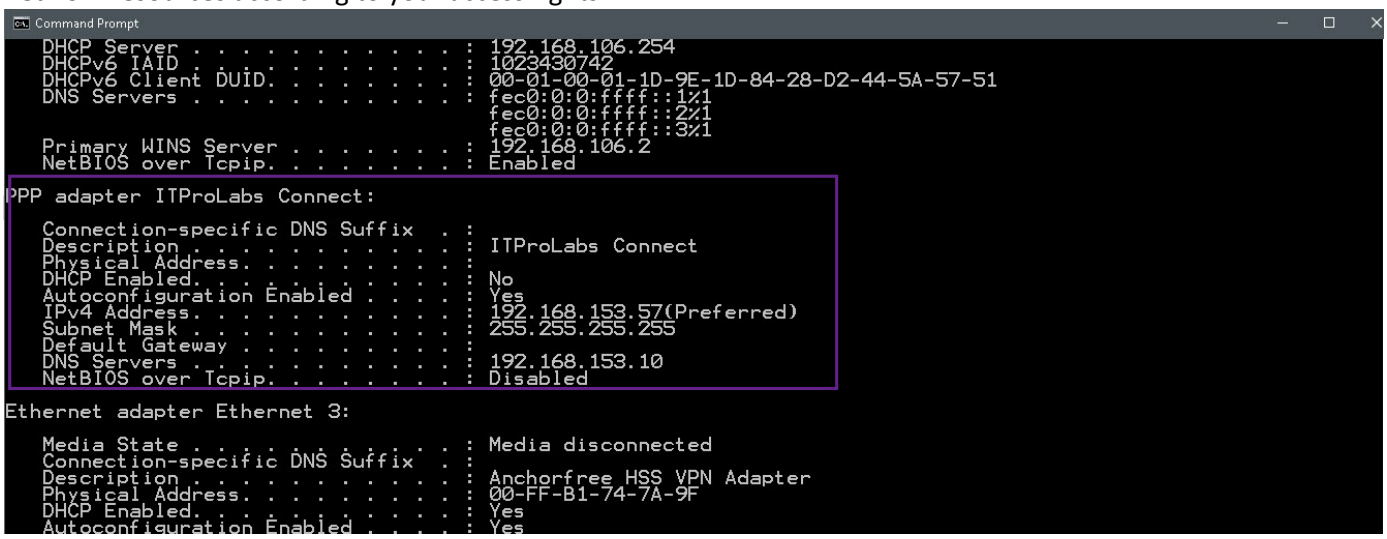
Connect to VPN

You are now able to connect to the VPN using the aabdelwahed user, which has been granted access permissions based on its membership in the VPN_Users group.



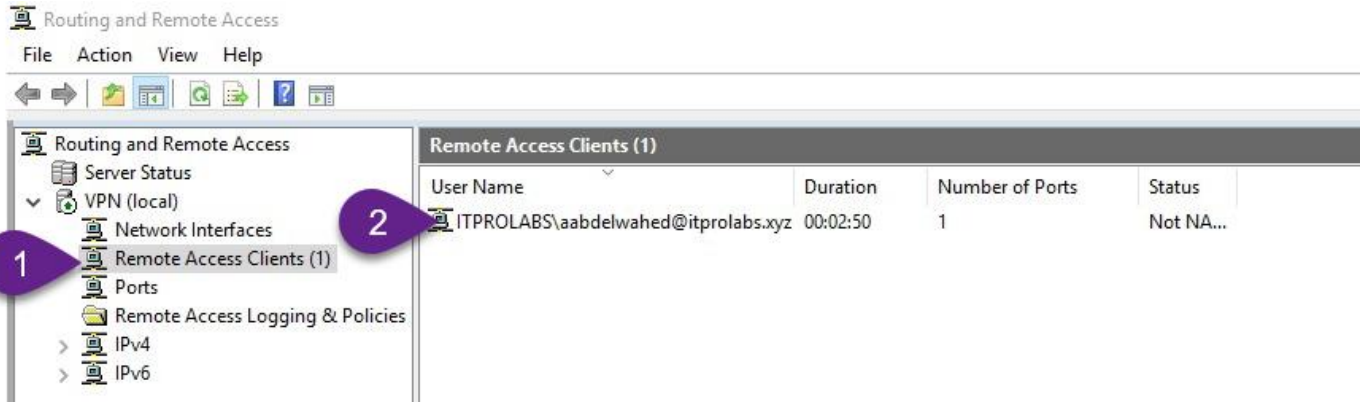


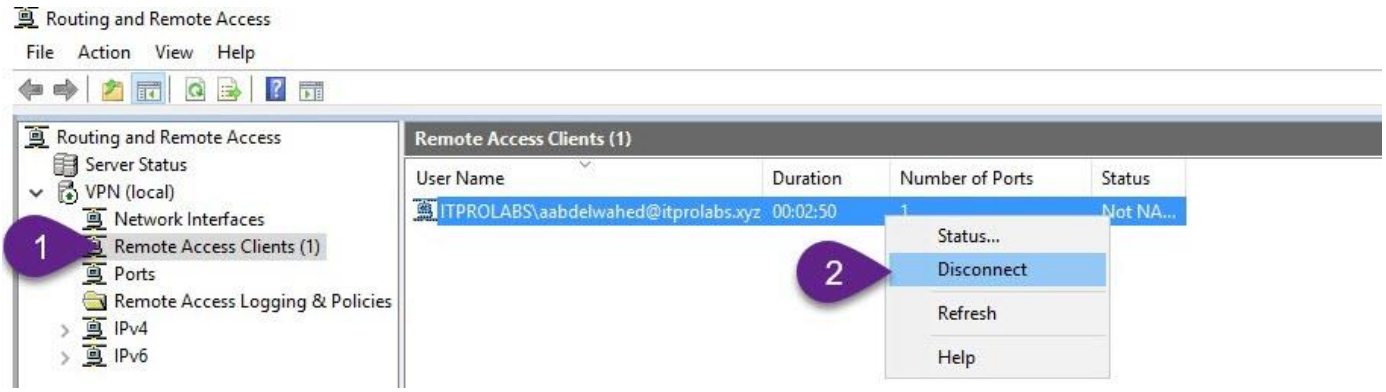
Execute the ipconfig /all command to review your VPN configuration details, which will allow you to utilize network resources according to your access rights.



Check connected VPN client Status

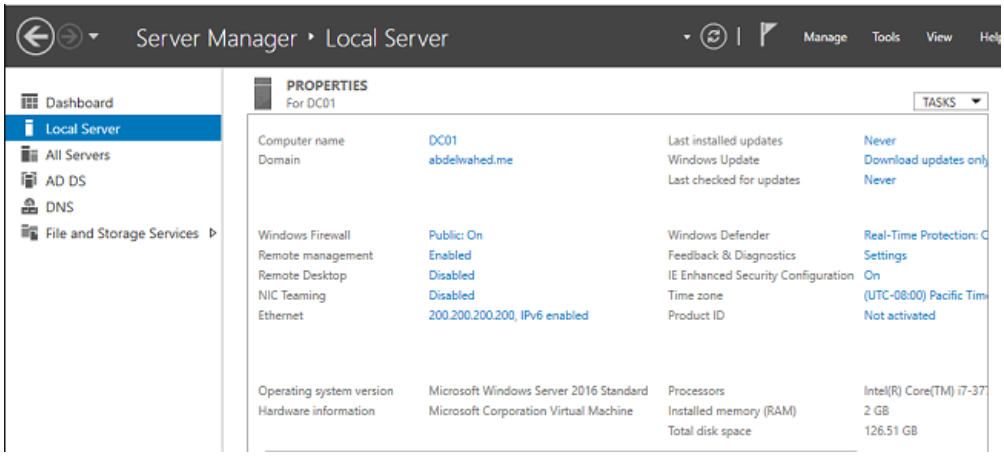
Next, return to the VPN server to verify the status of current user connections. Additionally, you have the option to forcibly disconnect any active users as depicted in the following figures.



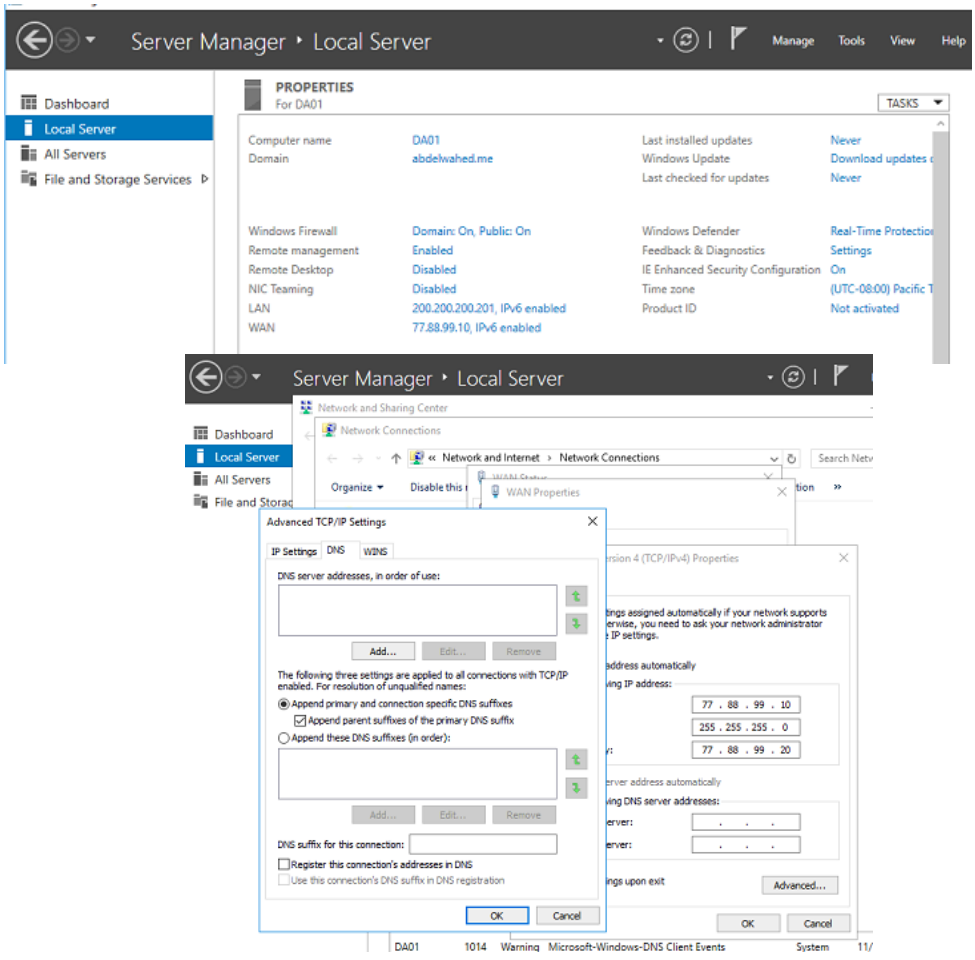


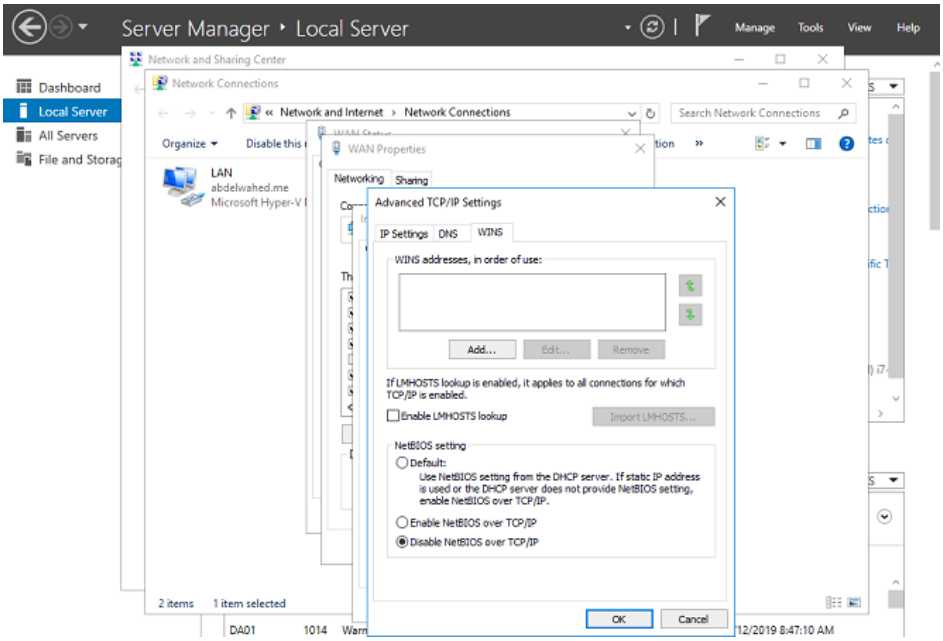
Direct Access

DC Configuration

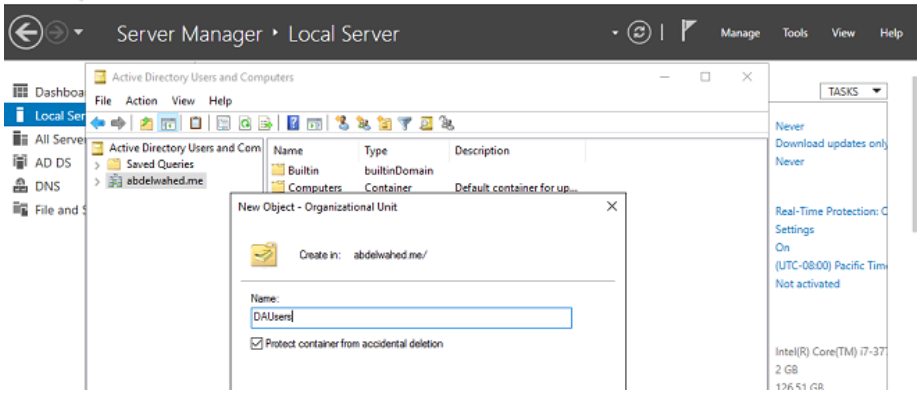


DA network configuration

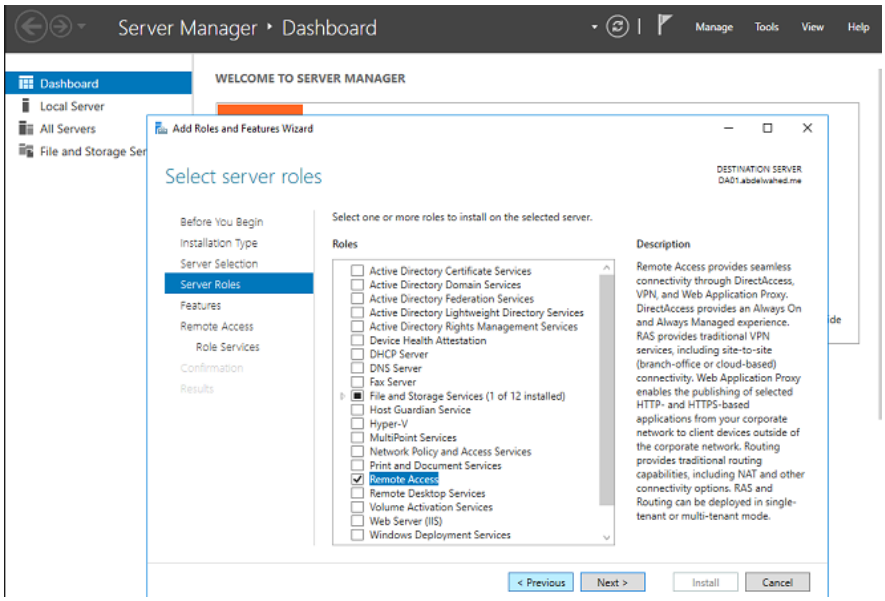


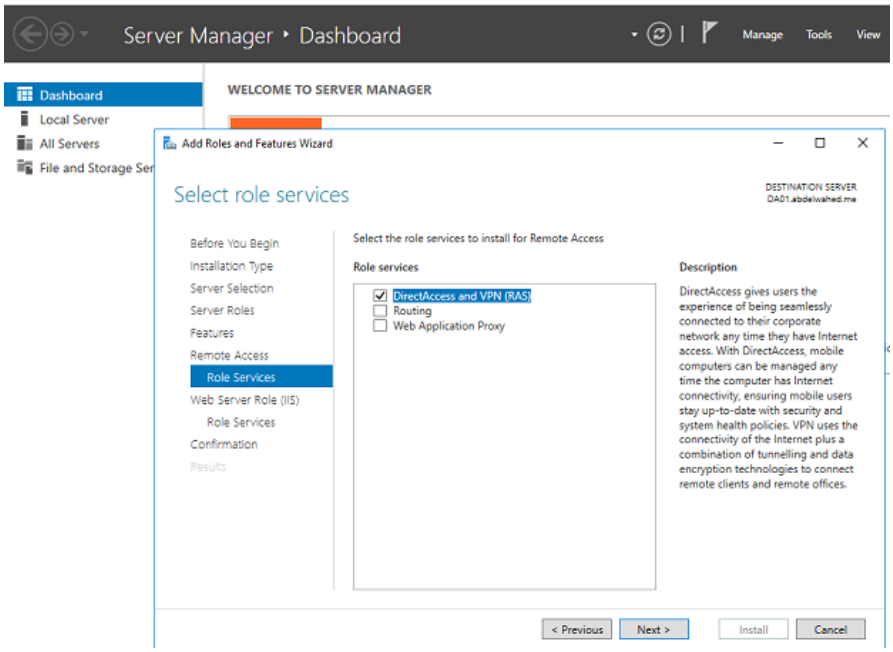


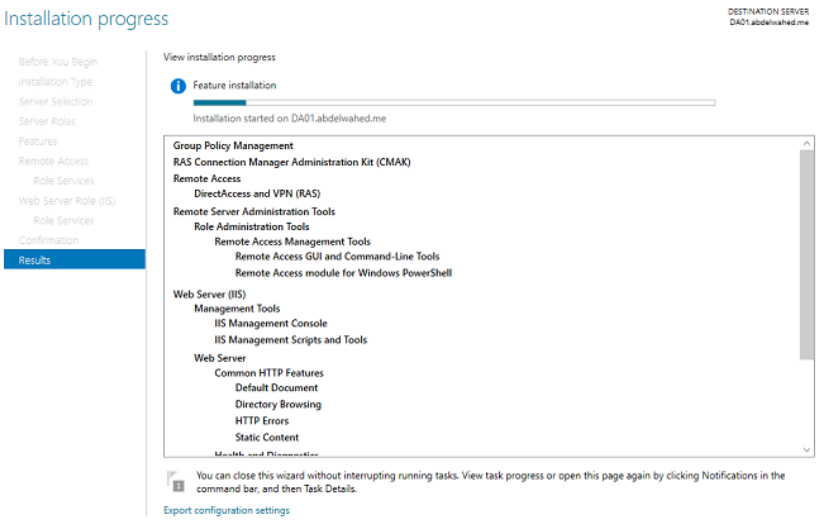
Setting Up a DirectAccess OU and Group in Active Directory

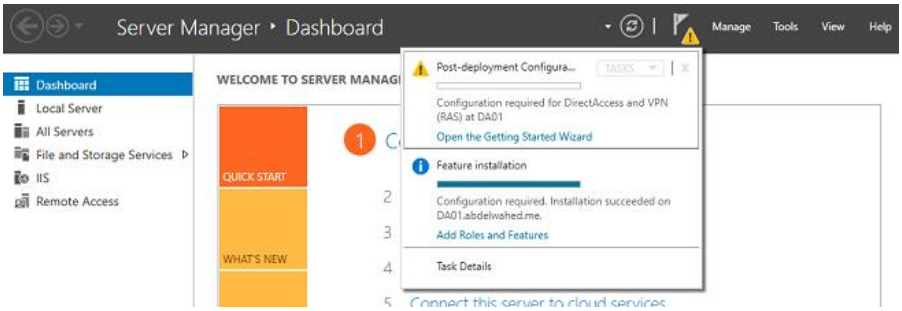


Now install Remote Access on DA Server

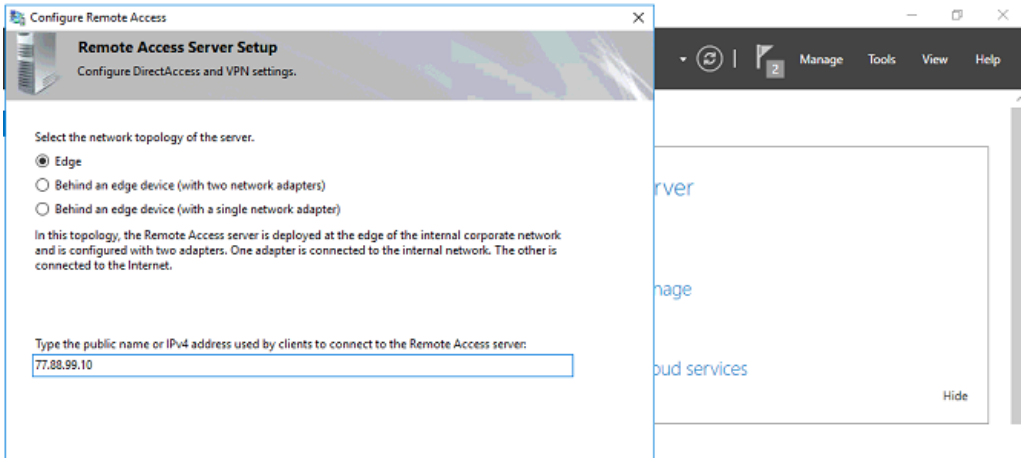




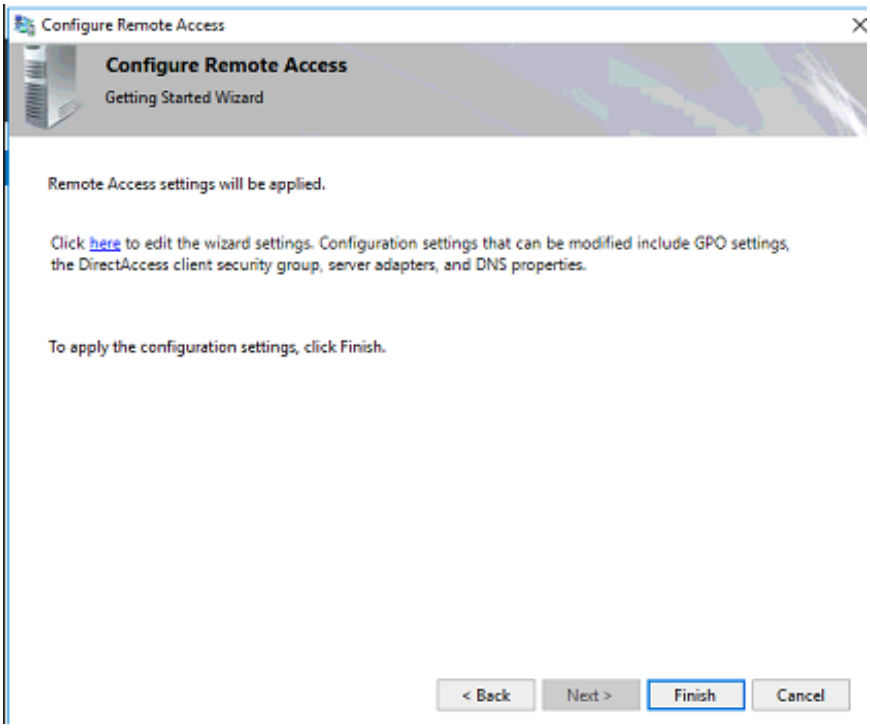


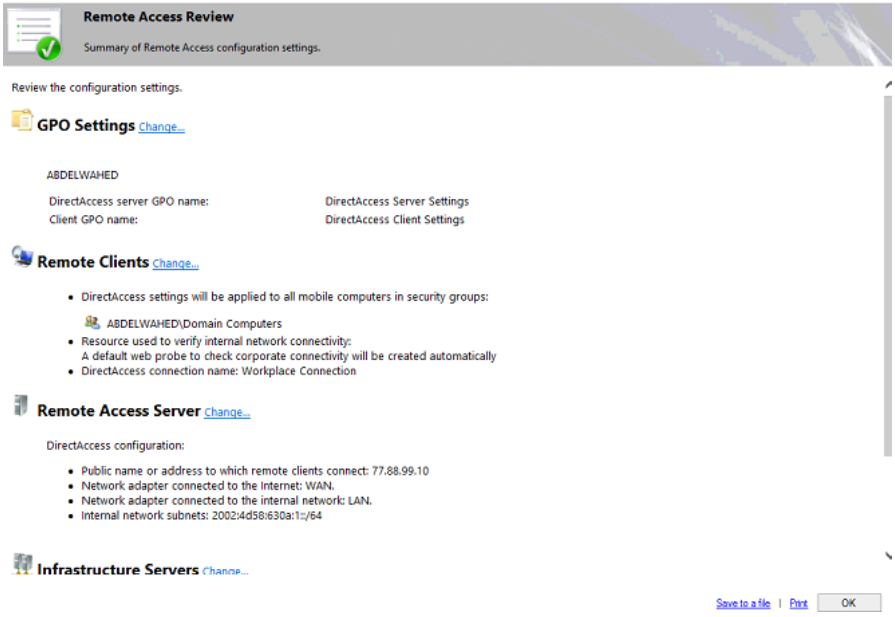


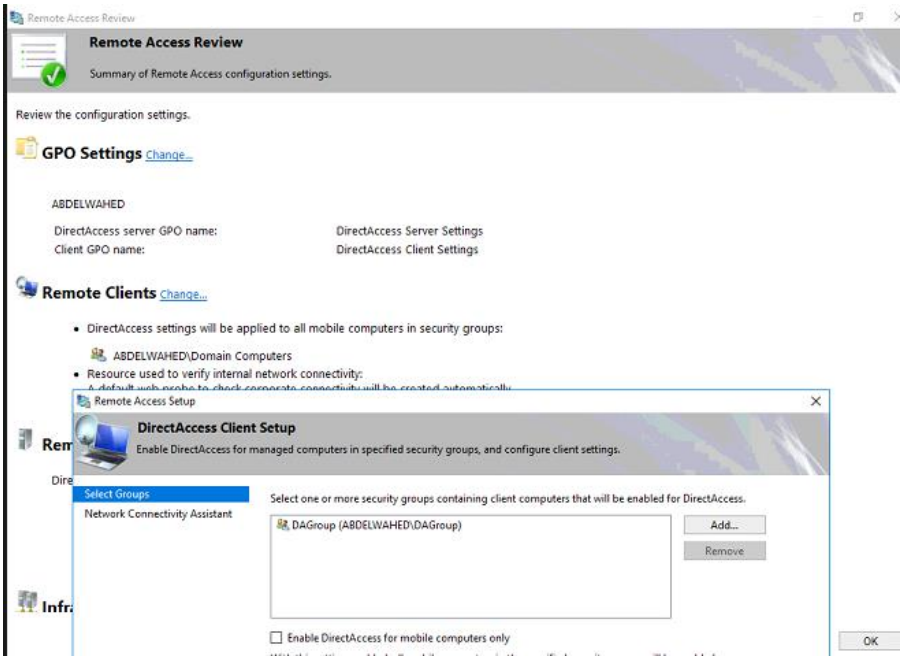
Select Deploy Direct Access only

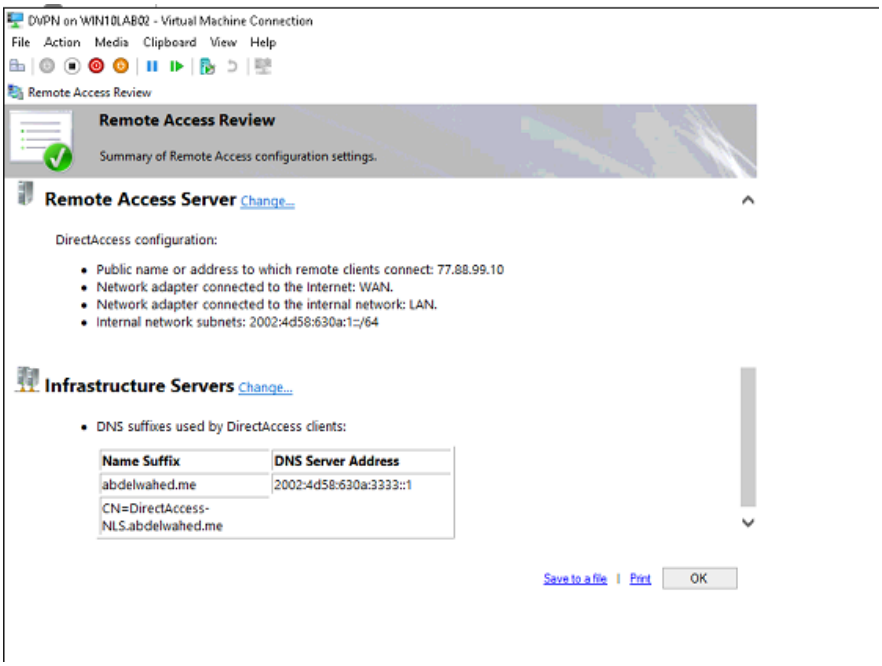


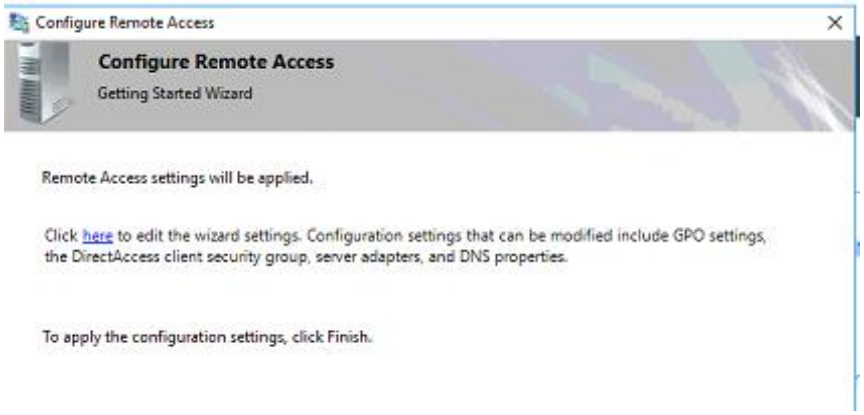
Click here to include permitted group

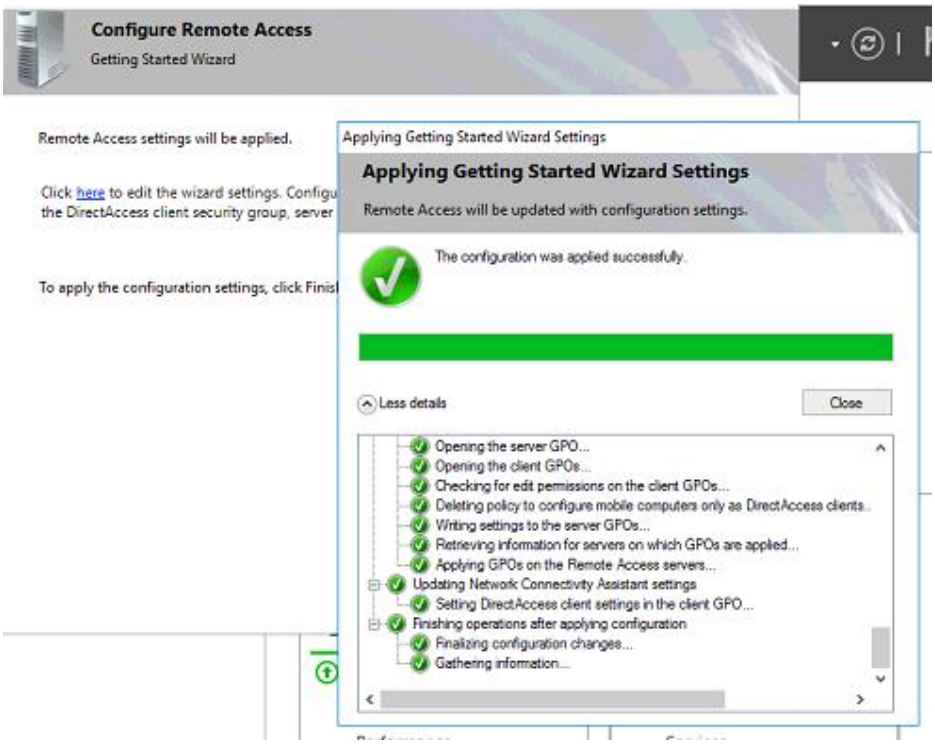


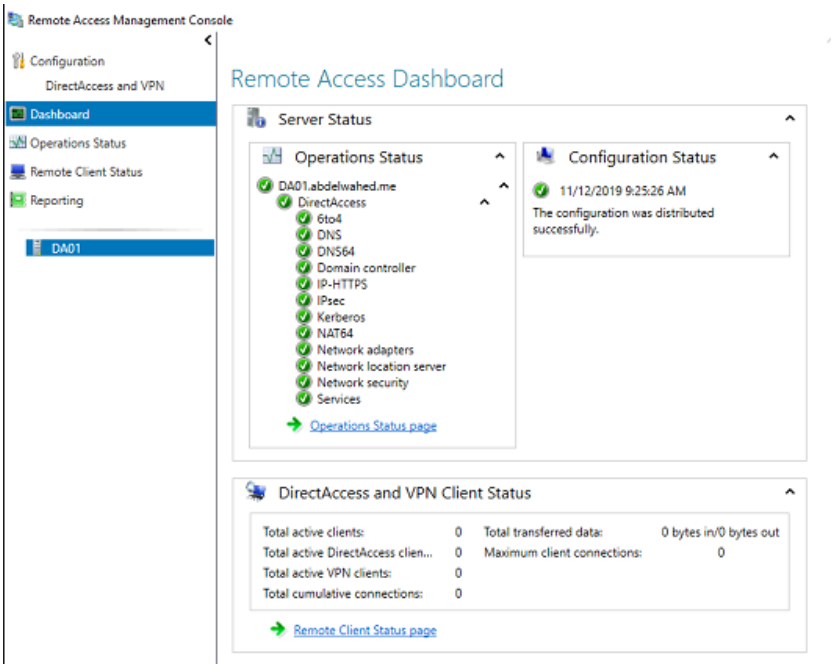



Remote Access Review
Remote Access Review
Summary of Remote Access configuration settings.
Review the configuration settings.
GPO Settings Change...
ABDELWAHED
DirectAccess server GPO name:
DirectAccess Server Settings
Client GPO name:
DirectAccess Client Settings
Remote Clients Change...
DirectAccess settings will be applied to all mobile computers in security groups:
ABDELWAHED\Domain Computers
Resource used to verify internal network connectivity:
Remote Access Setup
DirectAccess Client Setup
Enable DirectAccess for managed computers in specified security groups, and configure client settings.
Select Groups
Network Connectivity Assistant
Select one or more security groups containing client computers that will be enabled for DirectAccess.
DAGroup (ABDELWAHED\DAGroup)
Add...
Remove
Enable DirectAccess for mobile computers only
OK


DVPN on WIN10LAB02 - Virtual Machine Connection
File Action Media Clipboard View Help
Remote Access Review
Remote Access Review
Summary of Remote Access configuration settings.
Remote Access Server Change...
DirectAccess configuration:
Public name or address to which remote clients connect: 77.88.99.10
Network adapter connected to the Internet: WAN.
Network adapter connected to the internal network: LAN.
Internal network subnets: 2002:4d58:630a:1::/64
Infrastructure Servers Change...
DNS suffixes used by DirectAccess clients:
Name Suffix
DNS Server Address
abdelwahed.me
2002:4d58:630a:3333::1
CN=DirectAccess-NLS.abdelwahed.me
Save to a file | Print
OK

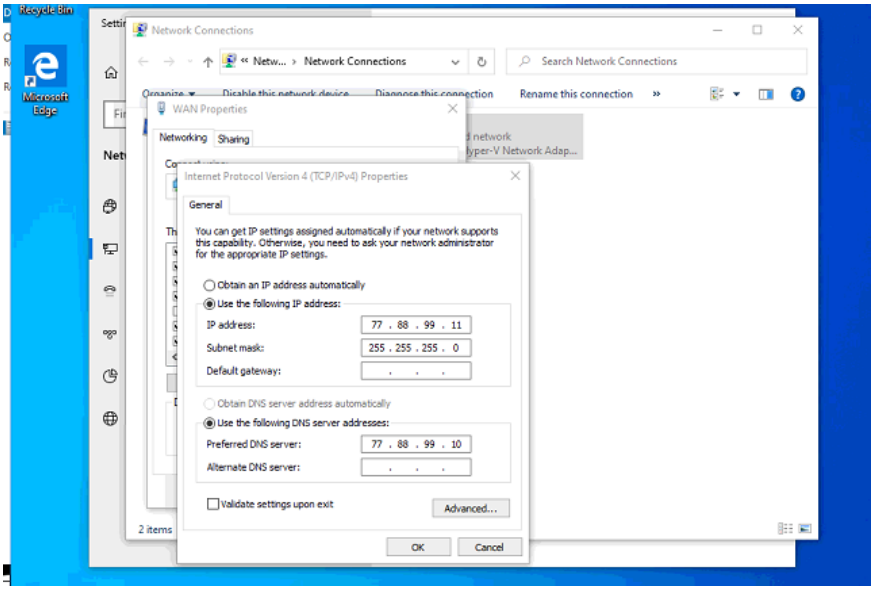

Configure Remote Access
Configure Remote Access
Getting Started Wizard
Remote Access settings will be applied.
Click here to edit the wizard settings. Configuration settings that can be modified include GPO settings, the DirectAccess client security group, server adapters, and DNS properties.
To apply the configuration settings, click Finish.

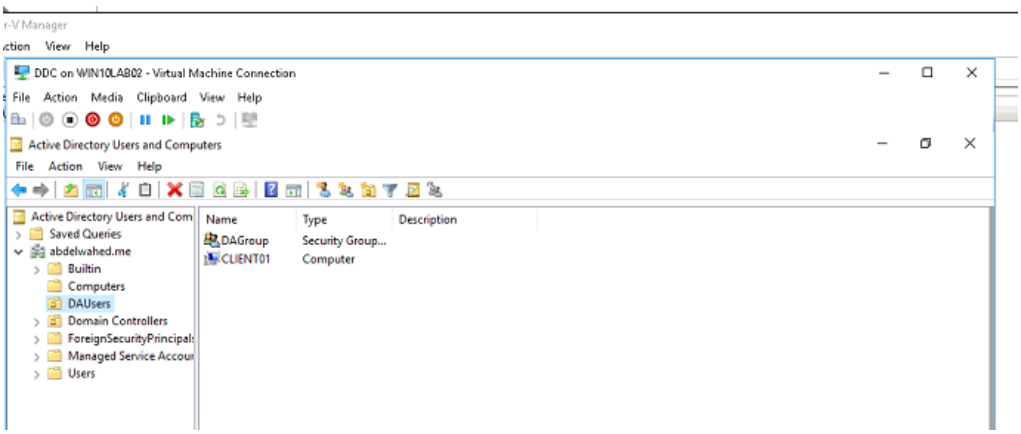

Configure Remote Access
Getting Started Wizard
Remote Access settings will be applied.
Click here to edit the wizard settings. Configu
the DirectAccess client security group, server
To apply the configuration settings, click Finis
Applying Getting Started Wizard Settings
Applying Getting Started Wizard Settings
Remote Access will be updated with configuration settings.
The configuration was applied successfully.
Less details
Close
Opening the server GPO...
Opening the client GPOs...
Checking for edit permissions on the client GPOs...
Deleting policy to configure mobile computers only as DirectAccess clients...
Writing settings to the server GPOs...
Retrieving information for servers on which GPOs are applied...
Applying GPOs on the Remote Access servers...
Updating Network Connectivity Assistant settings
Setting DirectAccess client settings in the client GPO...
Finishing operations after applying configuration
Finalizing configuration changes...
Gathering information...

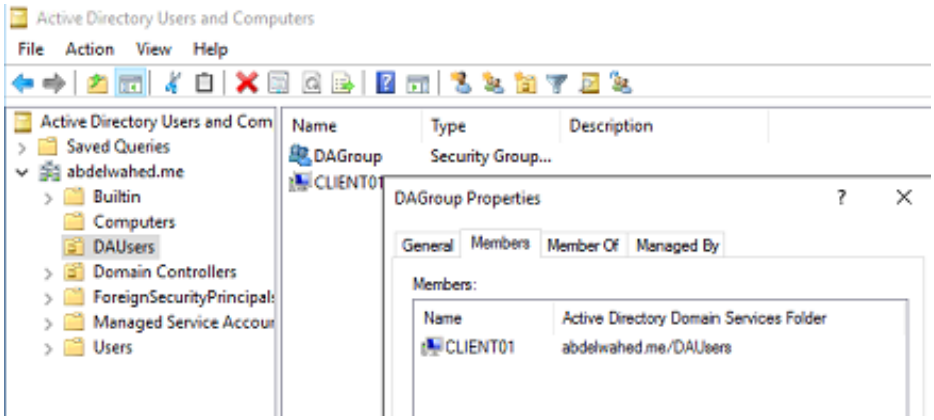


Client Configuration for Direct Access

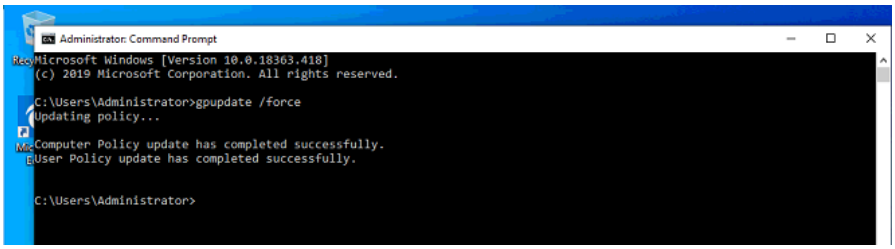
- OS: Windows 10 Enterprise
- add it DAGroup and to DAUSers OU
- L AN IP: 200.200.200.202, DNS: 200.200.200.200
- WAN IP: showed down



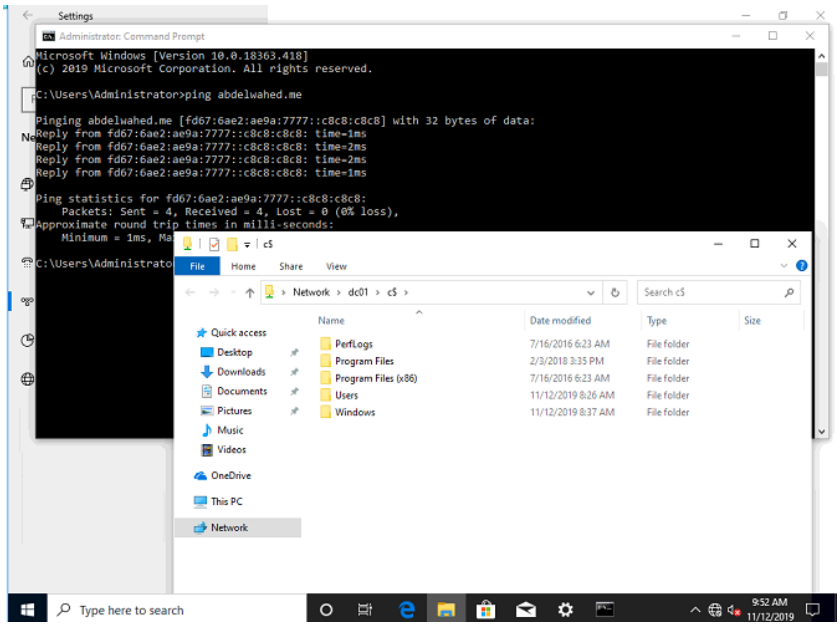


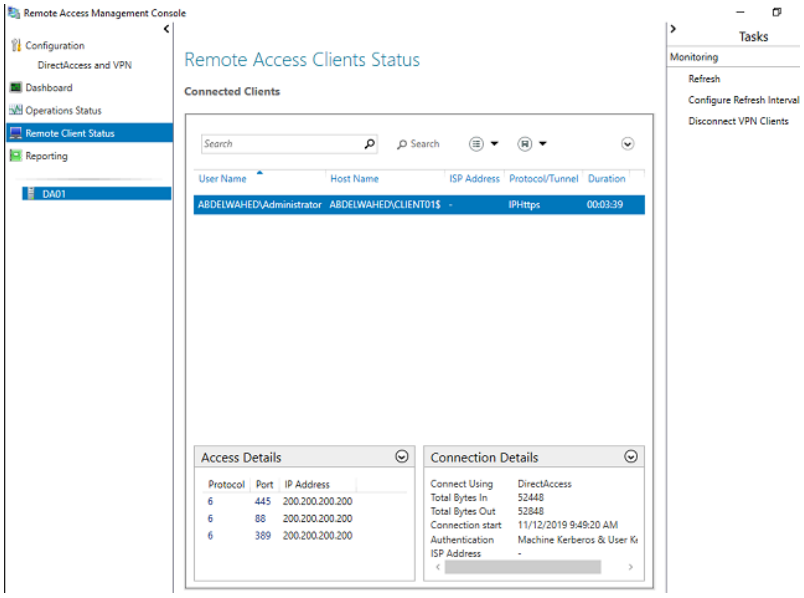


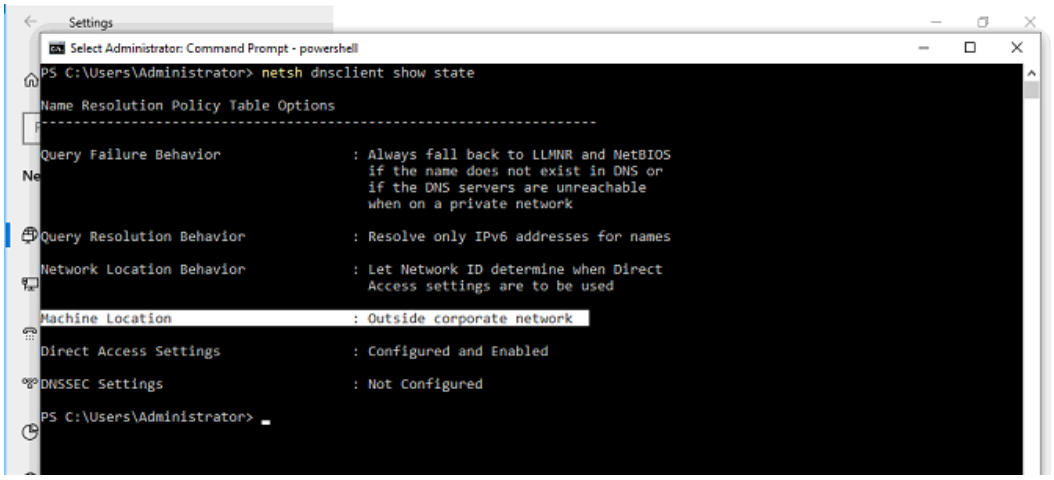
Execute gpupdate /force, then run Gpresult /r, and finally restart the computer once or twice.

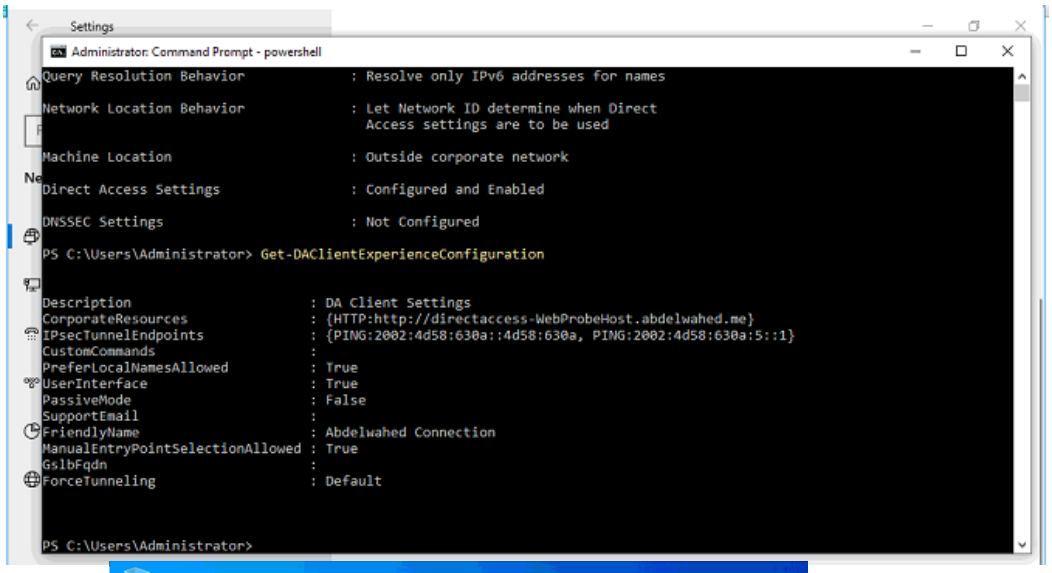


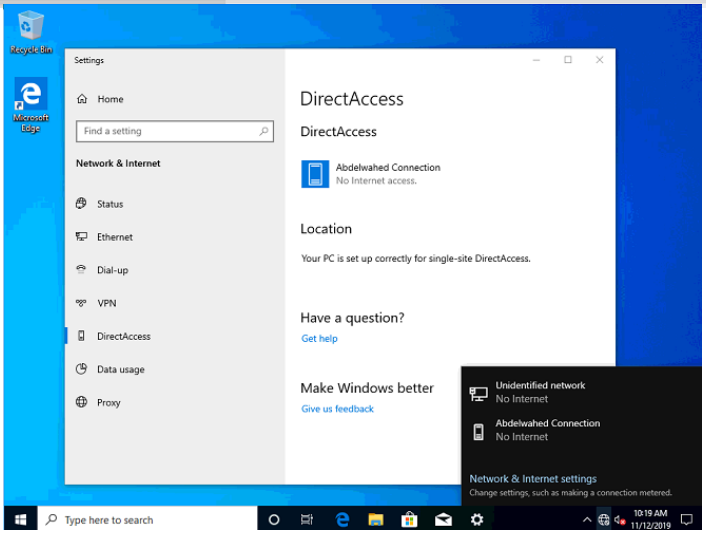
Next, turn off the LAN NIC and turn on the WAN to see if you can still reach the server resources.





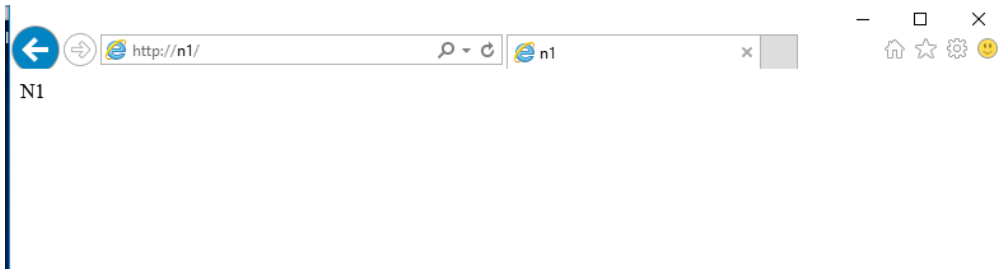

Settings
Select Administrator: Command Prompt - powershell
PS C:\Users\Administrator> netsh dnsclient show state
Name Resolution Policy Table Options
Query Failure Behavior : Always fall back to LLMNR and NetBIOS if the name does not exist in DNS or if the DNS servers are unreachable when on a private network
Query Resolution Behavior : Resolve only IPv6 addresses for names
Network Location Behavior : Let Network ID determine when Direct Access settings are to be used
Machine Location : Outside corporate network
Direct Access Settings : Configured and Enabled
DNSSEC Settings : Not Configured
PS C:\Users\Administrator>

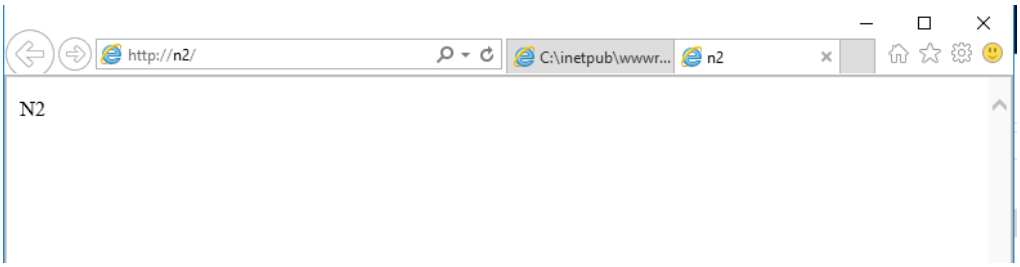

Settings
Administrator: Command Prompt - powershell
Query Resolution Behavior : Resolve only IPv6 addresses for names
Network Location Behavior : Let Network ID determine when Direct Access settings are to be used
Machine Location : Outside corporate network
Direct Access Settings : Configured and Enabled
DNSSEC Settings : Not Configured
PS C:\Users\Administrator> Get-DAClientExperienceConfiguration
Description : DA Client Settings
CorporateResources : {HTTP:http://directaccess-WebProbeHost.abdelwahed.me}
IPsecTunnelEndpoints : {PING:2002:4d58:630a::4d58:630a, PING:2002:4d58:630a:5::1}
CustomCommands :
PreferLocalNamesAllowed : True
UserInterface : True
PassiveMode : False
SupportEmail :
FriendlyName : Abdelwahed Connection
ManualEntryPointSelectionAllowed : True
GslbFqdn :
ForceTunneling : Default
PS C:\Users\Administrator>


Recycle Bin
Microsoft Edge
Settings
Home
Find a setting
Network & Internet
Status
Ethernet
Dial-up
VPN
DirectAccess
Data usage
Proxy
DirectAccess
DirectAccess
Abdelwahed Connection
No Internet access.
Location
Your PC is set up correctly for single-site DirectAccess.
Have a question?
Get help
Make Windows better
Give us feedback
Unidentified network
No Internet
Abdelwahed Connection
No Internet
Network & Internet settings
Change settings, such as making a connection metered.
Type here to search
10:19 AM
11/12/2019

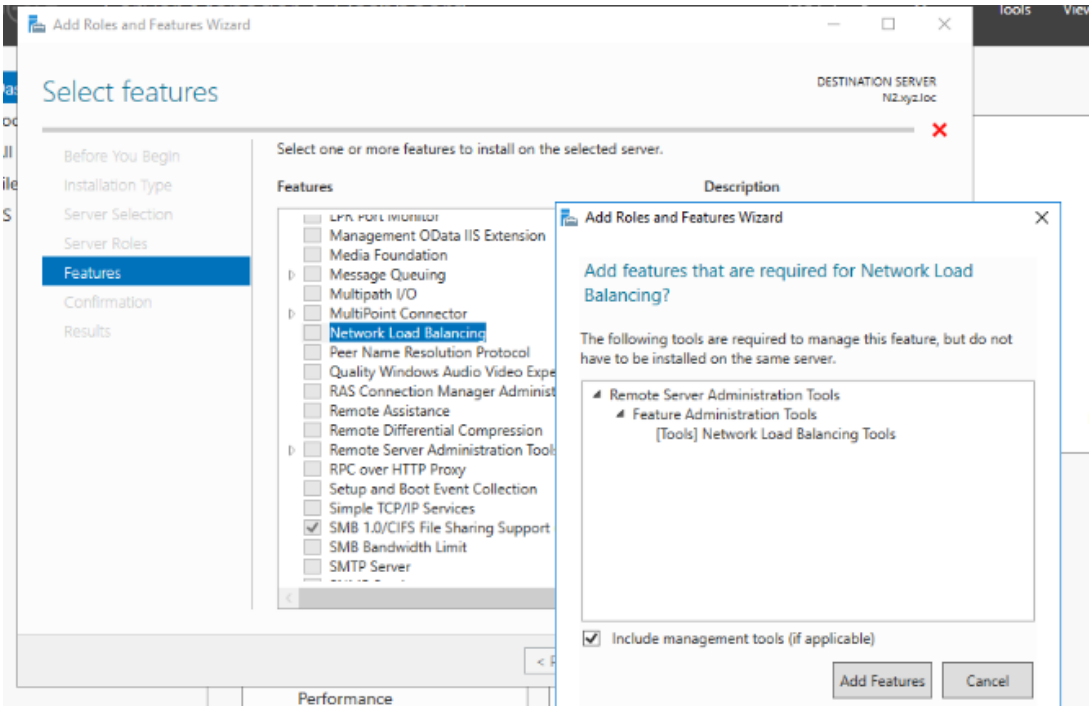
Network Load Balancer (Web Servers)

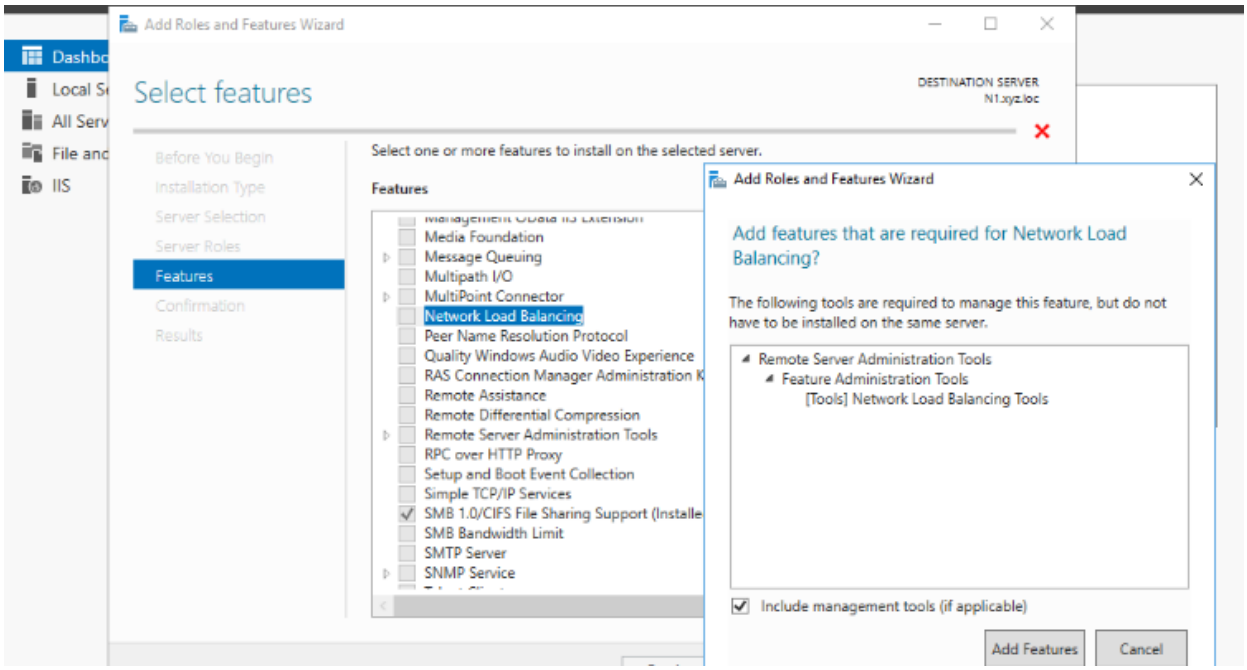
Initially, install IIS on both N1 and N2 servers.



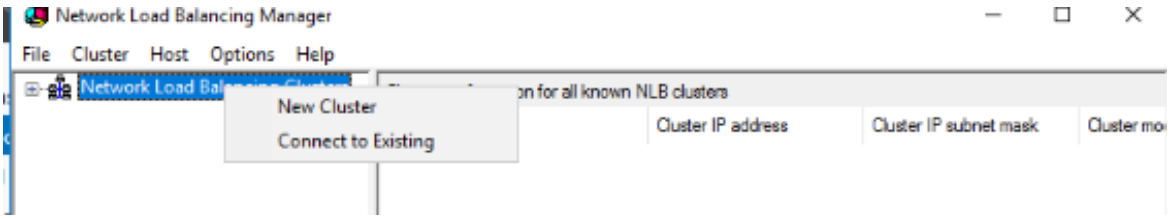


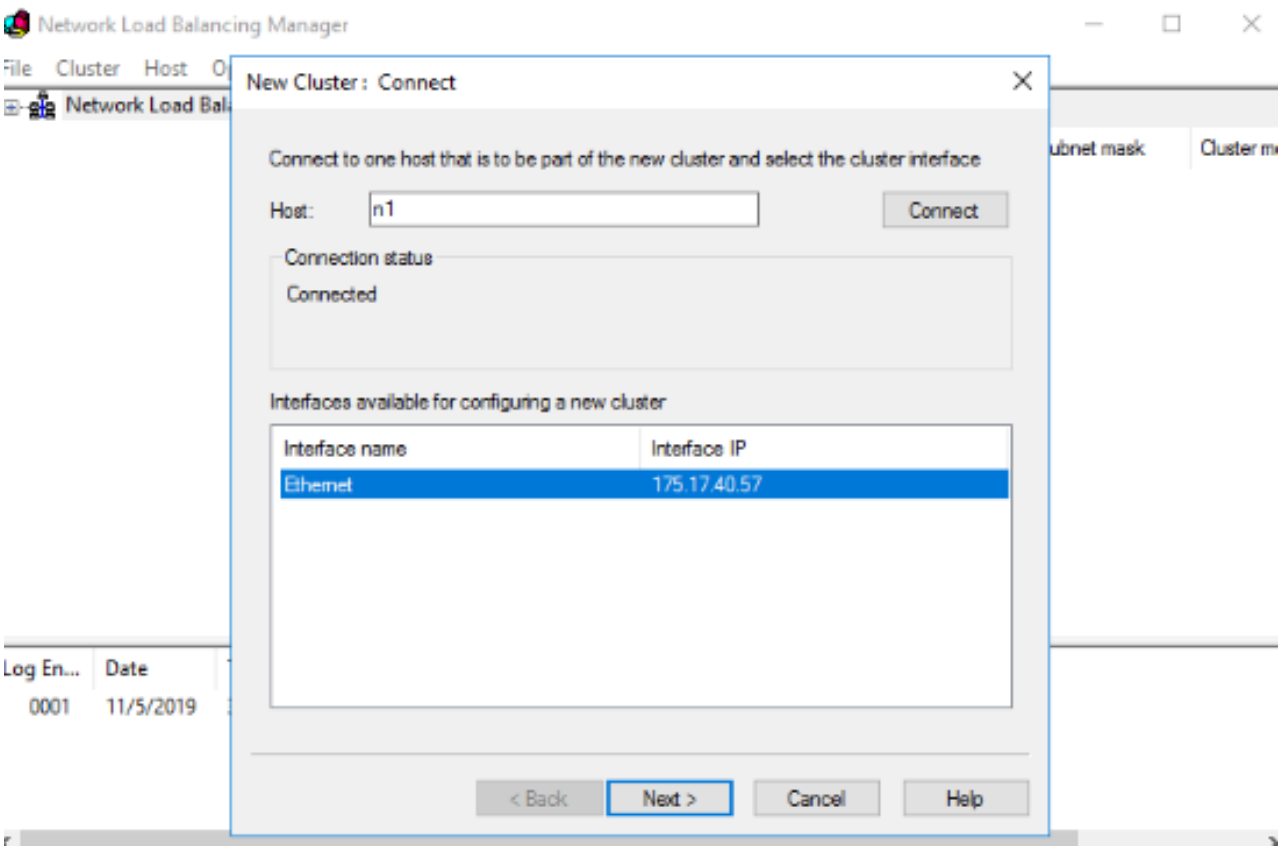
Please proceed to implement the network load balancing feature on both Load Balancer servers.

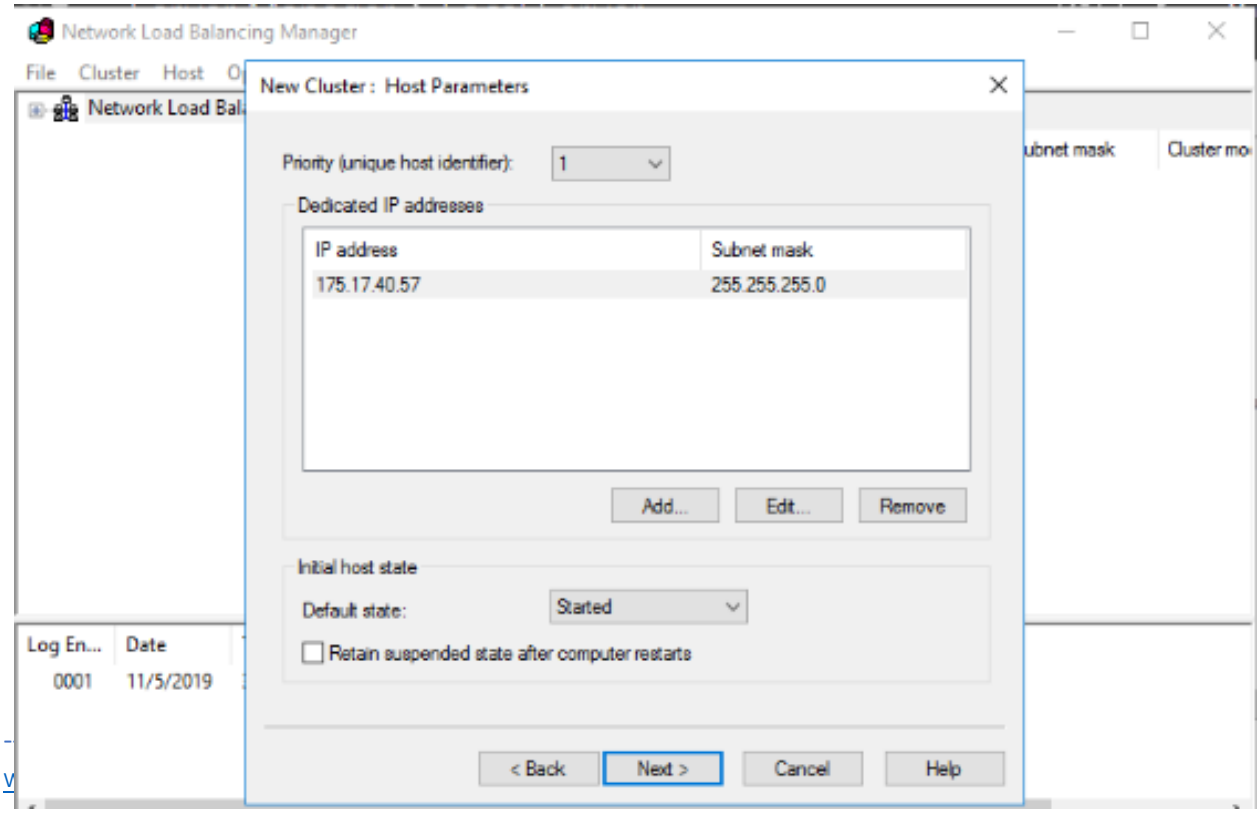


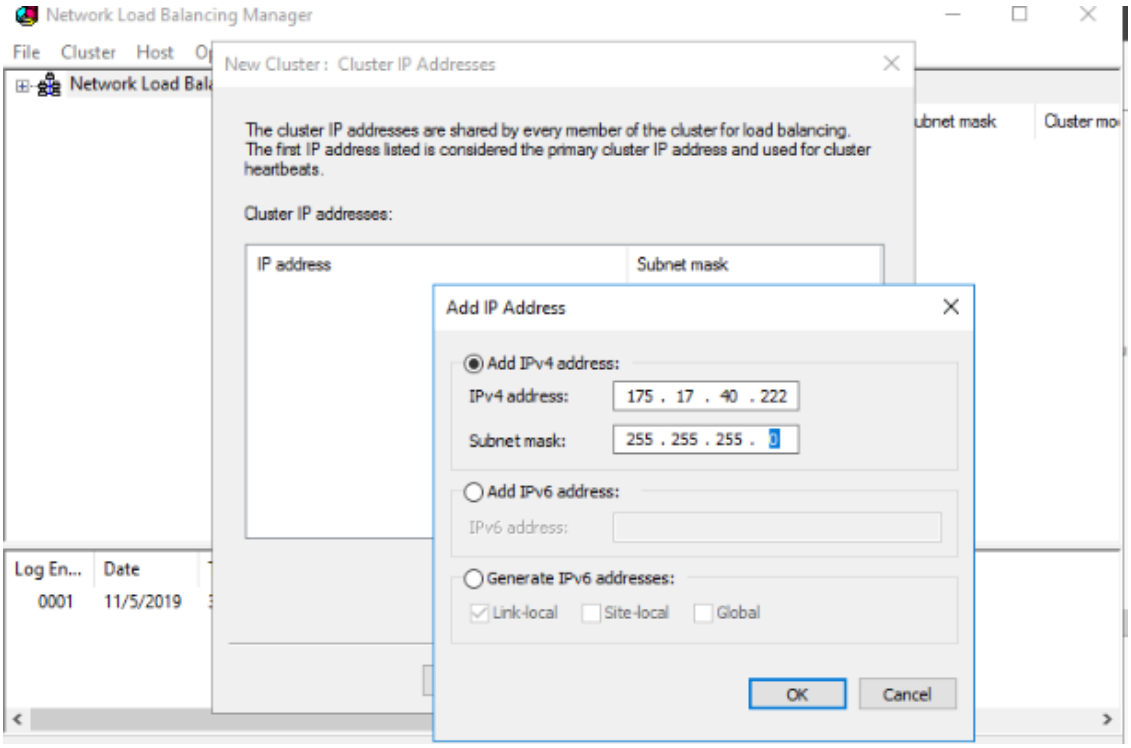


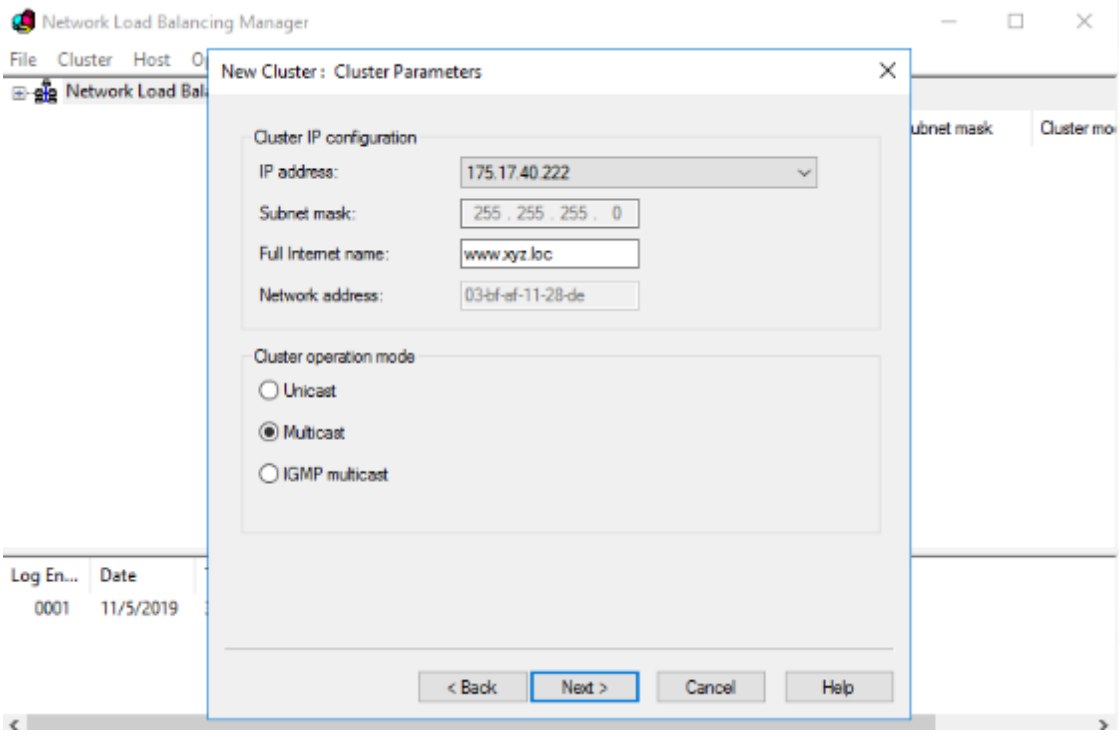
Launch a single NLB server and include the two servers.

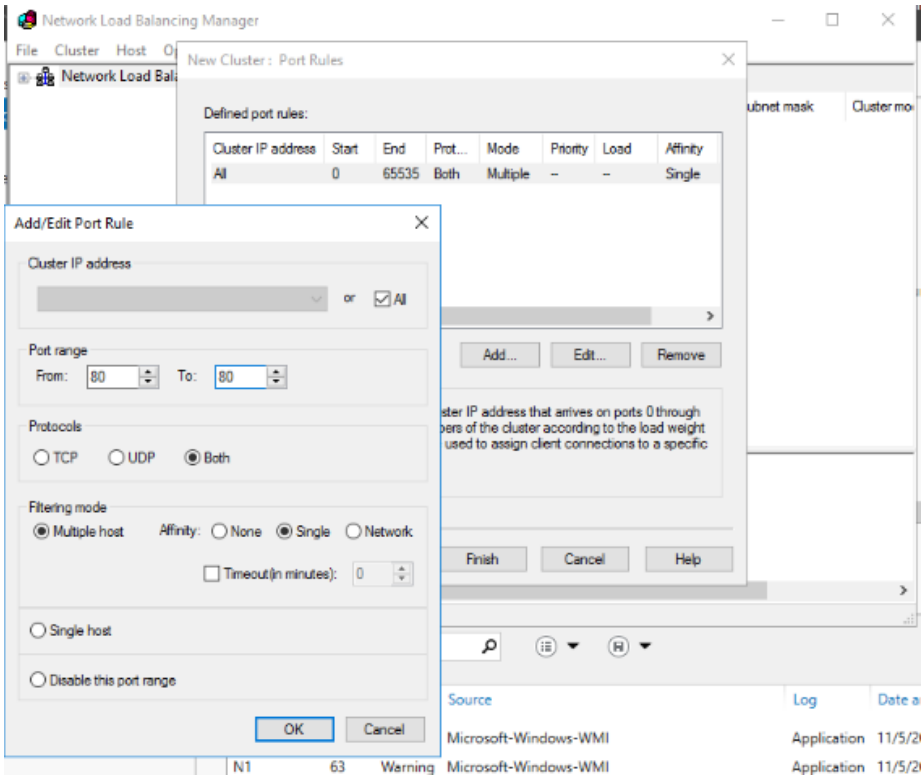



Network Load Balancing Manager
File Cluster Host O
Network Load Bal
New Cluster : Connect
Connect to one host that is to be part of the new cluster and select the cluster interface
Host:
n1
Connect
Connection status
Connected
Interfaces available for configuring a new cluster
Interface name
Interface IP
Ethernet
175.17.40.57
< Back
Next >
Cancel
Help
Log En...
Date
0001
11/5/2019

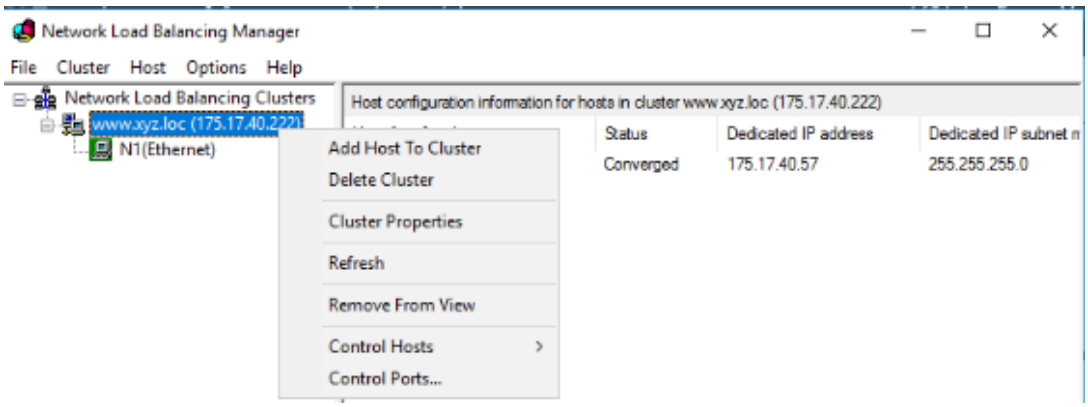

Network Load Balancing Manager
File Cluster Host O
Network Load Bal
New Cluster : Host Parameters
Priority (unique host identifier):
1
Dedicated IP addresses
IP address
Subnet mask
175.17.40.57
255.255.255.0
Add...
Edit...
Remove
Initial host state
Default state:
Started
Retain suspended state after computer restarts
< Back
Next >
Cancel
Help
Log En...
Date
0001
11/5/2019

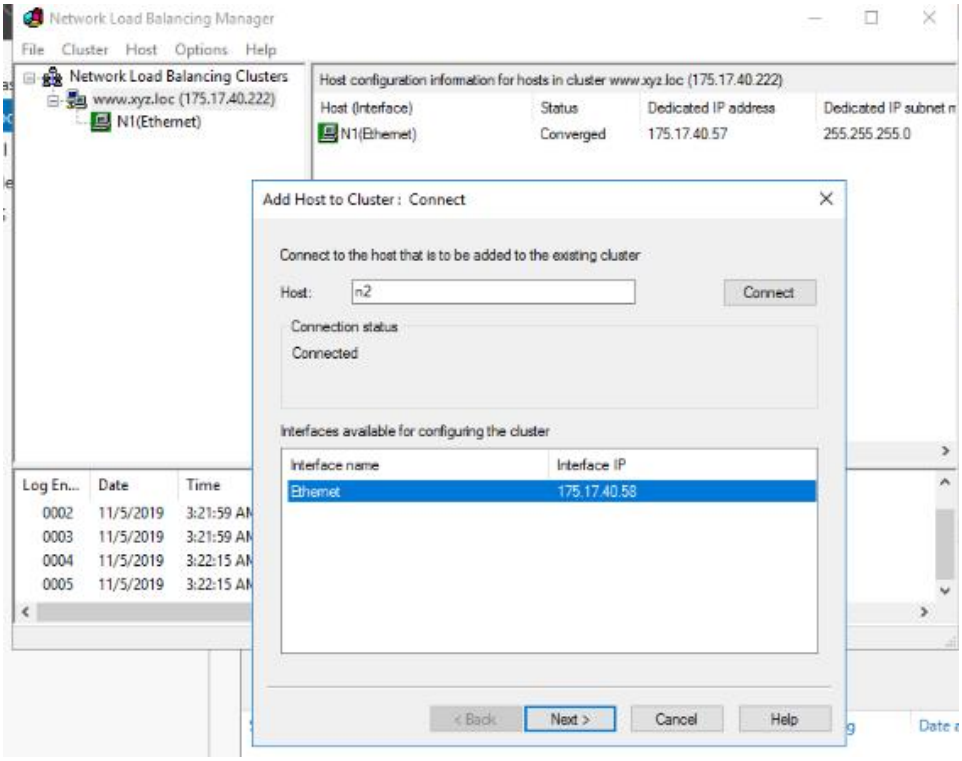

Network Load Balancing Manager
File Cluster Host
New Cluster : Cluster IP Addresses
The cluster IP addresses are shared by every member of the cluster for load balancing. The first IP address listed is considered the primary cluster IP address and used for cluster heartbeats.
Cluster IP addresses:
IP address
Subnet mask
Add IP Address
Add IPv4 address:
IPv4 address: 175 . 17 . 40 . 222
Subnet mask: 255 . 255 . 255 . 0
Add IPv6 address:
IPv6 address:
Generate IPv6 addresses:
Link-local Site-local Global
OK Cancel
Log En... Date
0001 11/5/2019

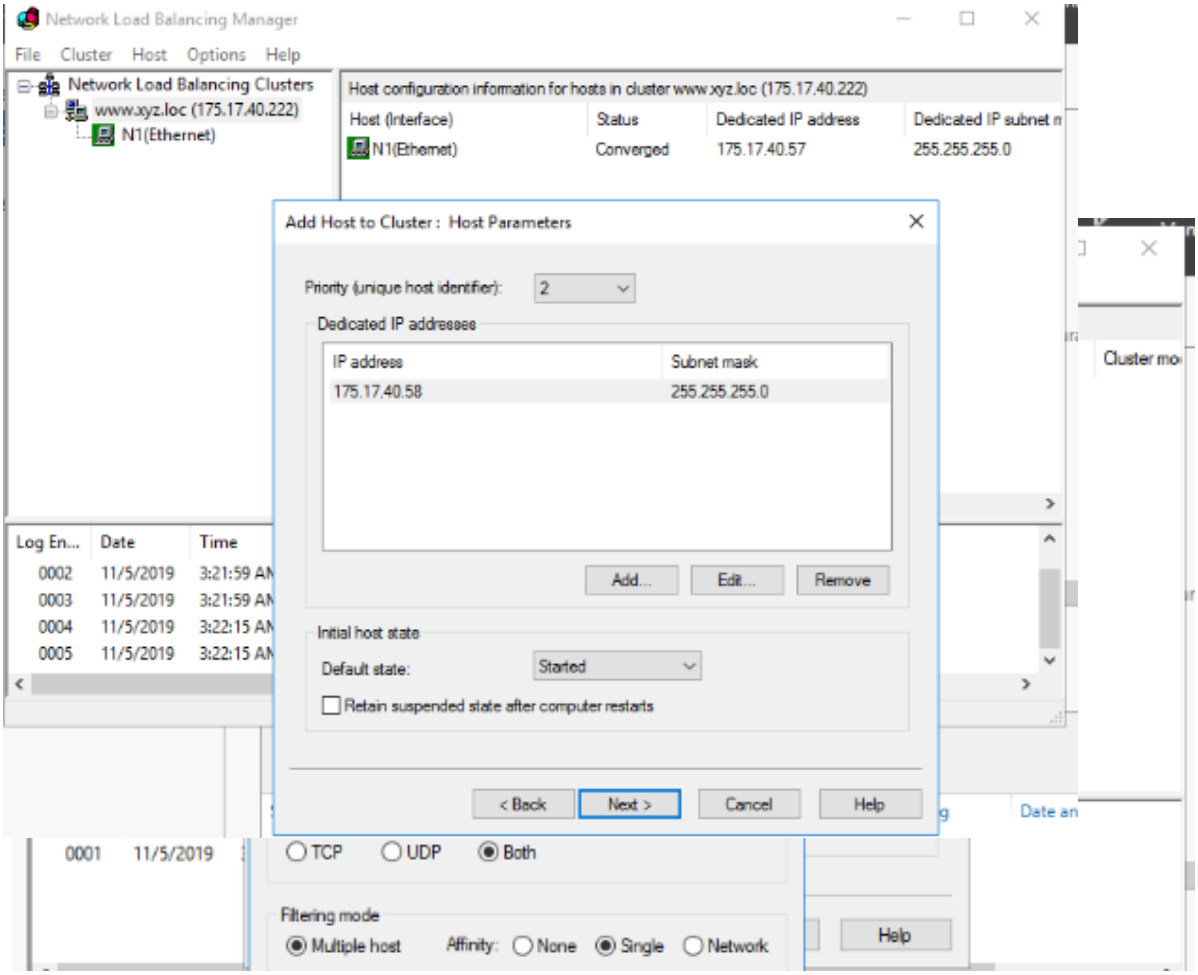

Network Load Balancing Manager
File Cluster Host
New Cluster : Cluster Parameters
Cluster IP configuration
IP address: 175.17.40.222
Subnet mask: 255 . 255 . 255 . 0
Full Internet name: www.xyz.loc
Network address: 03-bf-af-11-28-de
Cluster operation mode
Unicast
Multicast
IGMP multicast
< Back Next > Cancel Help
Log En... Date
0001 11/5/2019

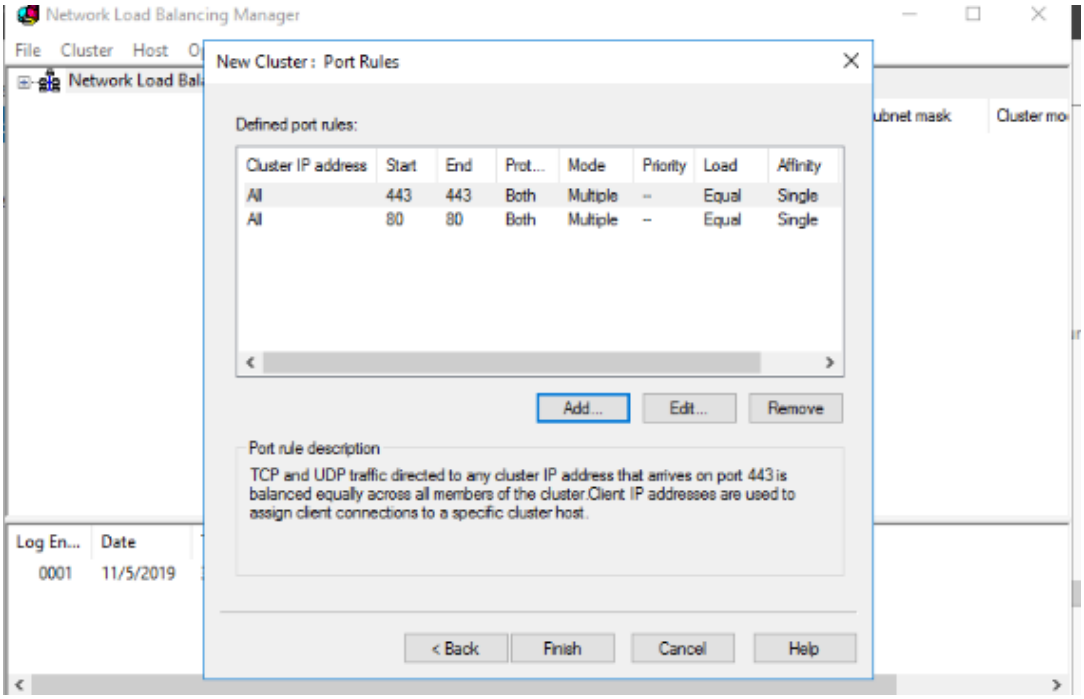


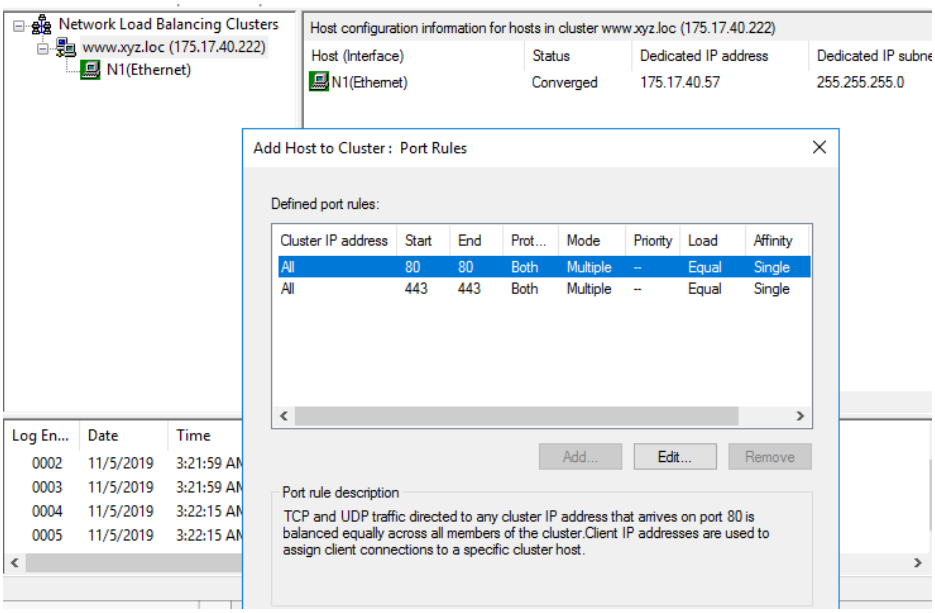
Include an additional N2 host in the cluster.



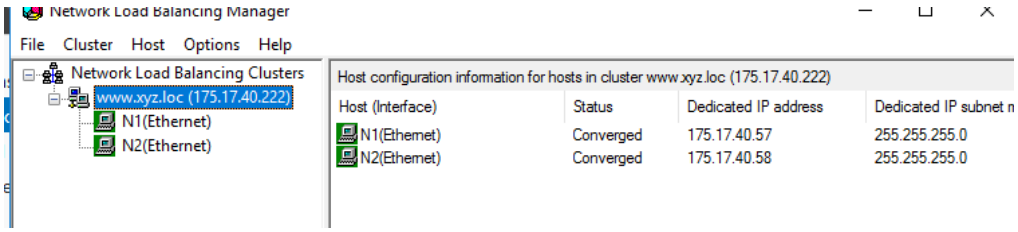

Network Load Balancing Manager
File Cluster Host Options Help
Network Load Balancing Clusters
www.xyz.loc (175.17.40.222)
N1(Ethernet)
Host configuration information for hosts in cluster www.xyz.loc (175.17.40.222)
Host (Interface)
Status
Dedicated IP address
Dedicated IP subnet m
N1(Ethernet)
Converged
175.17.40.57
255.255.255.0
Add Host to Cluster : Connect
Connect to the host that is to be added to the existing cluster
Host:
n2
Connect
Connection status
Connected
Interfaces available for configuring the cluster
Interface name
Interface IP
Ethernet
175.17.40.58
Log En...
Date
Time
0002 11/5/2019 3:21:59 AM
0003 11/5/2019 3:21:59 AM
0004 11/5/2019 3:22:15 AM
0005 11/5/2019 3:22:15 AM
< Back
Next >
Cancel
Help


Network Load Balancing Manager
File Cluster Host Options Help
Network Load Balancing Clusters
www.xyz.loc (175.17.40.222)
N1(Ethernet)
Host configuration information for hosts in cluster www.xyz.loc (175.17.40.222)
Host (Interface)
Status
Dedicated IP address
Dedicated IP subnet m
N1(Ethernet)
Converged
175.17.40.57
255.255.255.0
Add Host to Cluster : Host Parameters
Priority (unique host identifier):
2
Dedicated IP addresses
IP address
Subnet mask
175.17.40.58
255.255.255.0
Add...
Edit...
Remove
Initial host state
Default state:
Started
Retain suspended state after computer restarts
< Back
Next >
Cancel
Help
Log En...
Date
Time
0002 11/5/2019
0003 11/5/2019
0004 11/5/2019
0005 11/5/2019
0001 11/5/2019
TCP
UDP
Both
Filtering mode
Multiple host
Affinity:
None
Single
Network
Help

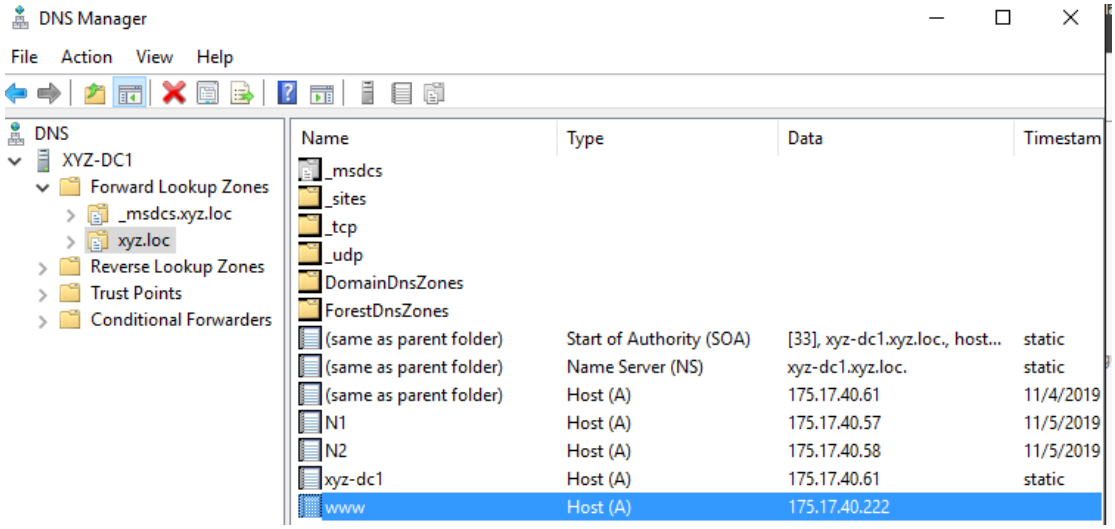




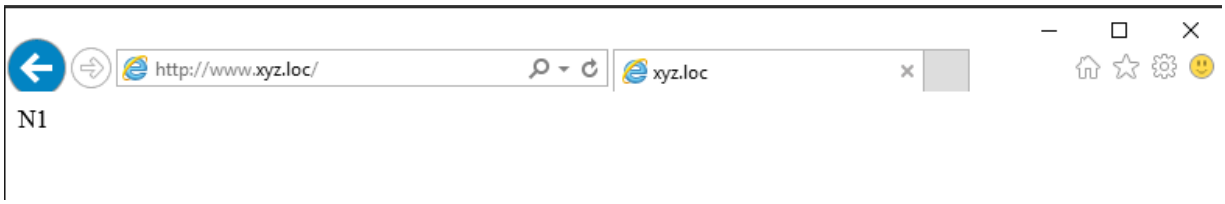
Both servers are now included in the same cluster.



Verify the IPV4 settings on both servers, and you will notice the cluster IP 175.17.40.222 has been assigned as a secondary IP to each server. And add DNS A record for cluster.



Check the connectivity to www.xyz.loc from a different computer (originating from N1).



To test, unplug N1 and attempt to reconnect (your access will be through N2).

Failover Cluster with File Server

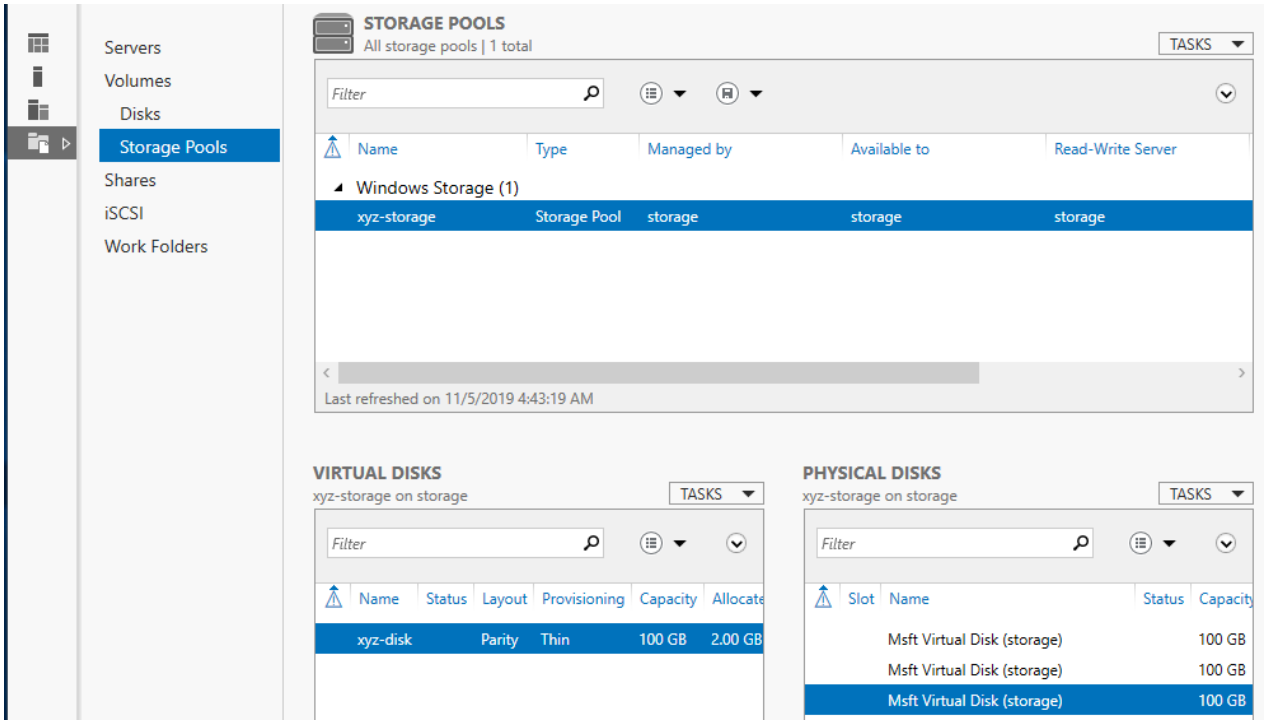
Requirements

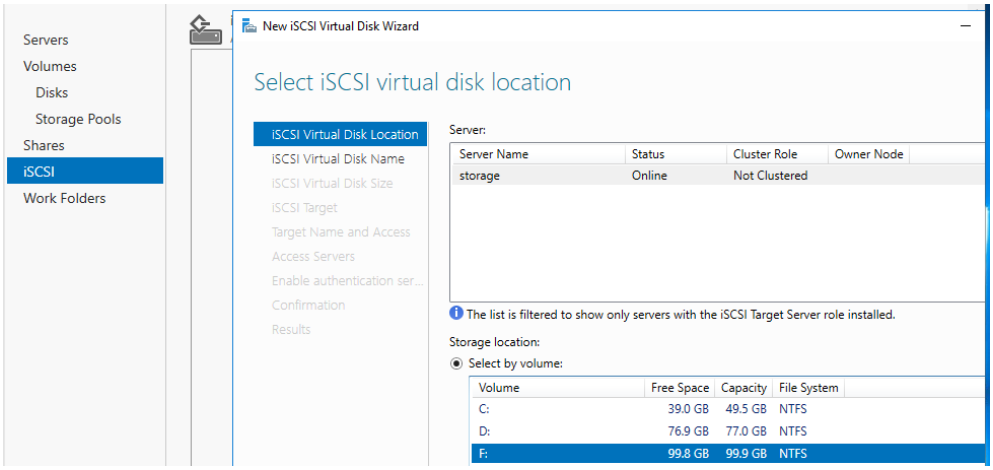
1- Configure Default Gateway for all servers
2- Carete 2 ISCSI Disk (one for Data and another for Quorum) and connect them to both Failover cluster nodes
3- Install file server role to both nodes
4- Install Failover cluster to both nodes
5- In case of file server availability add both nodes to the same cluster

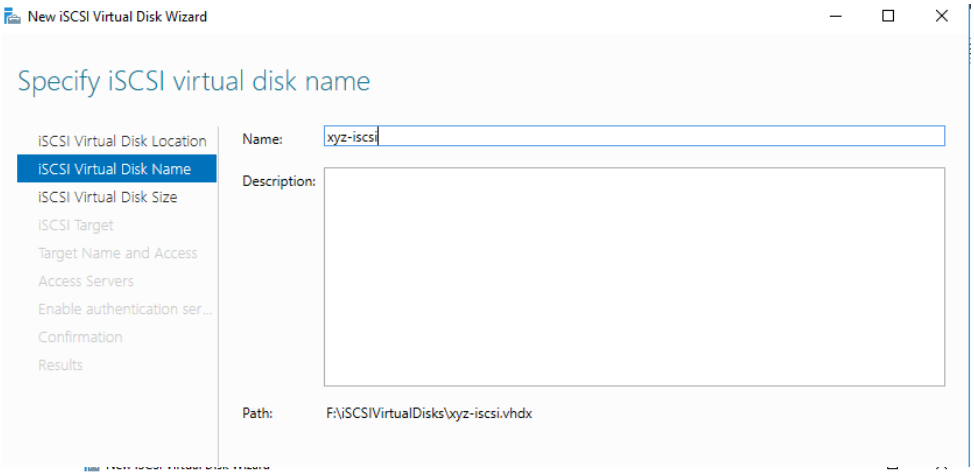
Current environment

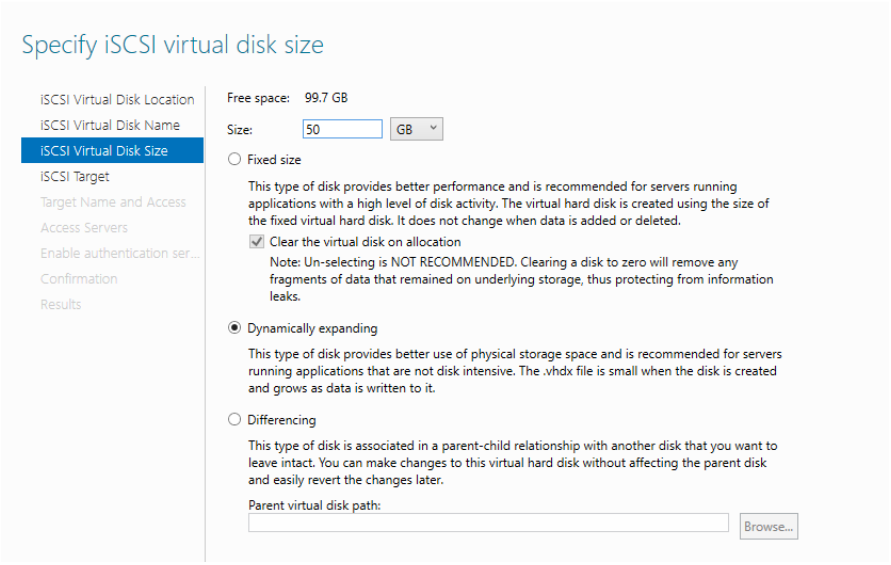
- Domain: xyz.com
- Storage server: storage.xyz.com
- Failover cluster node: F1 and F2 servers joined to xyz.com

Cerate 2 ISCSI Disk (one for Data and another for Quorum) and connect them to both Failover cluster nodes

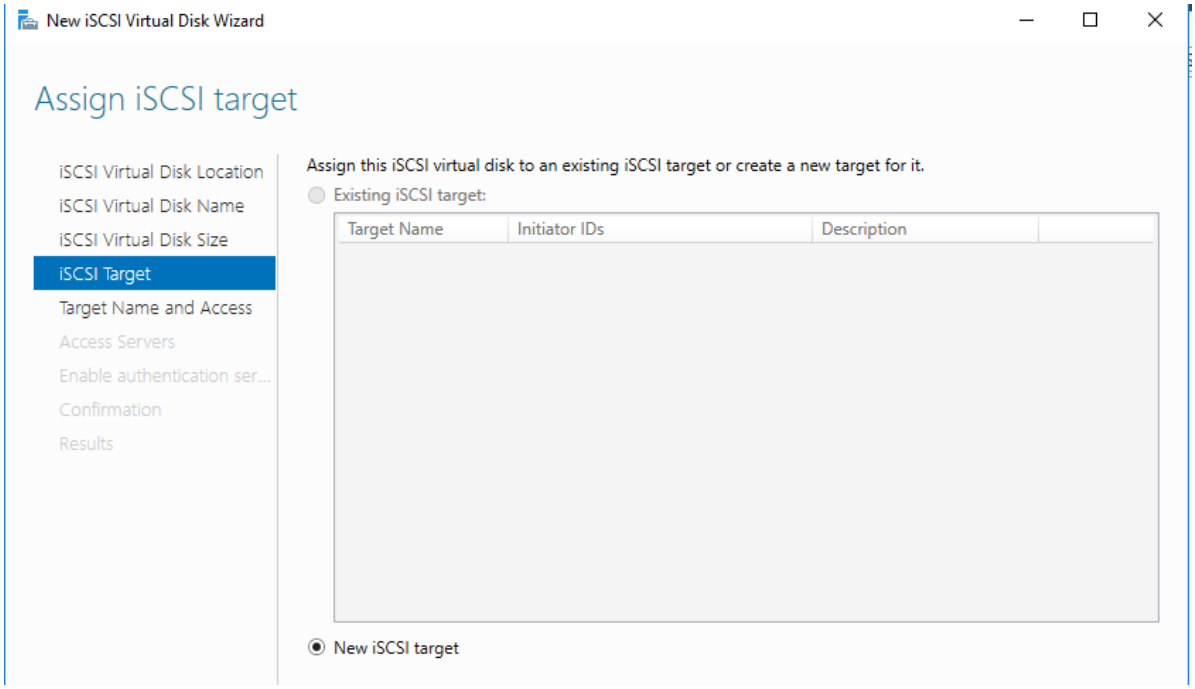


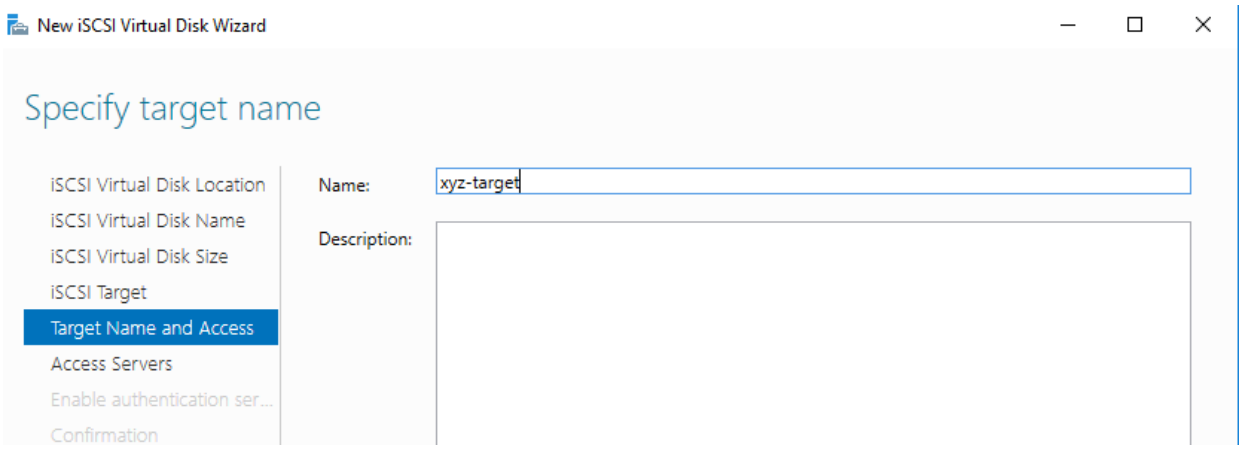

Servers
Volumes
Disks
Storage Pools
Shares
iSCSI
Work Folders
New iSCSI Virtual Disk Wizard
Select iSCSI virtual disk location
iSCSI Virtual Disk Location
iSCSI Virtual Disk Name
iSCSI Virtual Disk Size
iSCSI Target
Target Name and Access
Access Servers
Enable authentication ser...
Confirmation
Results
Server:
Server Name
Status
Cluster Role
Owner Node
storage
Online
Not Clustered
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:
39.0 GB
49.5 GB
NTFS
D:
76.9 GB
77.0 GB
NTFS
F:
99.8 GB
99.9 GB
NTFS

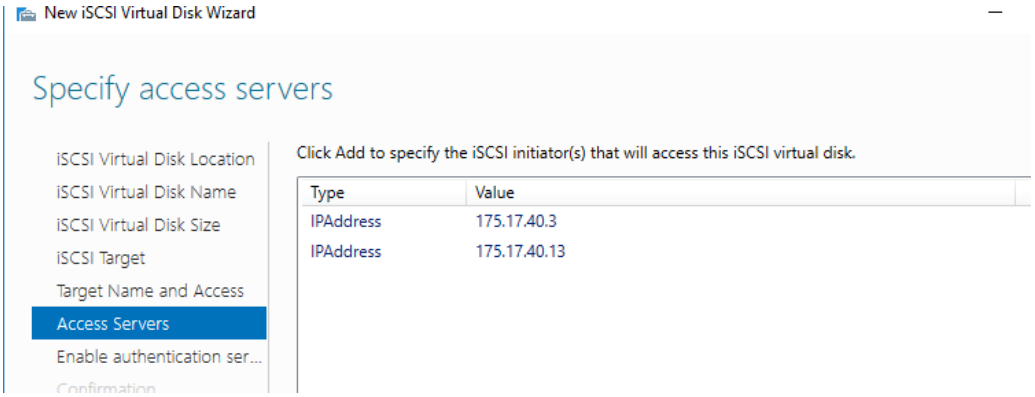

New iSCSI Virtual Disk Wizard
Specify iSCSI virtual disk name
iSCSI Virtual Disk Location
iSCSI Virtual Disk Name
iSCSI Virtual Disk Size
iSCSI Target
Target Name and Access
Access Servers
Enable authentication ser...
Confirmation
Results
Name:
xyz-iscsi
Description:
Path:
F:\iSCSIVirtualDisks\xyz-iscsi.vhdx

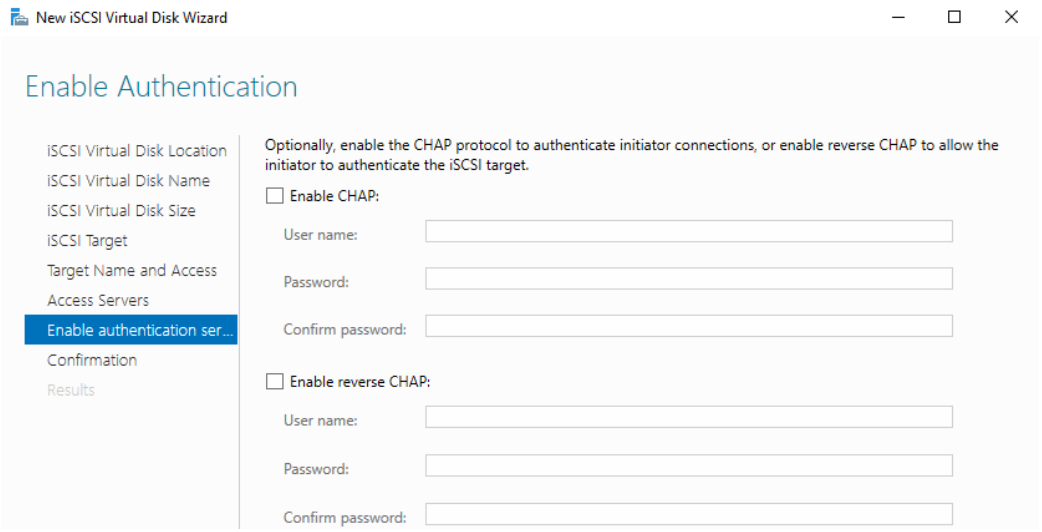

Specify iSCSI virtual disk size
iSCSI Virtual Disk Location
iSCSI Virtual Disk Name
iSCSI Virtual Disk Size
iSCSI Target
Target Name and Access
Access Servers
Enable authentication ser...
Confirmation
Results
Free space: 99.7 GB
Size:
50
GB
Fixed size
This type of disk provides better performance and 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:
Browse...

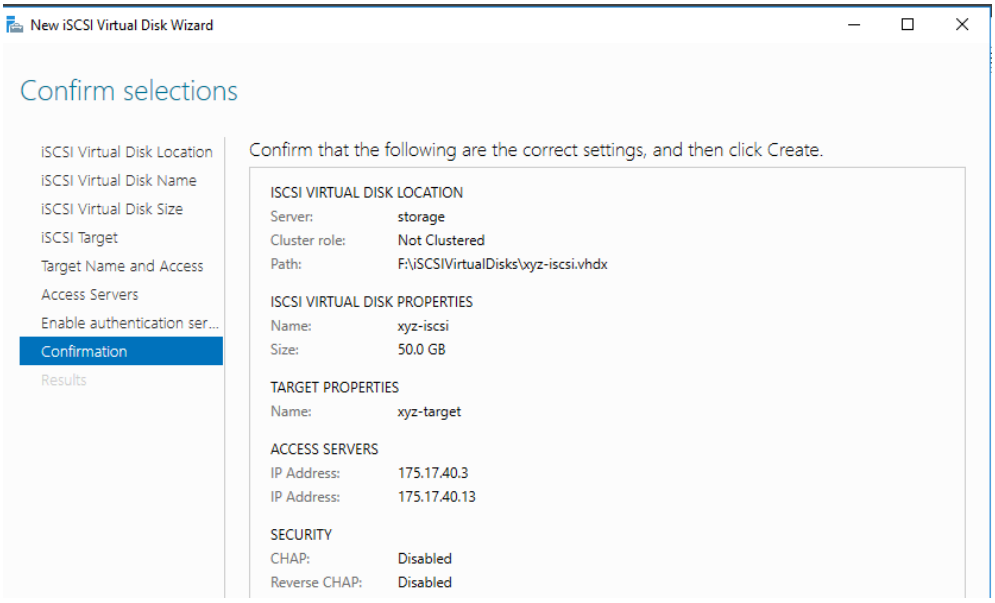
Configure the two failover nodes to function as iSCSI initiators.

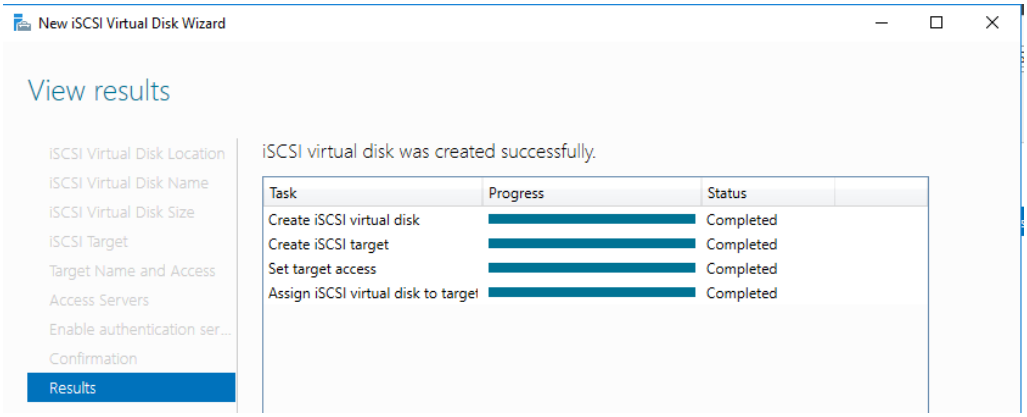




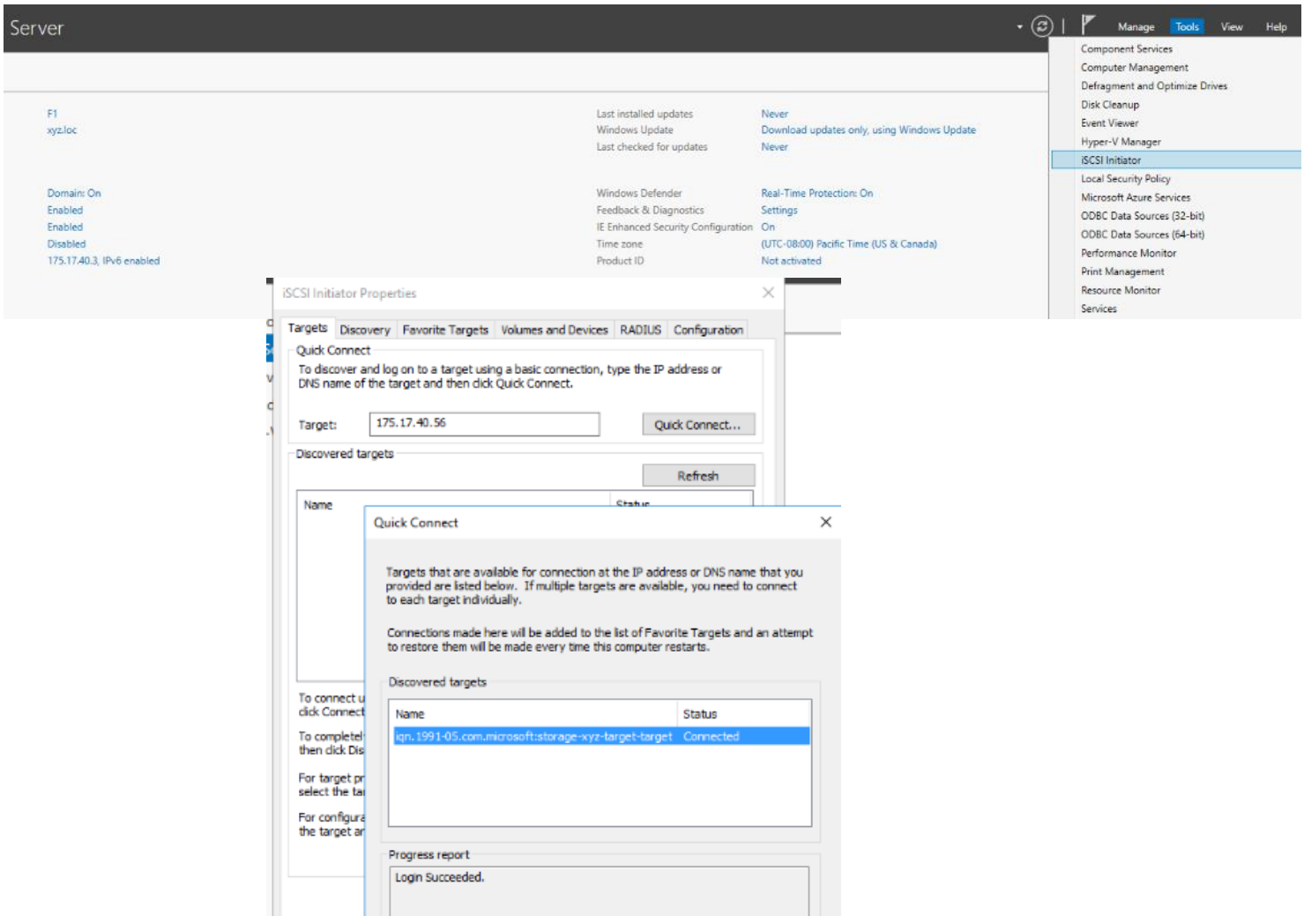

New iSCSI Virtual Disk Wizard
Specify access servers
iSCSI Virtual Disk Location
iSCSI Virtual Disk Name
iSCSI Virtual Disk Size
iSCSI Target
Target Name and Access
Access Servers
Enable authentication ser...
Click Add to specify the iSCSI initiator(s) that will access this iSCSI virtual disk.
Type
Value
IPAddress
175.17.40.3
IPAddress
175.17.40.13


New iSCSI Virtual Disk Wizard
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:

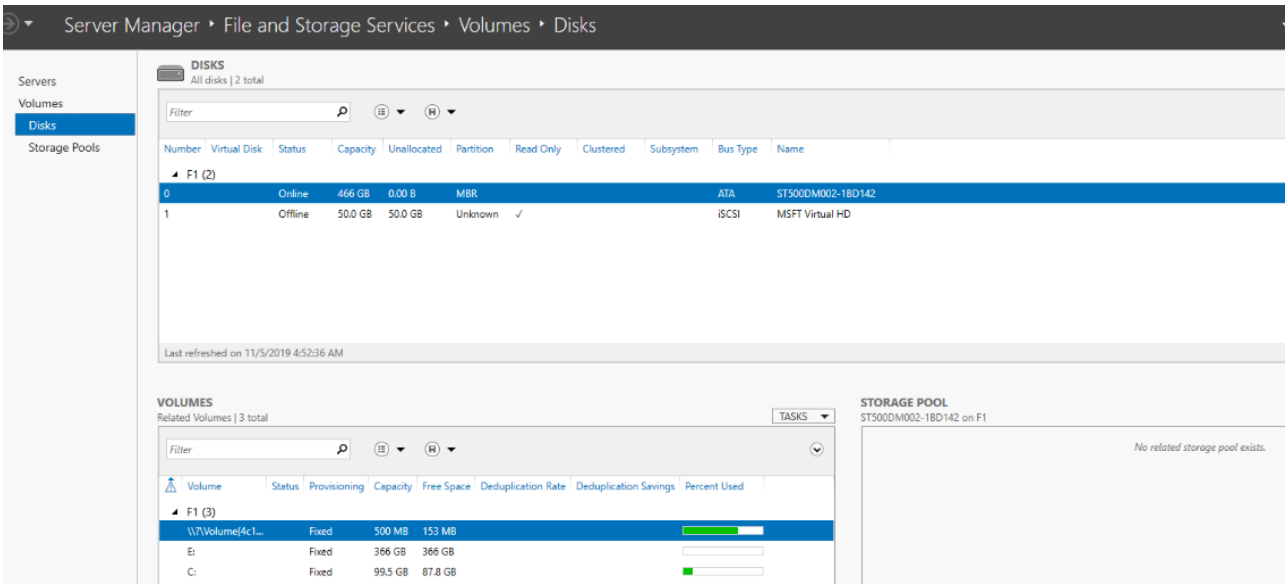

New iSCSI Virtual Disk Wizard
Confirm selections
iSCSI Virtual Disk Location
iSCSI Virtual Disk Name
iSCSI Virtual Disk Size
iSCSI Target
Target Name and Access
Access Servers
Enable authentication ser...
Confirmation
Results
Confirm that the following are the correct settings, and then click Create.
ISCSI VIRTUAL DISK LOCATION
Server: storage
Cluster role: Not Clustered
Path: F:\iSCSIVirtualDisks\xyz-iscsi.vhdx
ISCSI VIRTUAL DISK PROPERTIES
Name: xyz-iscsi
Size: 50.0 GB
TARGET PROPERTIES
Name: xyz-target
ACCESS SERVERS
IP Address: 175.17.40.3
IP Address: 175.17.40.13
SECURITY
CHAP: Disabled
Reverse CHAP: Disabled

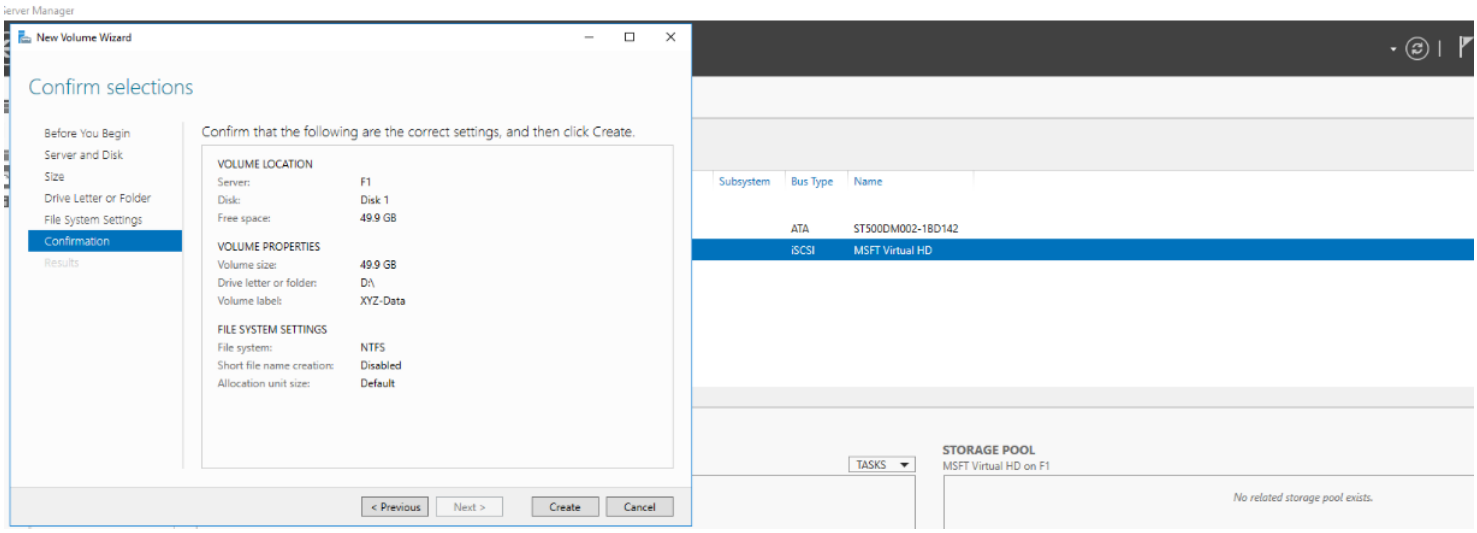


attach the isici target disk to each of the nodes.

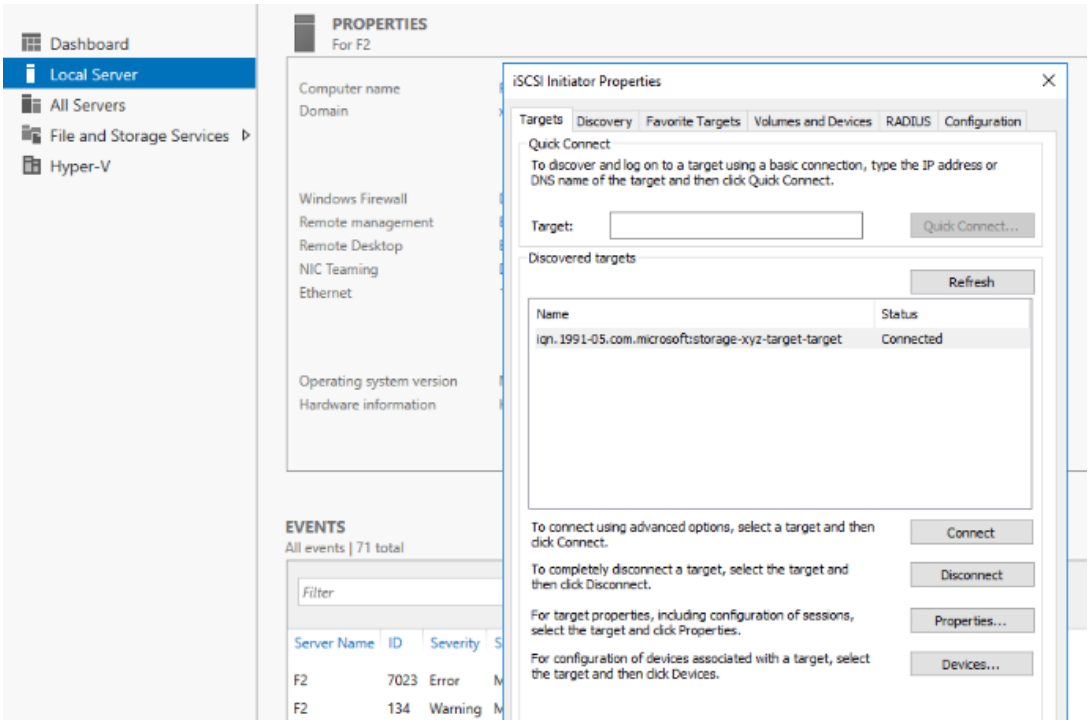


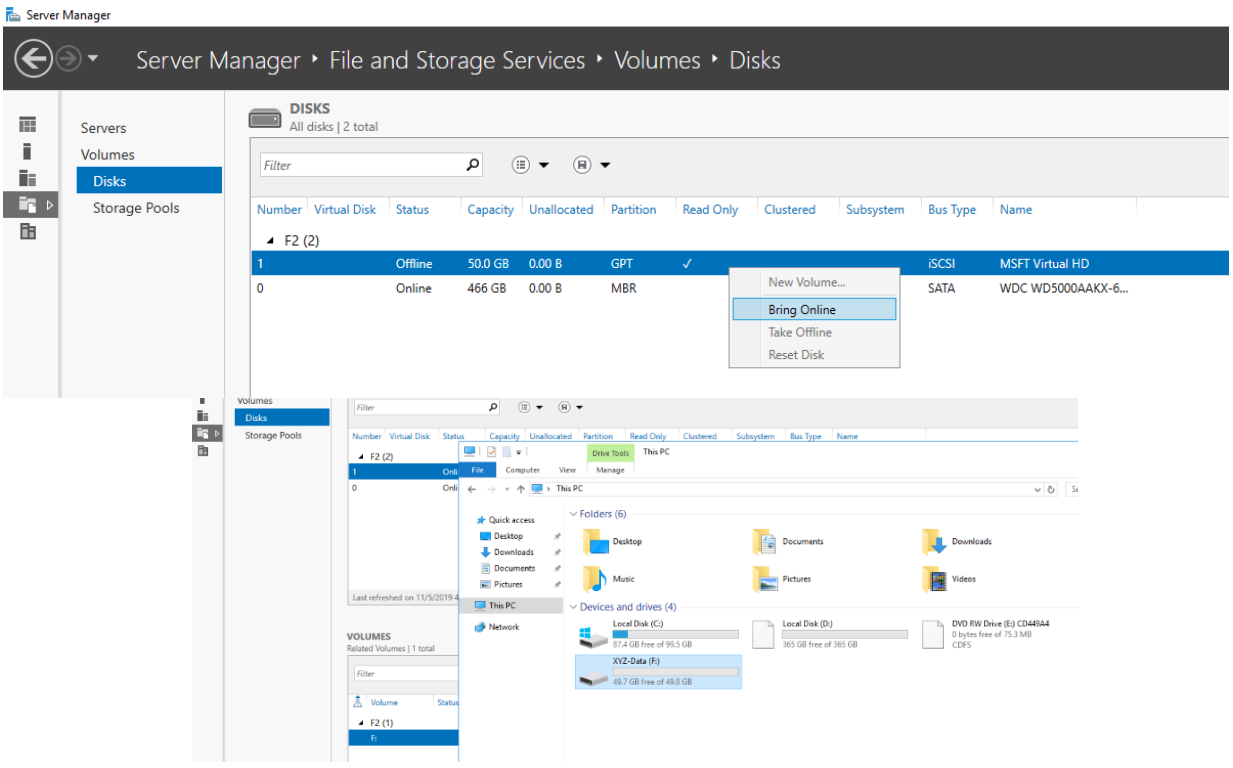
Bring the disk online and configure it





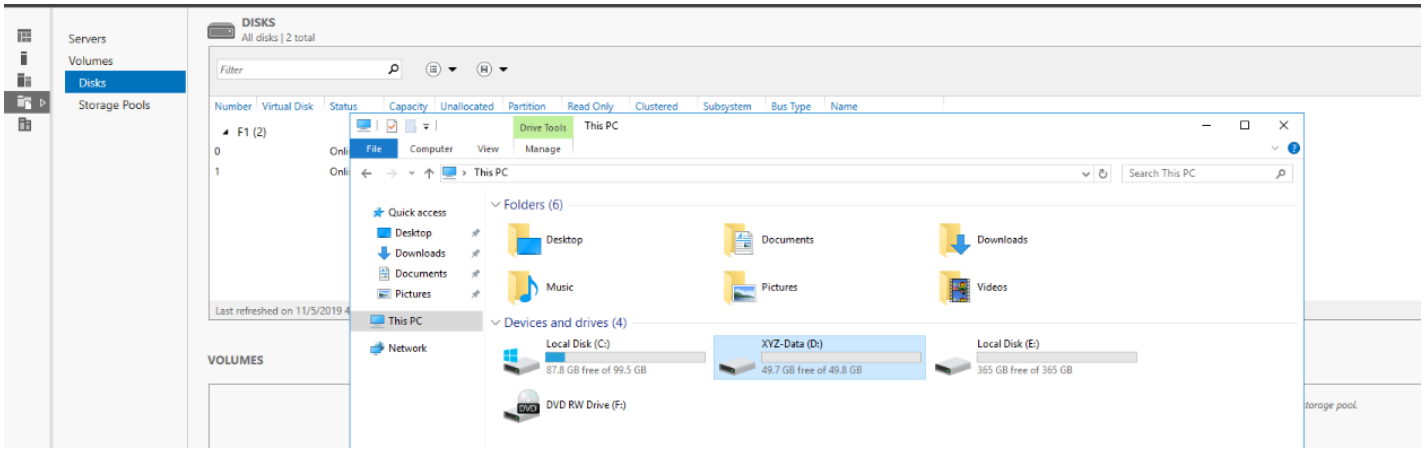
Now simply link the issci target from a separate node (there's no need for reformatting, just bring it online).



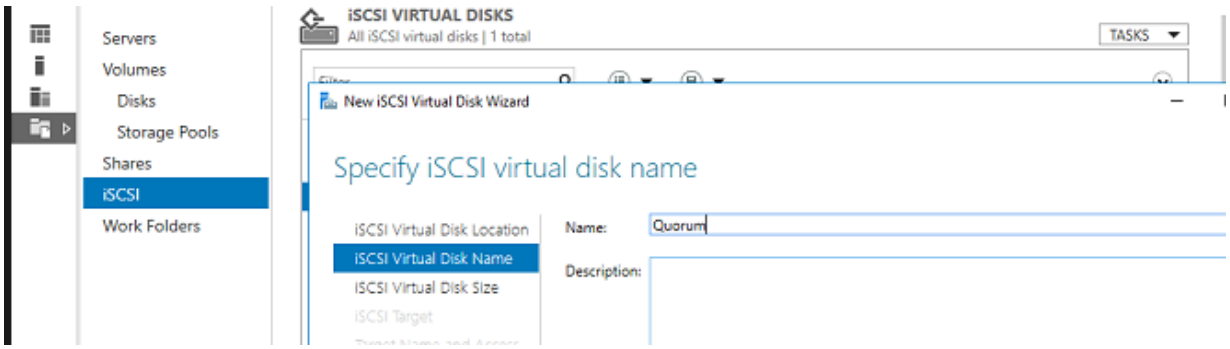


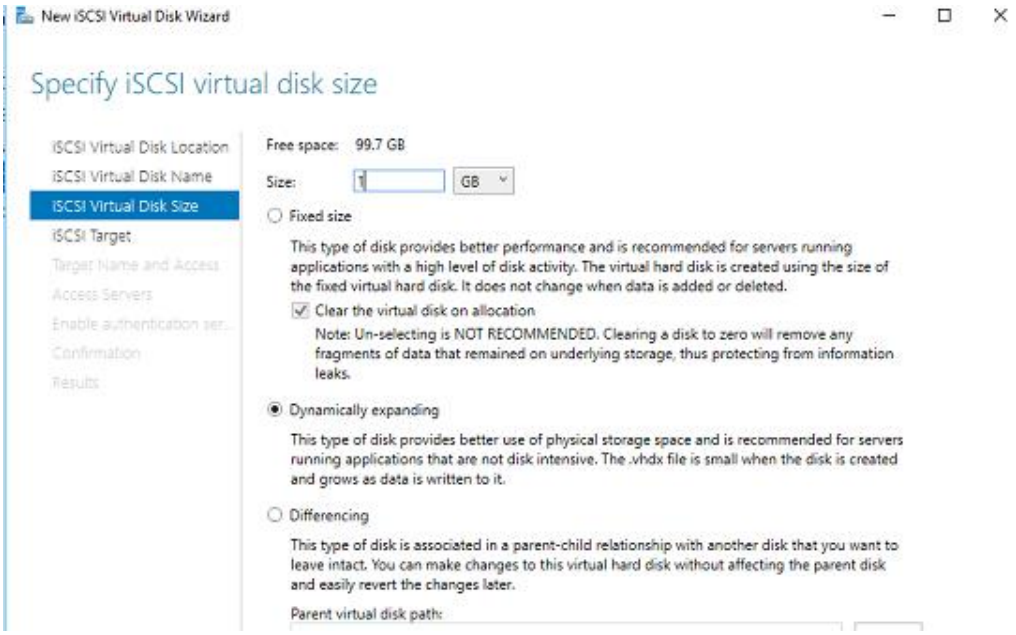
---

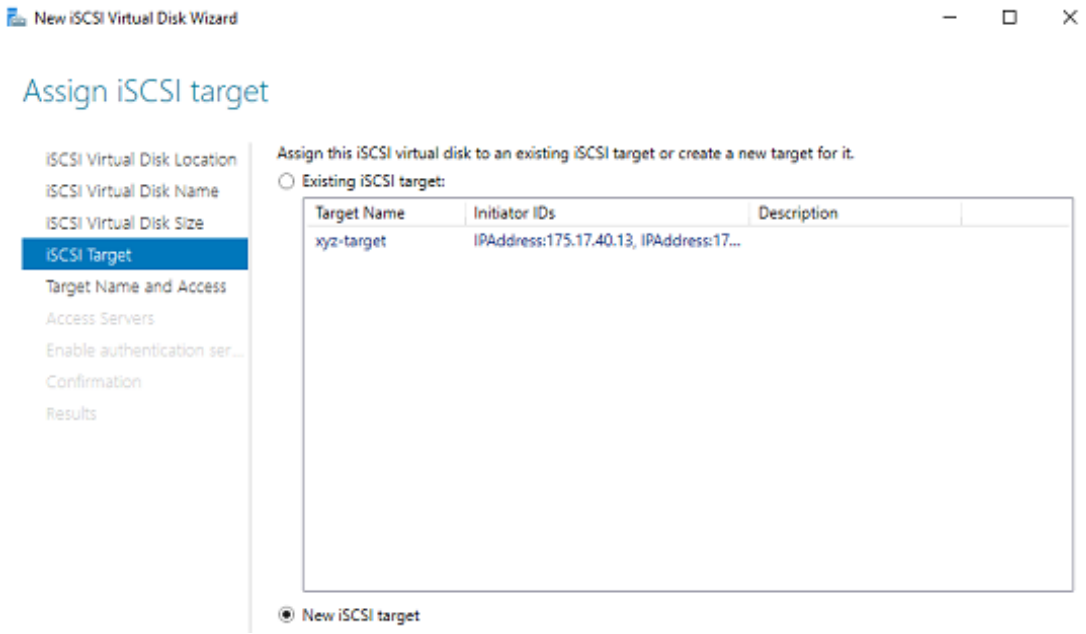
www.abdelwahed.me

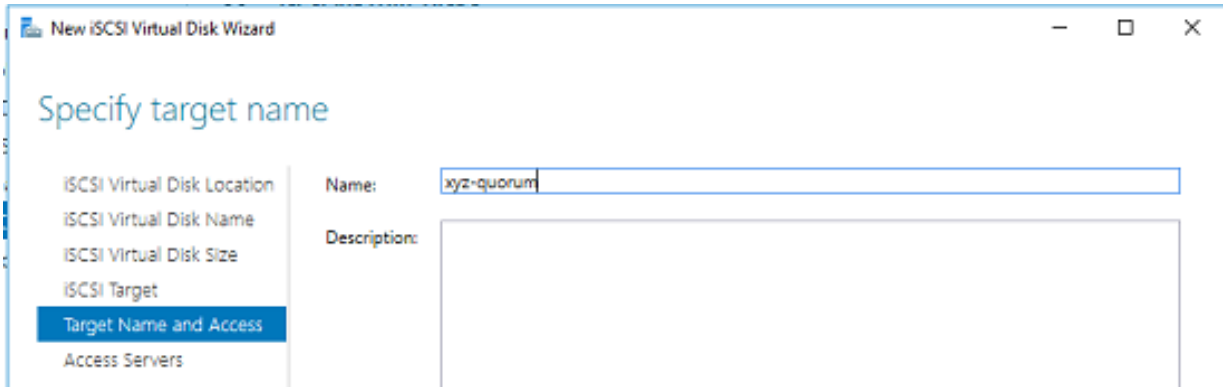


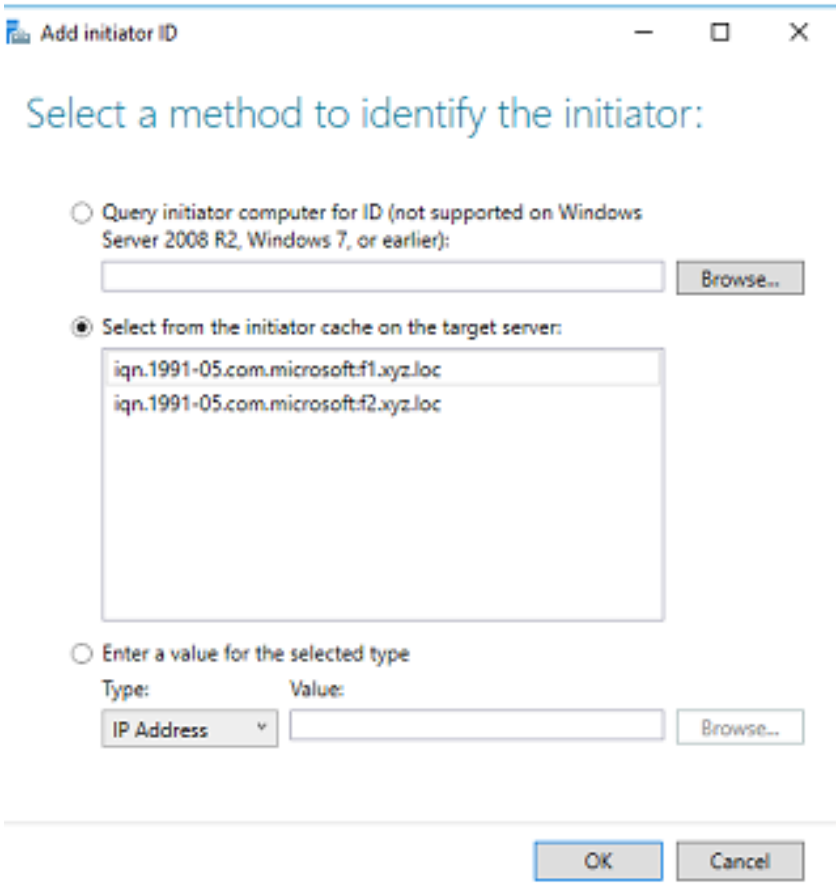
Incorporate an additional quorum disk as an iSCSI target on the storage server.

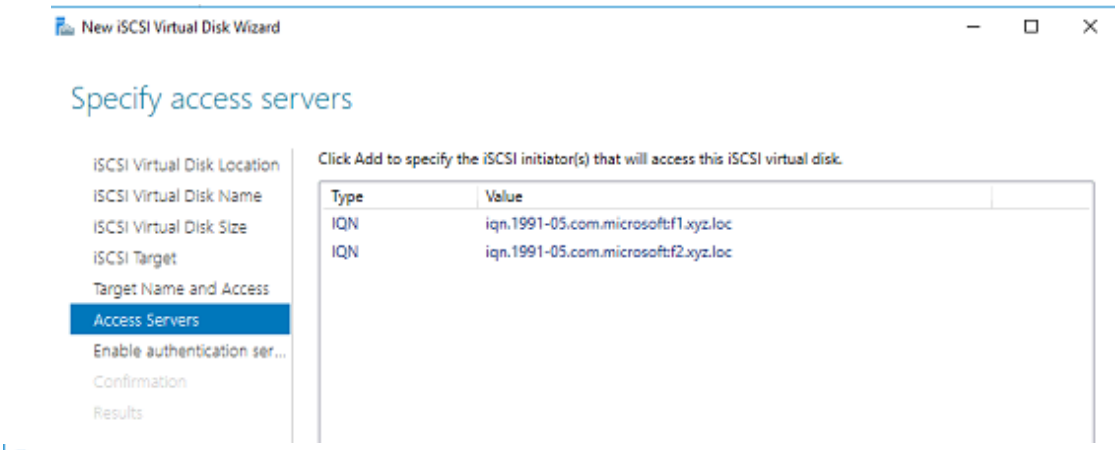


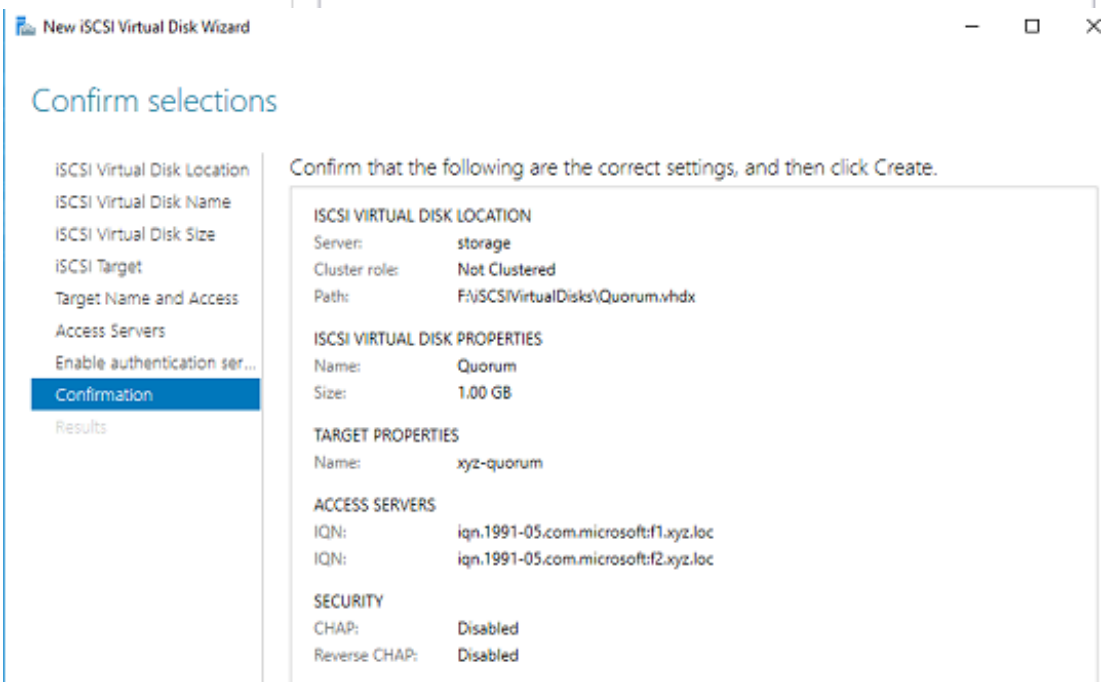

New iSCSI Virtual Disk Wizard
Specify iSCSI virtual disk size
iSCSI Virtual Disk Location
iSCSI Virtual Disk Name
iSCSI Virtual Disk Size
iSCSI Target
Target Name and Access
Access Servers
Enable authentication ser...
Confirmation
Results
Free space: 99.7 GB
Size: 1 GB
Fixed size
This type of disk provides 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:

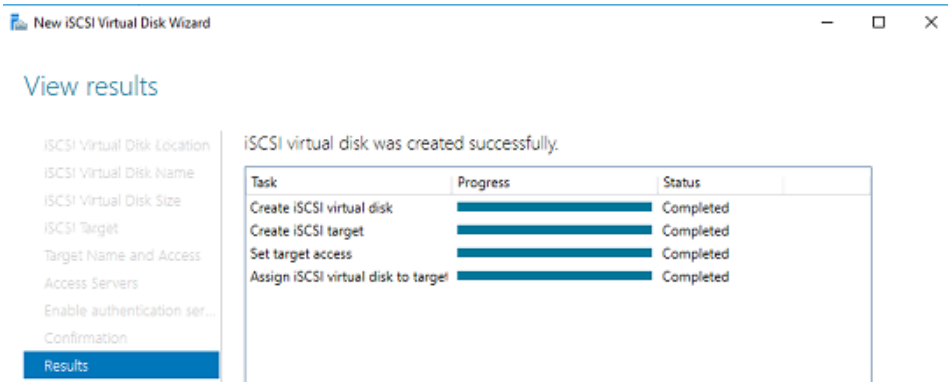

New iSCSI Virtual Disk Wizard
Assign iSCSI target
iSCSI Virtual Disk Location
iSCSI Virtual Disk Name
iSCSI Virtual Disk Size
iSCSI Target
Target Name and Access
Access Servers
Enable authentication ser...
Confirmation
Results
Assign this iSCSI virtual disk to an existing iSCSI target or create a new target for it.
Existing iSCSI target:
Target Name
Initiator IDs
Description
xyz-target
IPAddress:175.17.40.13, IPAddress:17...
New iSCSI target


New iSCSI Virtual Disk Wizard
Specify target name
iSCSI Virtual Disk Location
iSCSI Virtual Disk Name
iSCSI Virtual Disk Size
iSCSI Target
Target Name and Access
Access Servers
Name:
xyz-quorum
Description:

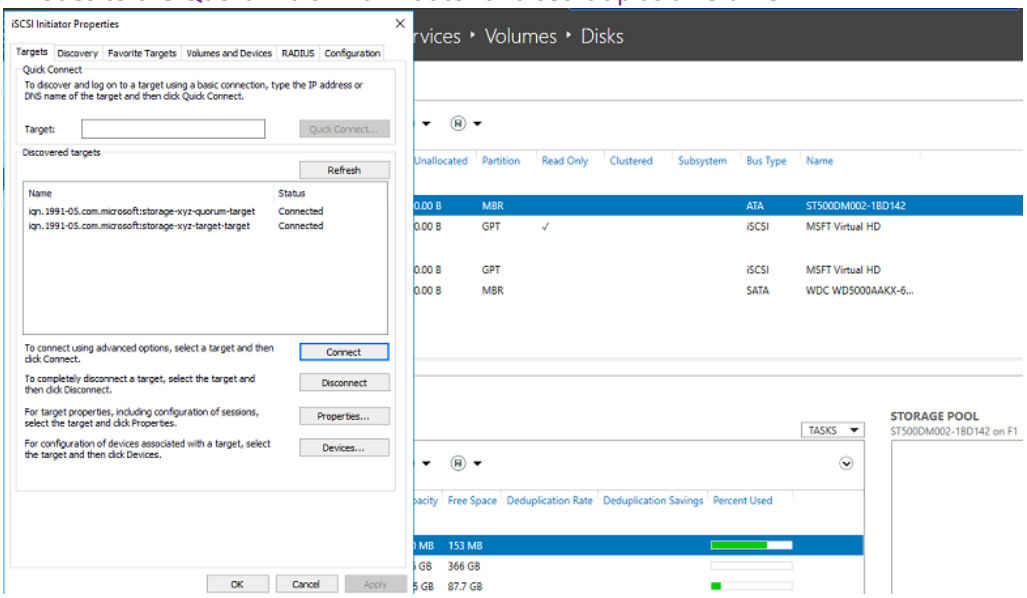

Add initiator ID
Select a method to identify the initiator:
Query initiator computer for ID (not supported on Windows Server 2008 R2, Windows 7, or earlier):
Browse...
Select from the initiator cache on the target server:
iqn.1991-05.com.microsoft:f1.xyz.loc
iqn.1991-05.com.microsoft:f2.xyz.loc
Enter a value for the selected type
Type:
Value:
IP Address
Browse...
OK
Cancel

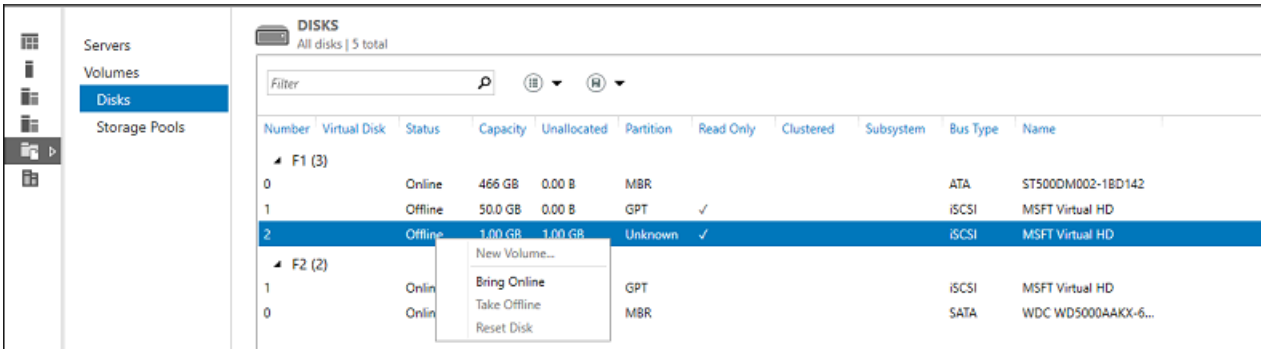

New iSCSI Virtual Disk Wizard
Specify access servers
iSCSI Virtual Disk Location
iSCSI Virtual Disk Name
iSCSI Virtual Disk Size
iSCSI Target
Target Name and Access
Access Servers
Enable authentication ser...
Confirmation
Results
Click Add to specify the iSCSI initiator(s) that will access this iSCSI virtual disk.
Type
Value
IQN
iqn.1991-05.com.microsoft:f1.xyz.loc
IQN
iqn.1991-05.com.microsoft:f2.xyz.loc

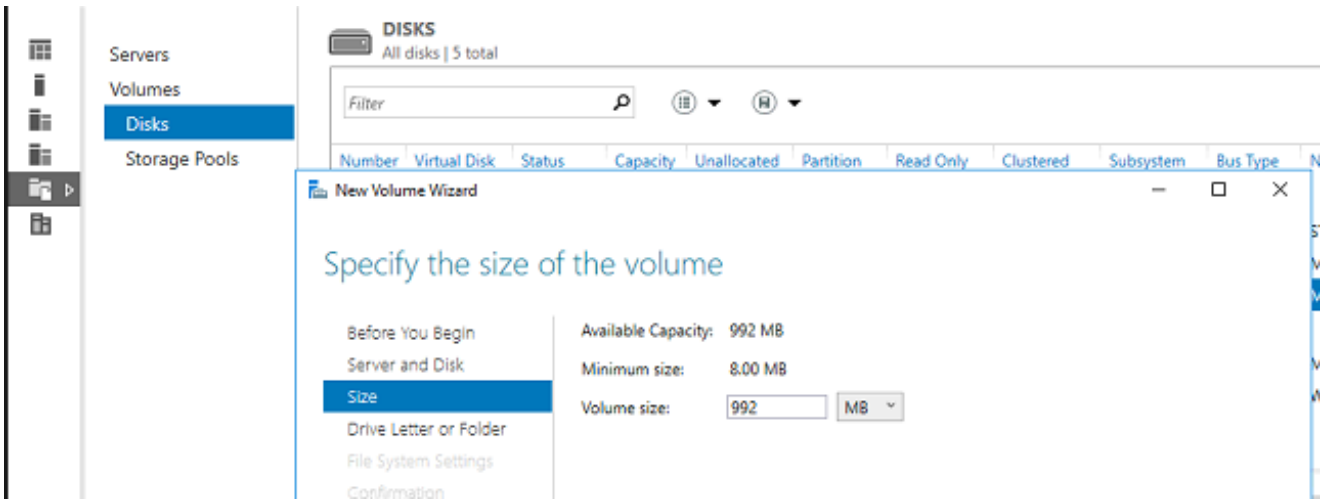

New iSCSI Virtual Disk Wizard
Confirm selections
iSCSI Virtual Disk Location
iSCSI Virtual Disk Name
iSCSI Virtual Disk Size
iSCSI Target
Target Name and Access
Access Servers
Enable authentication ser...
Confirmation
Results
Confirm that the following are the correct settings, and then click Create.
ISCSI VIRTUAL DISK LOCATION
Server: storage
Cluster role: Not Clustered
Path: F:\iSCSIVirtualDisks\Quorum.vhdx
ISCSI VIRTUAL DISK PROPERTIES
Name: Quorum
Size: 1.00 GB
TARGET PROPERTIES
Name: xyz-quorum
ACCESS SERVERS
IQN: iqn.1991-05.com.microsoft:f1.xyz.loc
IQN: iqn.1991-05.com.microsoft:f2.xyz.loc
SECURITY
CHAP: Disabled
Reverse CHAP: Disabled


New iSCSI Virtual Disk Wizard
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

Link both nodes to the Quorum disk via initiator and set it up as a volume.

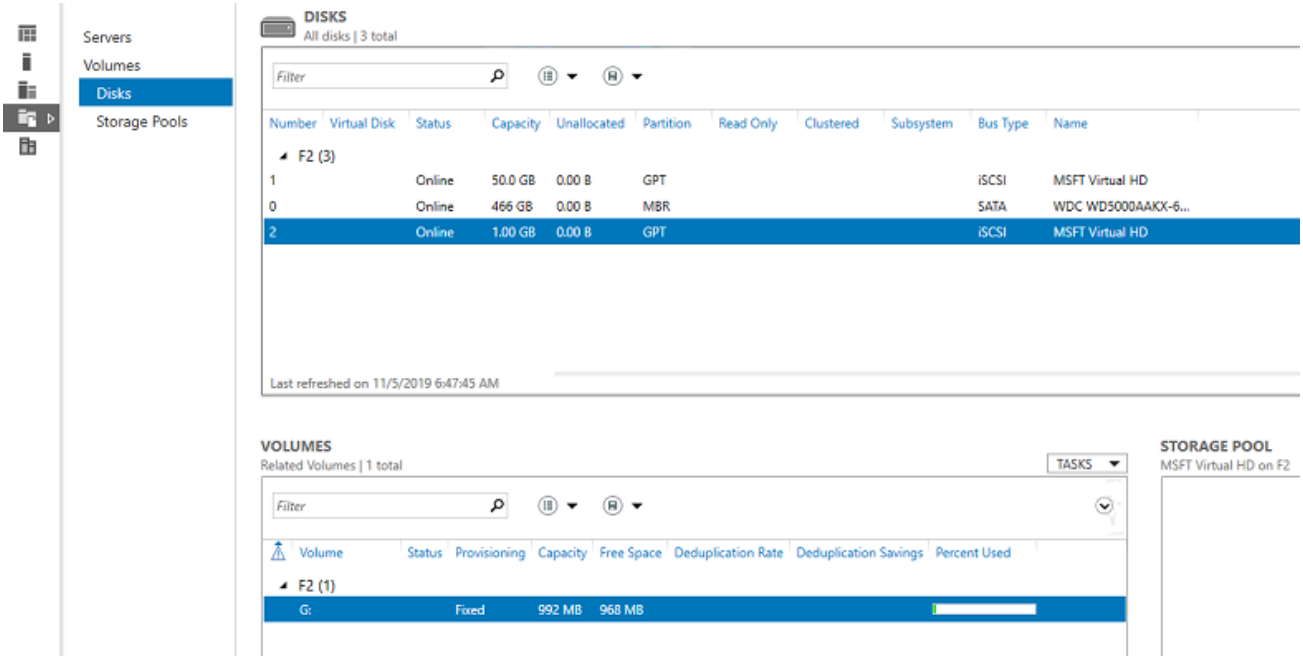






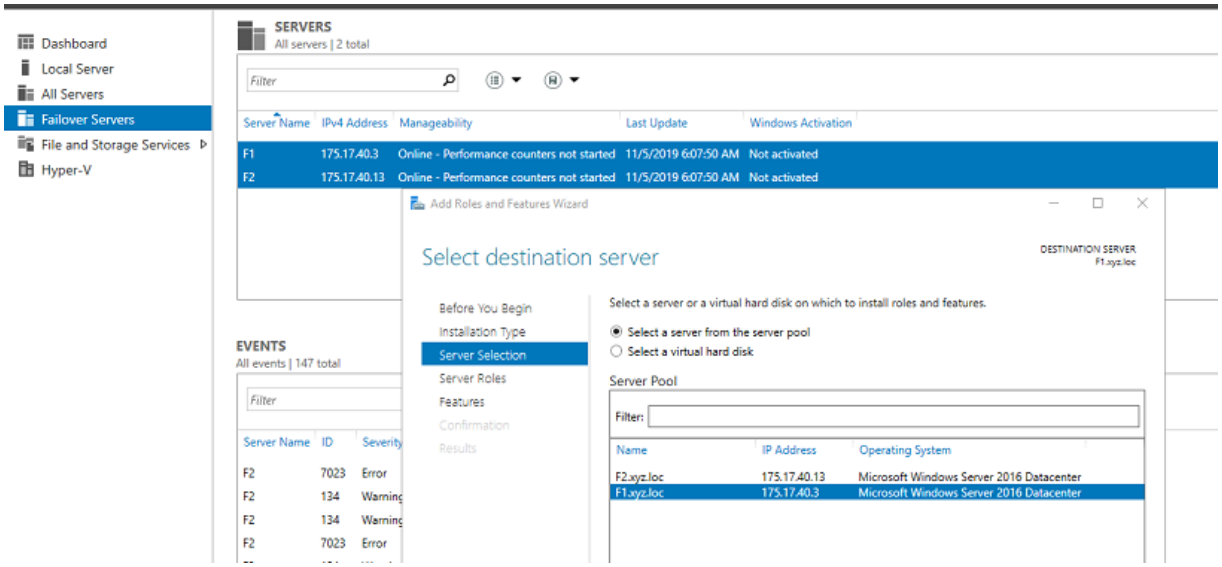
---

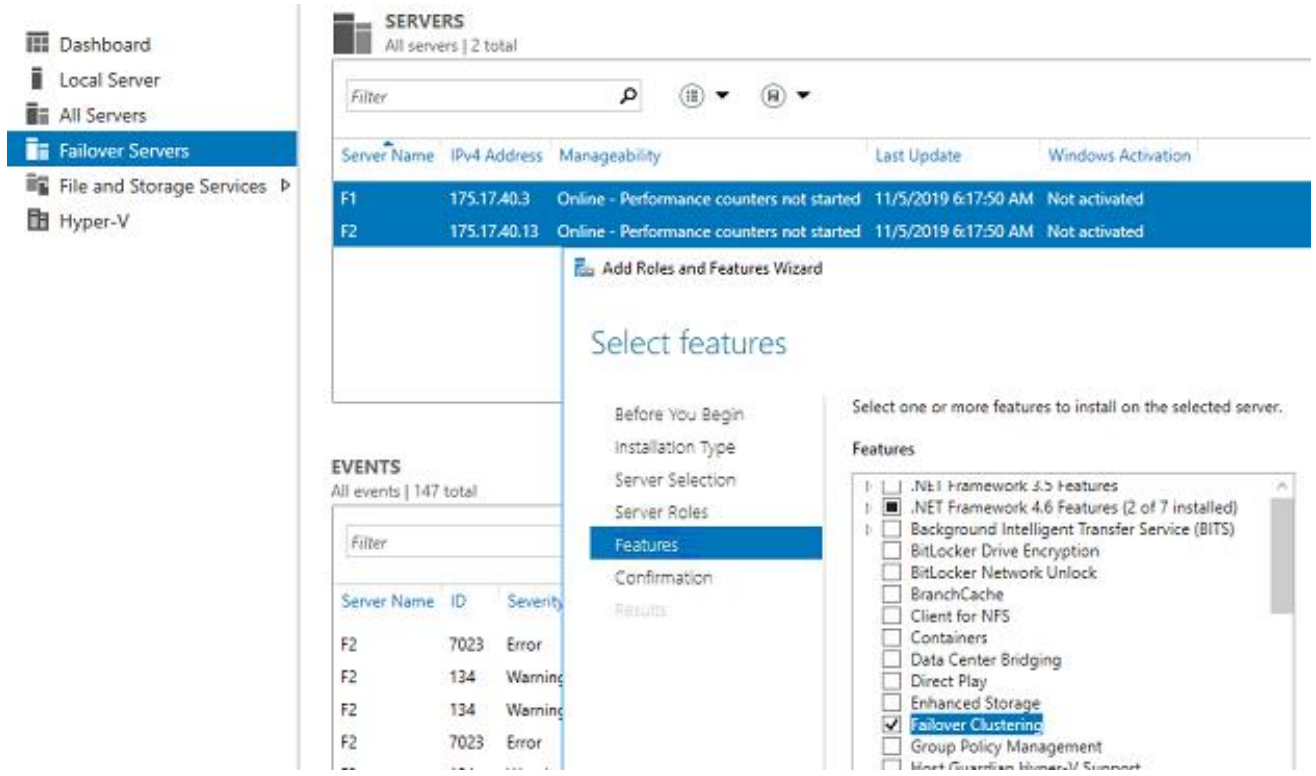
now attach it to a different node

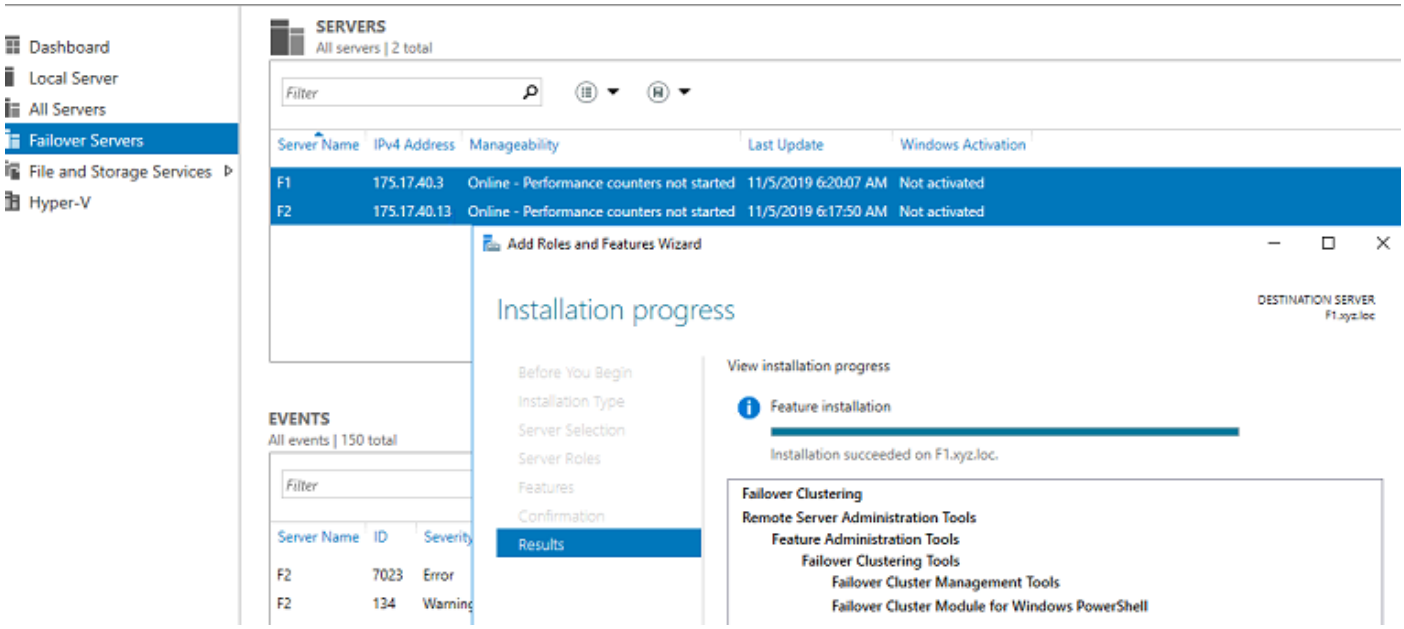


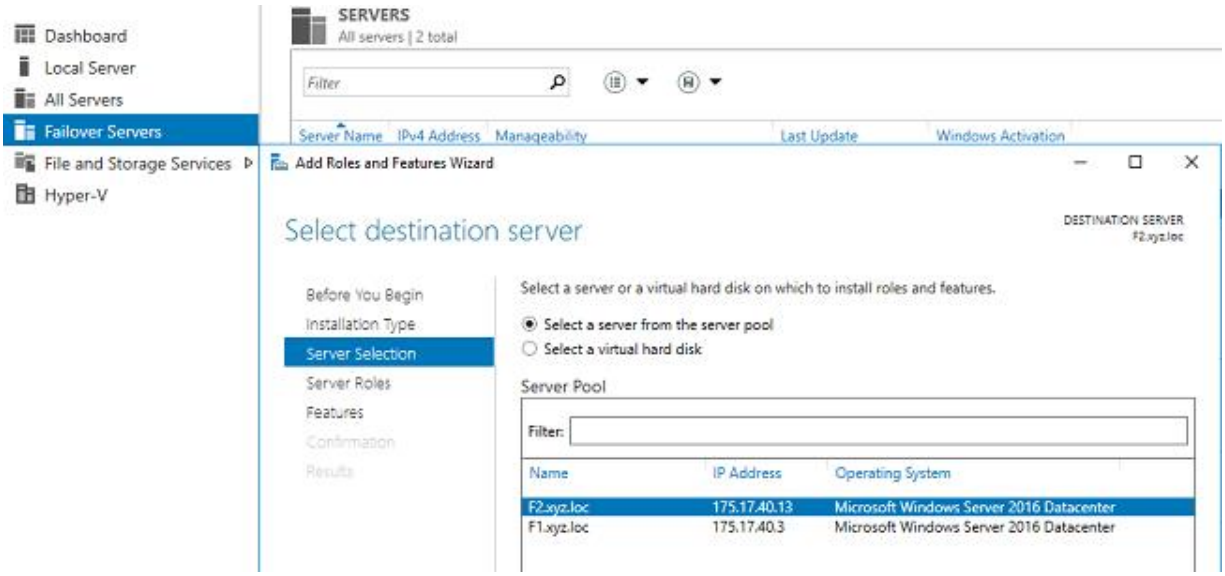
Set up the failover cluster on both nodes.

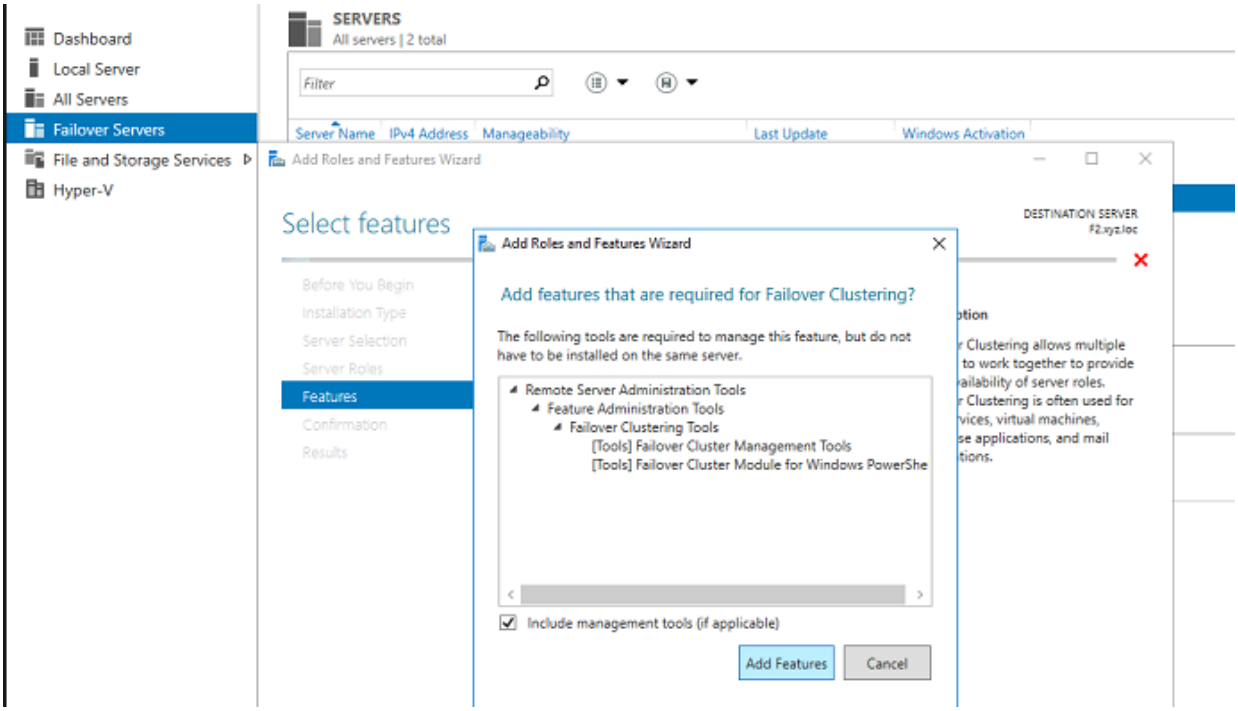
It's advised to set up the file server initially in case it needs to serve as a failover system.

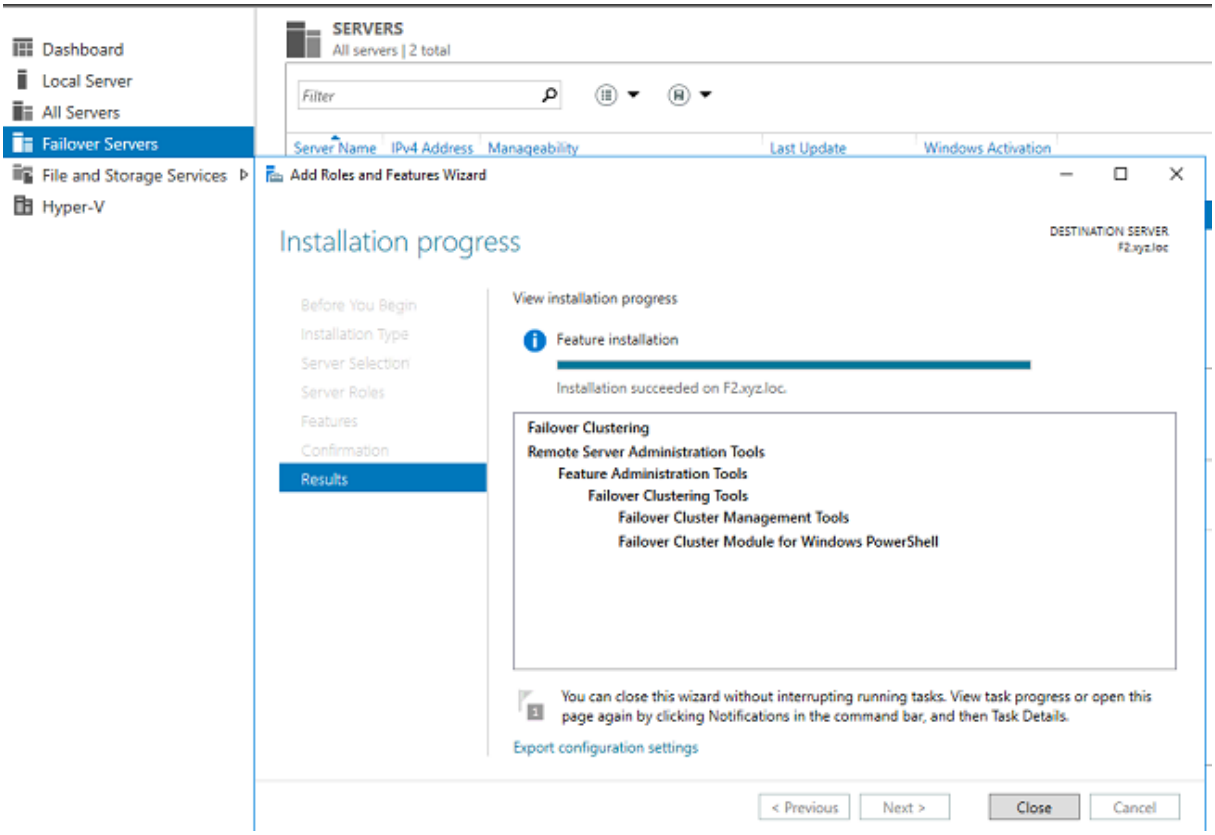



Dashboard
Local Server
All Servers
Failover Servers
File and Storage Services
Hyper-V
SERVERS
All servers | 2 total
Filter
Server Name
IPv4 Address
Manageability
Last Update
Windows Activation
F1 175.17.40.3 Online - Performance counters not started 11/5/2019 6:17:50 AM Not activated
F2 175.17.40.13 Online - Performance counters not started 11/5/2019 6:17:50 AM Not activated
Add Roles and Features Wizard
Select features
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 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
Group Policy Management
EVENTS
All events | 147 total
Server Name
ID
Severity
F2 7023 Error
F2 134 Warning
F2 134 Warning
F2 7023 Error


Dashboard
Local Server
All Servers
Failover Servers
File and Storage Services
Hyper-V
SERVERS
All servers | 2 total
Filter
Server Name
IPv4 Address
Manageability
Last Update
Windows Activation
F1 175.17.40.3 Online - Performance counters not started 11/5/2019 6:20:07 AM Not activated
F2 175.17.40.13 Online - Performance counters not started 11/5/2019 6:17:50 AM Not activated
Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
F1.xyz.loc
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
View installation progress
Feature installation
Installation succeeded on F1.xyz.loc.
Failover Clustering
Remote Server Administration Tools
Feature Administration Tools
Failover Clustering Tools
Failover Cluster Management Tools
Failover Cluster Module for Windows PowerShell
EVENTS
All events | 150 total
Server Name
ID
Severity
F2 7023 Error
F2 134 Warning

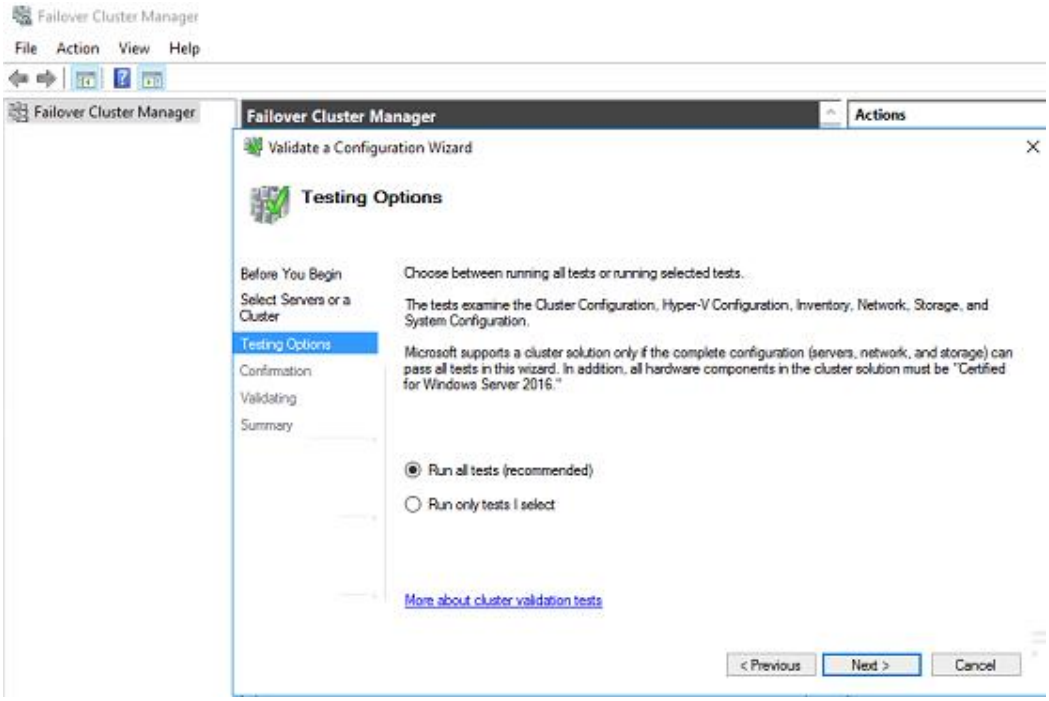

Dashboard
Local Server
All Servers
Failover Servers
File and Storage Services
Hyper-V
SERVERS
All servers | 2 total
Filter
Server Name
IPv4 Address
Manageability
Last Update
Windows Activation
Add Roles and Features Wizard
Select destination server
DESTINATION SERVER
F2.xyz.loc
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
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
F2.xyz.loc
175.17.40.13
Microsoft Windows Server 2016 Datacenter
F1.xyz.loc
175.17.40.3
Microsoft Windows Server 2016 Datacenter

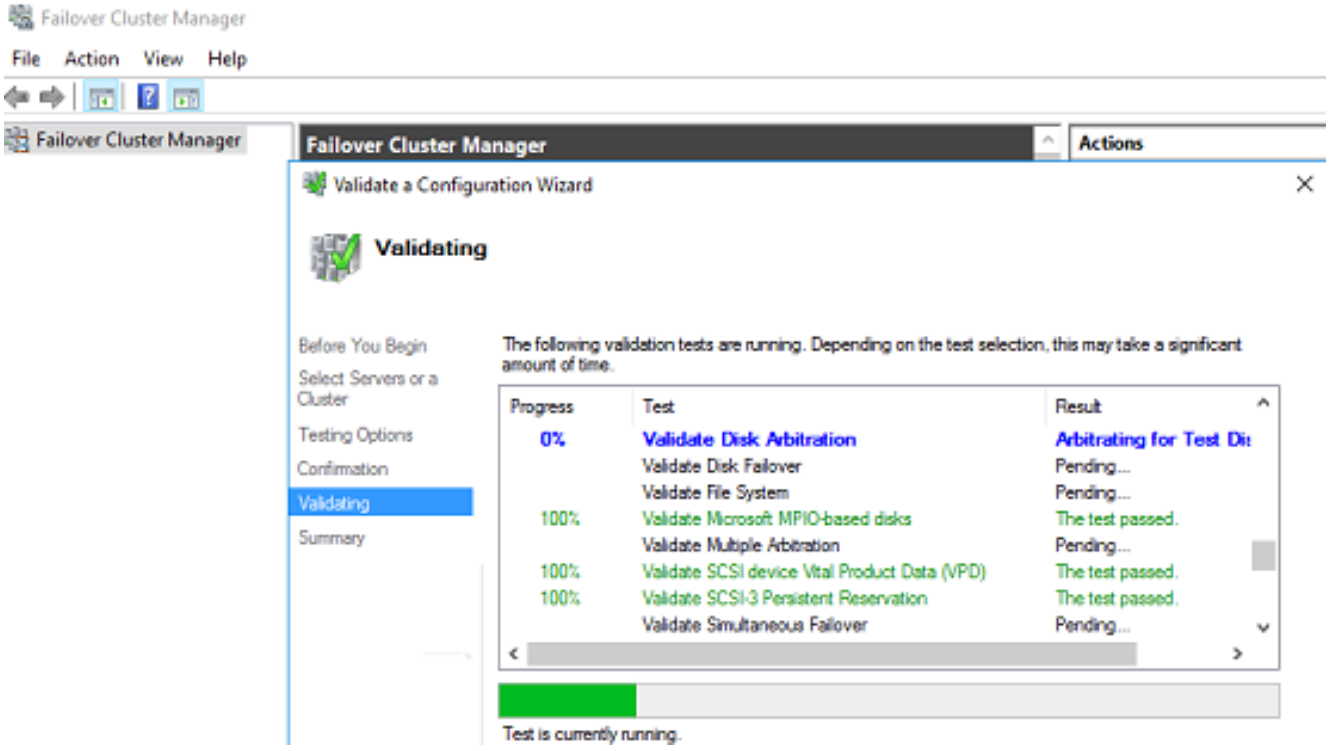

Dashboard
Local Server
All Servers
Failover Servers
File and Storage Services
Hyper-V
SERVERS
All servers | 2 total
Filter
Server Name
IPv4 Address
Manageability
Last Update
Windows Activation
Add Roles and Features Wizard
Select features
DESTINATION SERVER
F2.xyz.loc
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Add Roles and Features Wizard
Add features that are required for Failover Clustering?
The following tools are required to manage this feature, but do not have to be installed on the same server.
Remote Server Administration Tools
Feature Administration Tools
Failover Clustering Tools
[Tools] Failover Cluster Management Tools
[Tools] Failover Cluster Module for Windows PowerShe
Include management tools (if applicable)
Add Features
Cancel



We're prepared to integrate two nodes into the cluster now.

First, check that the required setup is in place on both nodes to function as a failover cluster.


Failover Cluster Manager
File Action View Help
Failover Cluster Manager
Failover Cluster Manager
Actions
Validate a Configuration Wizard
Testing Options
Before You Begin
Select Servers or a Cluster
Testing Options
Confirmation
Validating
Summary
Choose between running all tests or running selected tests.
The tests examine the Cluster Configuration, Hyper-V Configuration, Inventory, Network, Storage, and System Configuration.
Microsoft supports a cluster solution only if the complete configuration (servers, network, and storage) can pass all tests in this wizard. In addition, all hardware components in the cluster solution must be "Certified for Windows Server 2016."
Run all tests (recommended)
Run only tests I select
More about cluster validation tests
< Previous
Next >
Cancel


Failover Cluster Manager
File Action View Help
Failover Cluster Manager
Failover Cluster Manager
Actions
Validate a Configuration Wizard
Validating
Before You Begin
Select Servers or a Cluster
Testing Options
Confirmation
Validating
Summary
The following validation tests are running. Depending on the test selection, this may take a significant amount of time.
Progress
Test
Result
0%
Validate Disk Arbitration
Arbitrating for Test Di
Validate Disk Failover
Pending...
Validate File System
Pending...
100%
Validate Microsoft MPIO-based disks
The test passed.
Validate Multiple Arbitration
Pending...
100%
Validate SCSI device Vital Product Data (VPD)
The test passed.
100%
Validate SCSI-3 Persistent Reservation
The test passed.
Validate Simultaneous Failover
Pending...
Test is currently running.

Examine the test report and address any highlighted issues.

C:\Users\Administrator.XYZ\AppData\Local\Temp\tmpEE1D.tmp.htm — Failover Cluster Validation R...

Microsoft Home

Failover Cluster Validation Report

Node:	F1.xyz.loc	Validated
Node:	F2.xyz.loc	Validated
Started	11/5/2019 6:49:25 AM	
Completed	11/5/2019 6:51:58 AM	

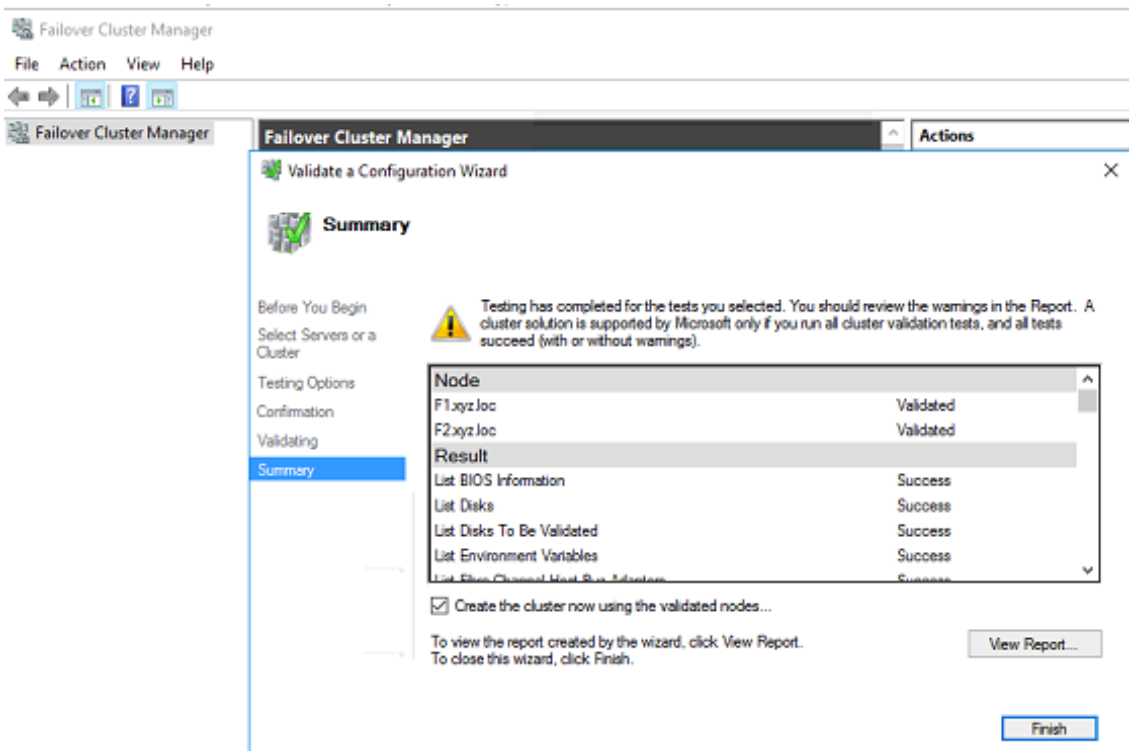
The Validate a Configuration Wizard must be run after any change is made to the configuration of the cluster or hardware. For more information, see http://go.microsoft.com/fwlink/p/?LinkId=280145.

Results by Category

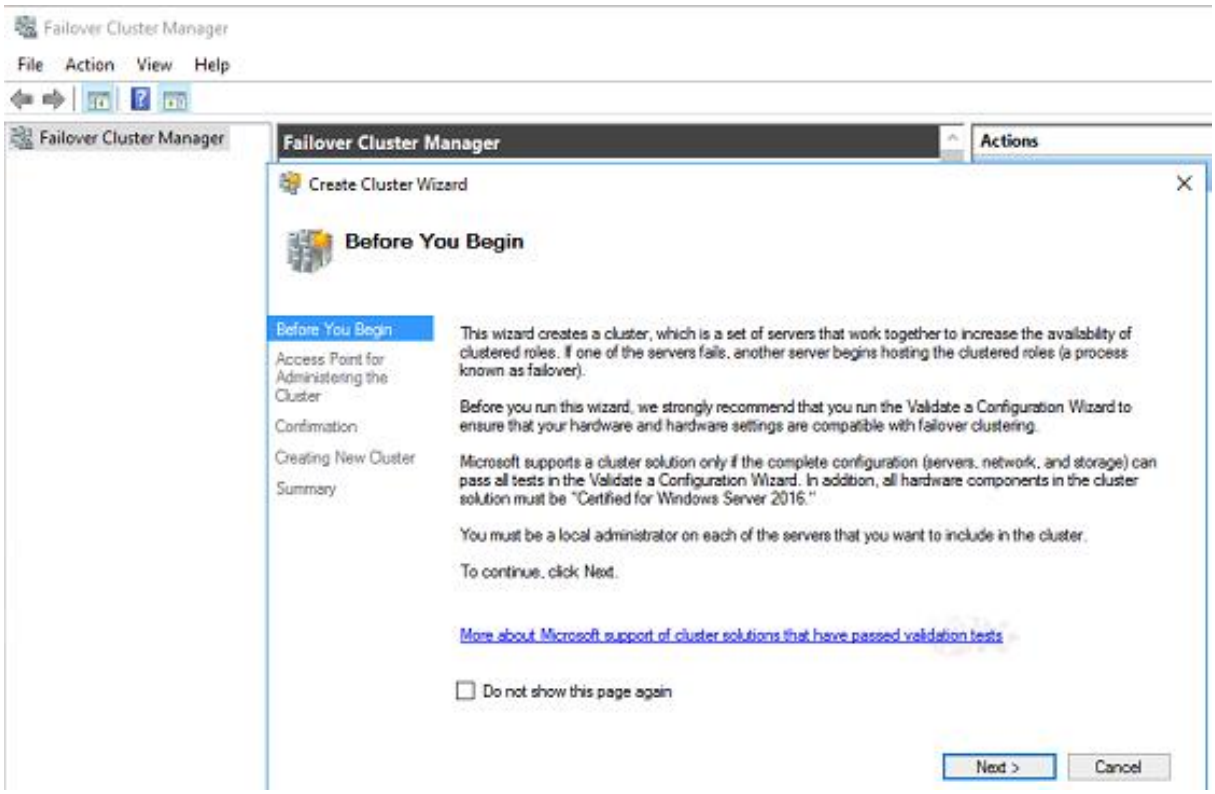
Name	Result Summary	Description
Hyper-V Configuration		Success
Inventory		Success
Network		Warning
Storage		Success
System Configuration		Success

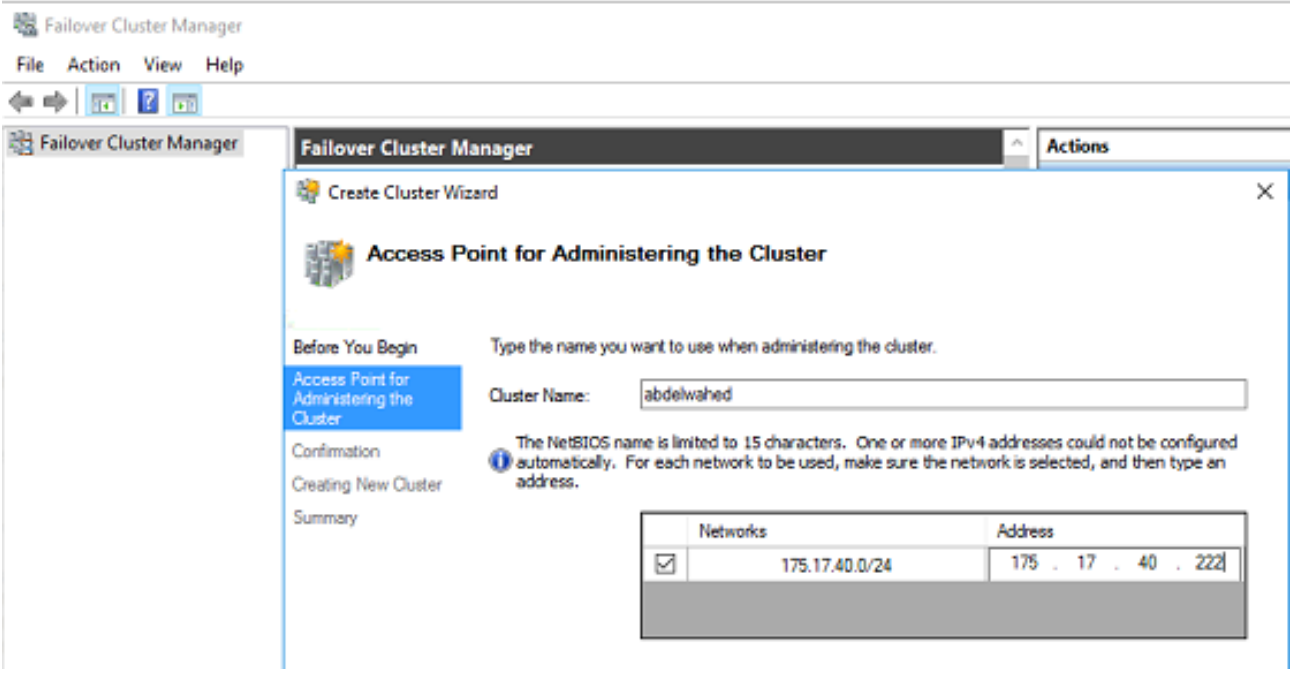
Hyper-V Configuration

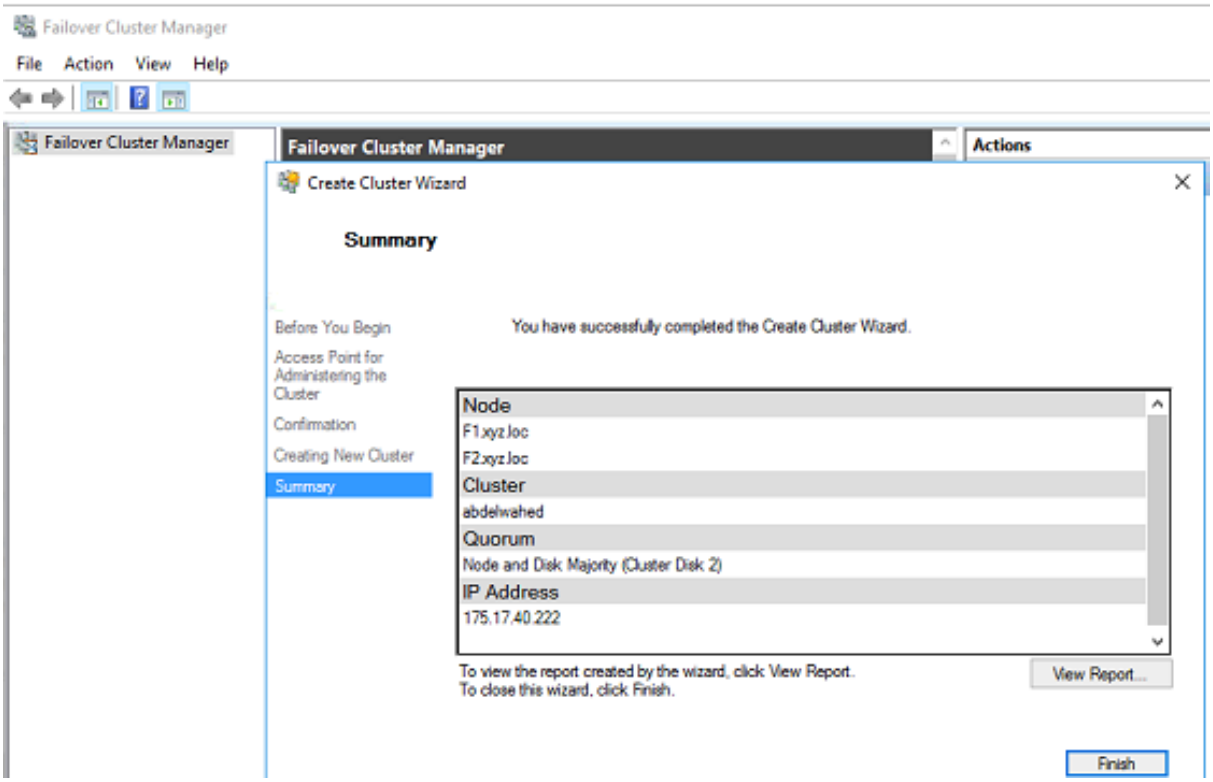
Name	Result	Description
List Information About Servers Running Hyper-V		Success
Validate Compatibility of Virtual Fibre Channel SANs for Hyper-V		Success
Validate Hyper-V Memory Resource Pool Compatibility		Success
Validate Hyper-V Network Resource Pool And Virtual Switch Compatibility		Success
Validate Hyper-V Processor Resource Pool Compatibility		Success
Validate Hyper-V Role Installed		Success
Validate Hyper-V Storage Resource Pool Compatibility		Success

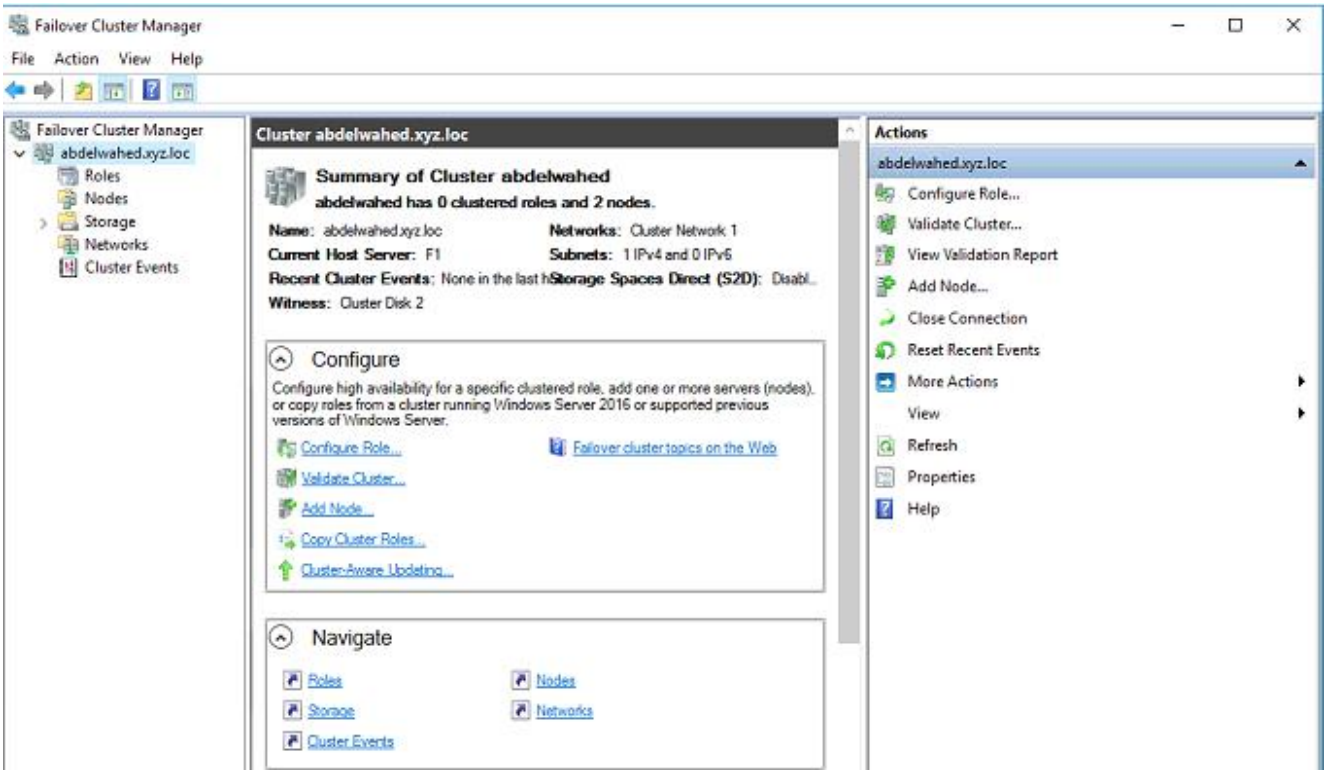


Now, we are prepared to construct our cluster.

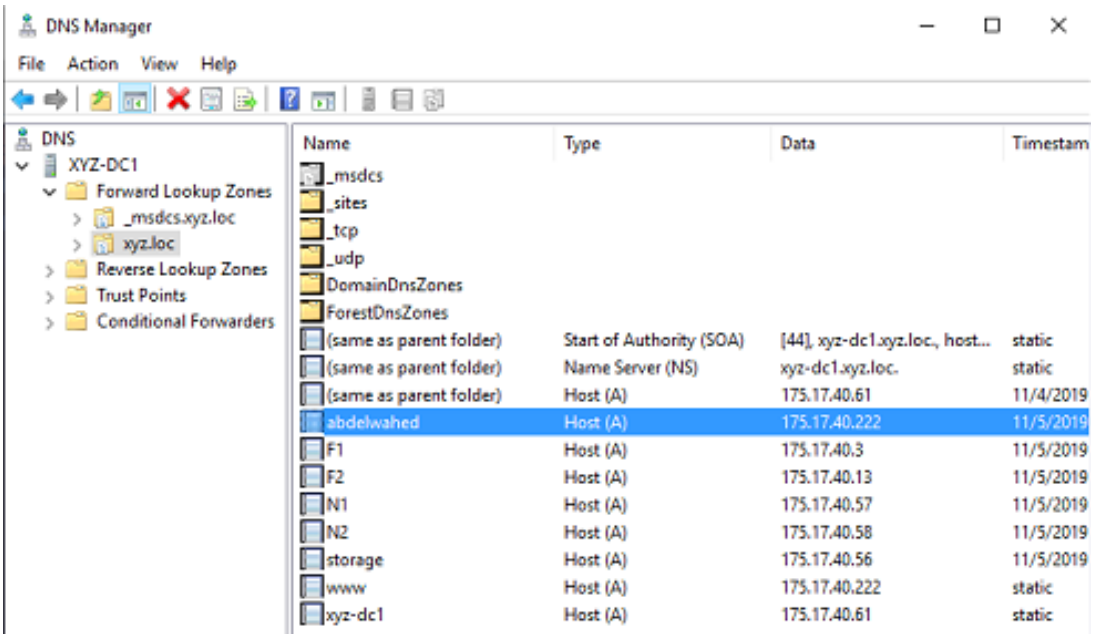

Failover Cluster Manager
File Action View Help
Failover Cluster Manager
Failover Cluster Manager
Actions
Create Cluster Wizard
Before You Begin
Before You Begin
Access Point for Administering the Cluster
Confirmation
Creating New Cluster
Summary
This wizard creates a cluster, which is a set of servers that work together to increase the availability of clustered roles. If one of the servers fails, another server begins hosting the clustered roles (a process known as failover).
Before you run this wizard, we strongly recommend that you run the Validate a Configuration Wizard to ensure that your hardware and hardware settings are compatible with failover clustering.
Microsoft supports a cluster solution only if the complete configuration (servers, network, and storage) can pass all tests in the Validate a Configuration Wizard. In addition, all hardware components in the cluster solution must be "Certified for Windows Server 2016."
You must be a local administrator on each of the servers that you want to include in the cluster.
To continue, click Next.
More about Microsoft support of cluster solutions that have passed validation tests
Do not show this page again
Next >
Cancel

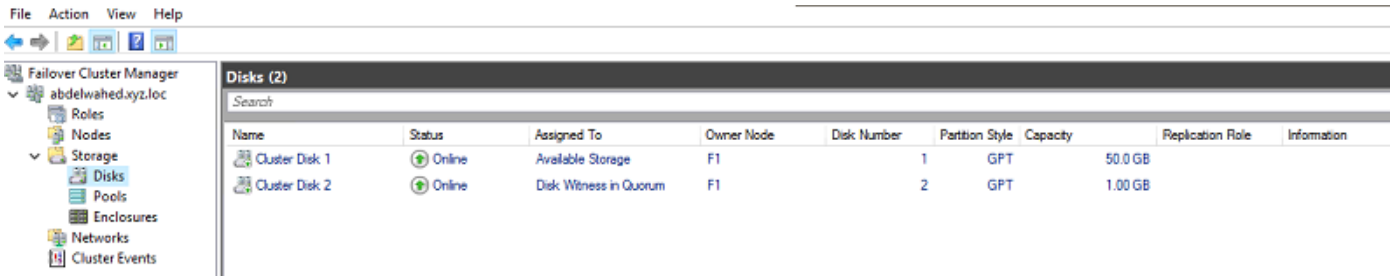

Failover Cluster Manager
File Action View Help
Failover Cluster Manager
Failover Cluster Manager
Actions
Create Cluster Wizard
Access Point for Administering the Cluster
Before You Begin
Access Point for Administering the Cluster
Confirmation
Creating New Cluster
Summary
Type the name you want to use when administering the cluster.
Cluster Name:
abdelwahed
The NetBIOS name is limited to 15 characters. One or more IPv4 addresses could not be configured automatically. For each network to be used, make sure the network is selected, and then type an address.
Networks
Address
175.17.40.0/24
175 . 17 . 40 . 222

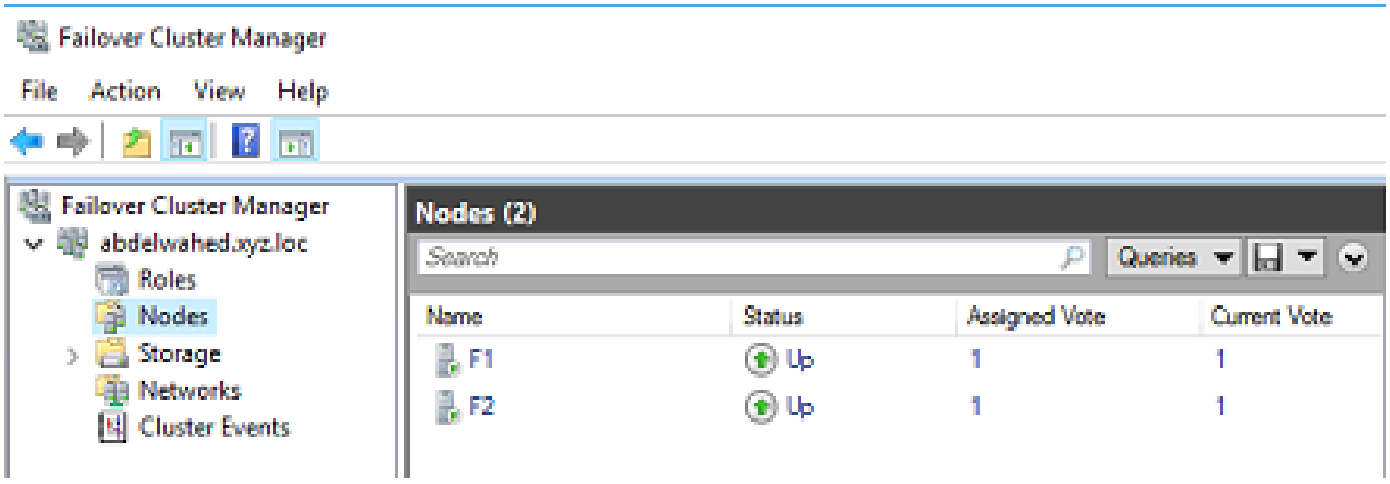

Failover Cluster Manager
File Action View Help
Failover Cluster Manager
Failover Cluster Manager
Actions
Create Cluster Wizard
Summary
Before You Begin
Access Point for Administering the Cluster
Confirmation
Creating New Cluster
Summary
You have successfully completed the Create Cluster Wizard.
Node
F1.xyz.loc
F2.xyz.loc
Cluster
abdelwahed
Quorum
Node and Disk Majority (Cluster Disk 2)
IP Address
175.17.40.222
To view the report created by the wizard, click View Report.
To close this wizard, click Finish.
View Report...
Finish


Failover Cluster Manager
File Action View Help
Failover Cluster Manager
abdelwahed.xyz.loc
Roles
Nodes
Storage
Networks
Cluster Events
Cluster abdelwahed.xyz.loc
Summary of Cluster abdelwahed
abdelwahed has 0 clustered roles and 2 nodes.
Name: abdelwahed.xyz.loc
Networks: Cluster Network 1
Current Host Server: F1
Subnets: 1 IPv4 and 0 IPv6
Recent Cluster Events: None in the last h
Storage Spaces Direct (S2D): Disabl...
Witness: Cluster Disk 2
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
Navigate
Roles
Nodes
Storage
Networks
Cluster Events
Actions
abdelwahed.xyz.loc
Configure Role...
Validate Cluster...
View Validation Report
Add Node...
Close Connection
Reset Recent Events
More Actions
View
Refresh
Properties
Help

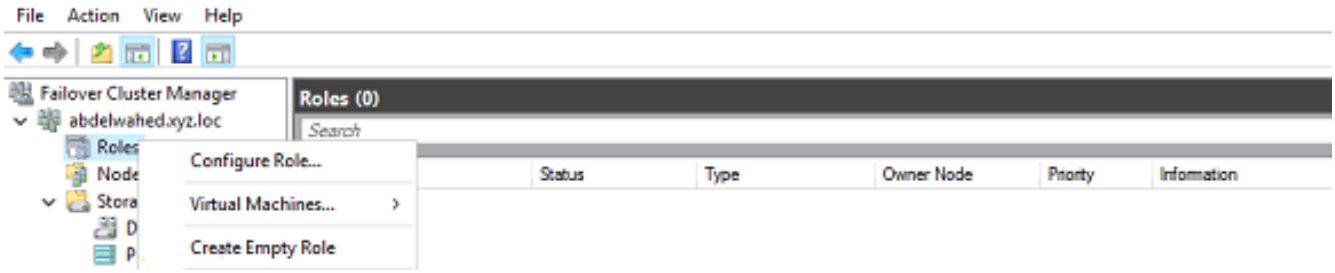
A record for the cluster name is created in the DNS server, allowing us to access the cluster via its name.

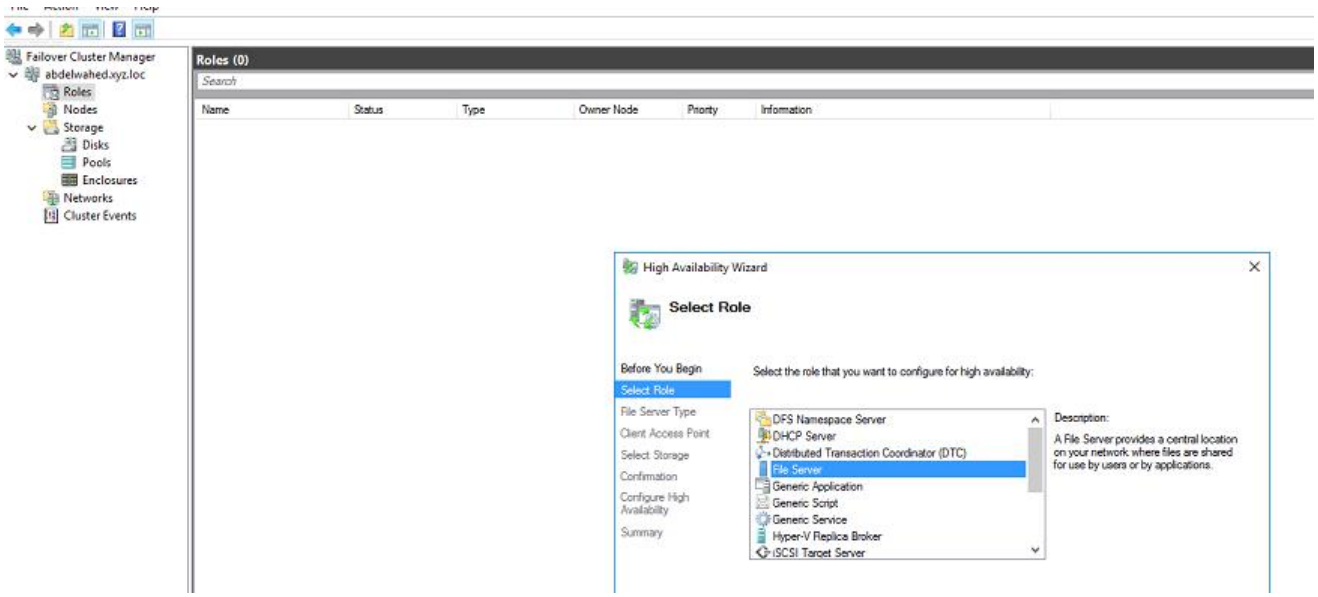


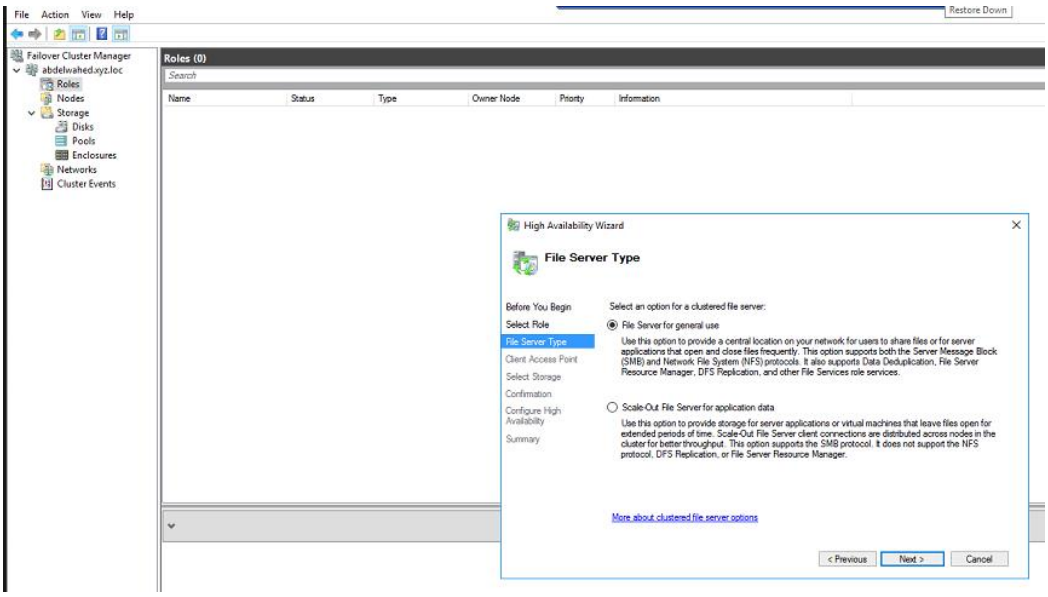


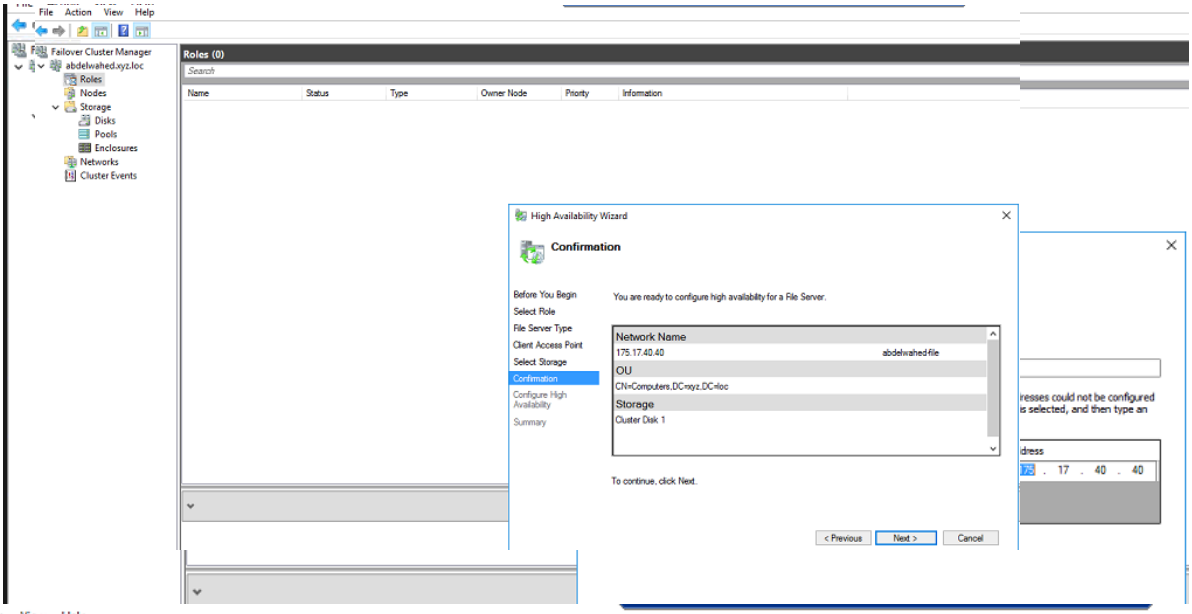


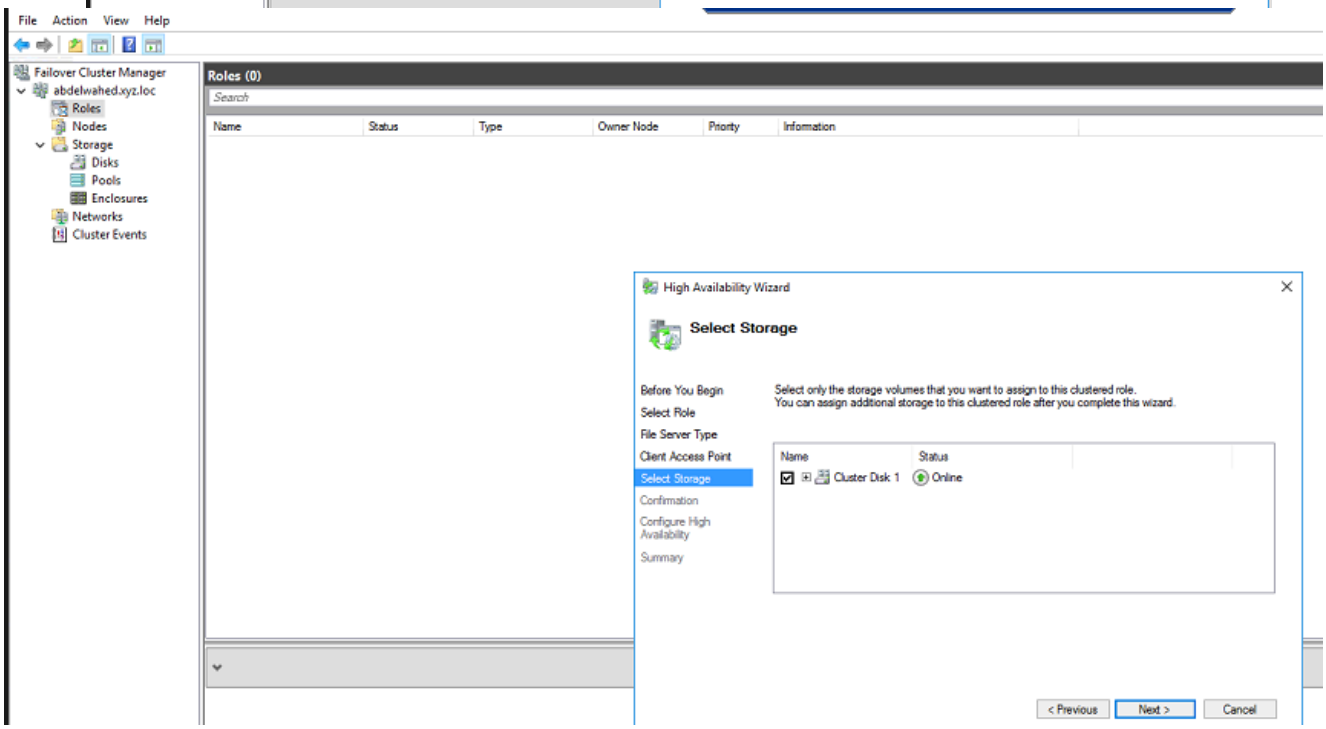
Testing: To start, install the file server role on both nodes before proceeding to the next step.

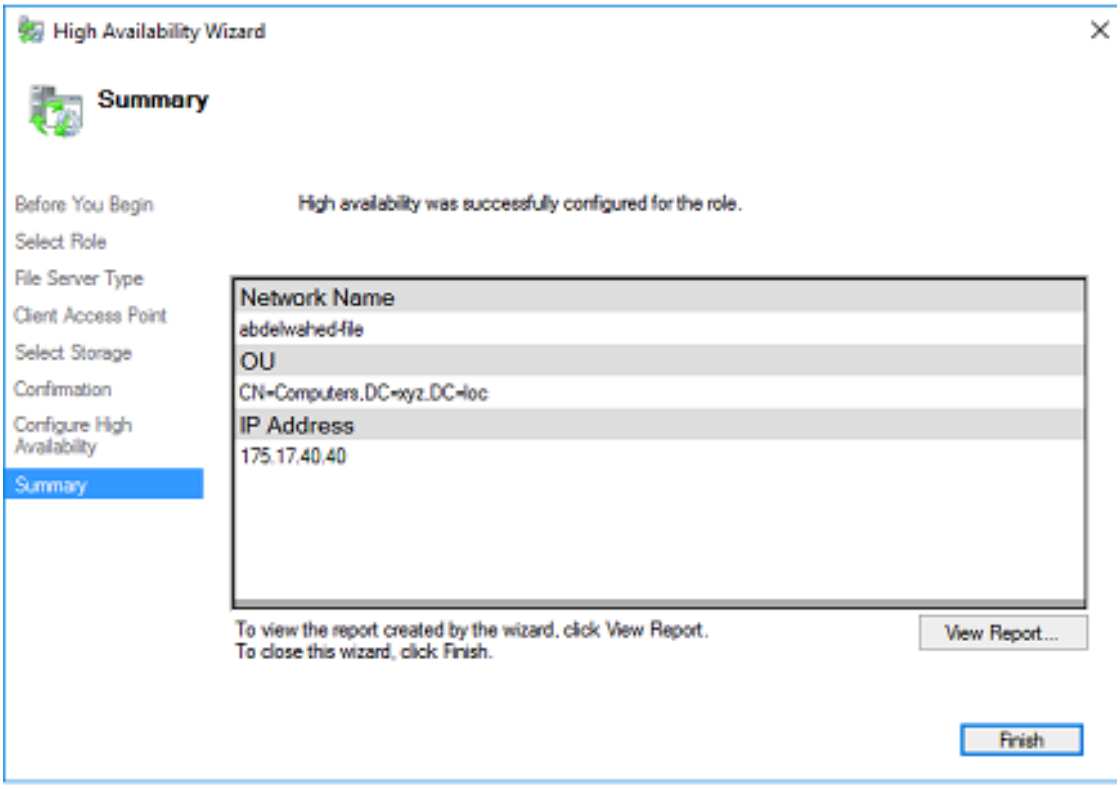


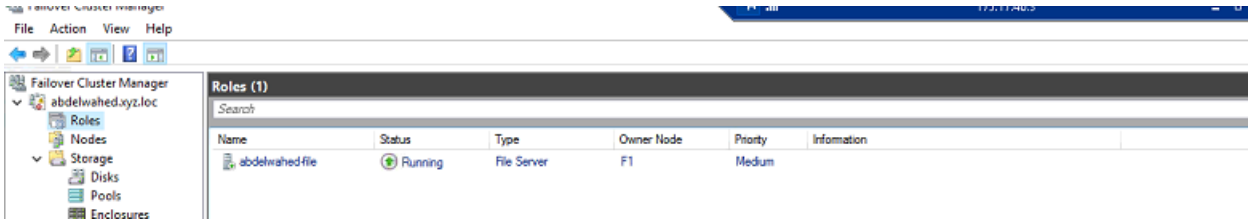




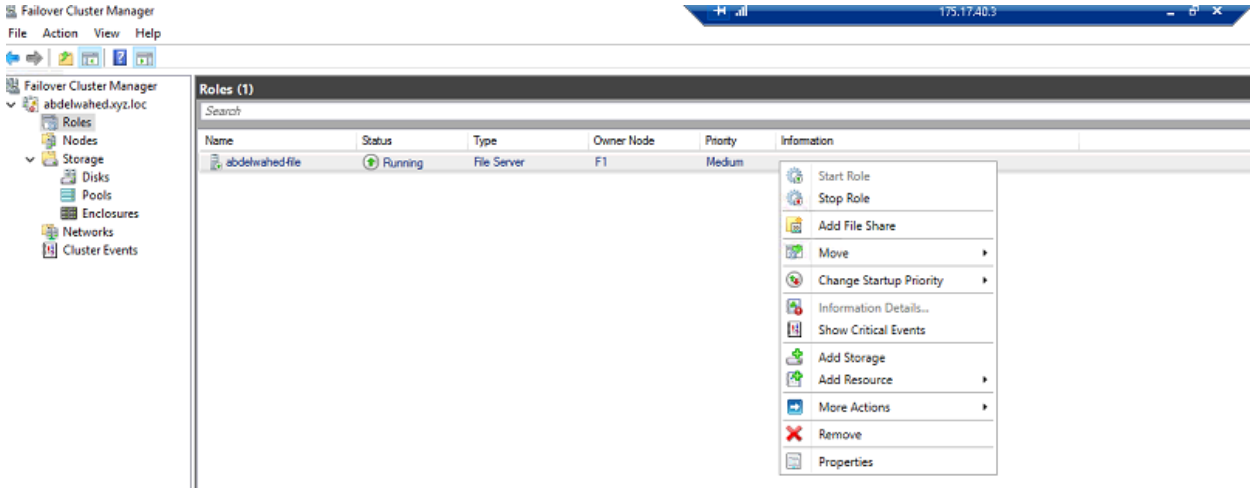

File Action View Help
Failover Cluster Manager
abdelwahed.xyz.loc
Roles
Nodes
Storage
Disks
Pools
Enclosures
Networks
Cluster Events
Roles (0)
Search
Name
Status
Type
Owner Node
Priority
Information
High Availability Wizard
Confirmation
Before You Begin
Select Role
File Server Type
Client Access Point
Select Storage
Confirmation
Configure High Availability
Summary
You are ready to configure high availability for a File Server.
Network Name
175.17.40.40
abdelwahed-file
OU
CN=Computers,DC=xyz,DC=loc
Storage
Cluster Disk 1
To continue, click Next.
< Previous
Next >
Cancel

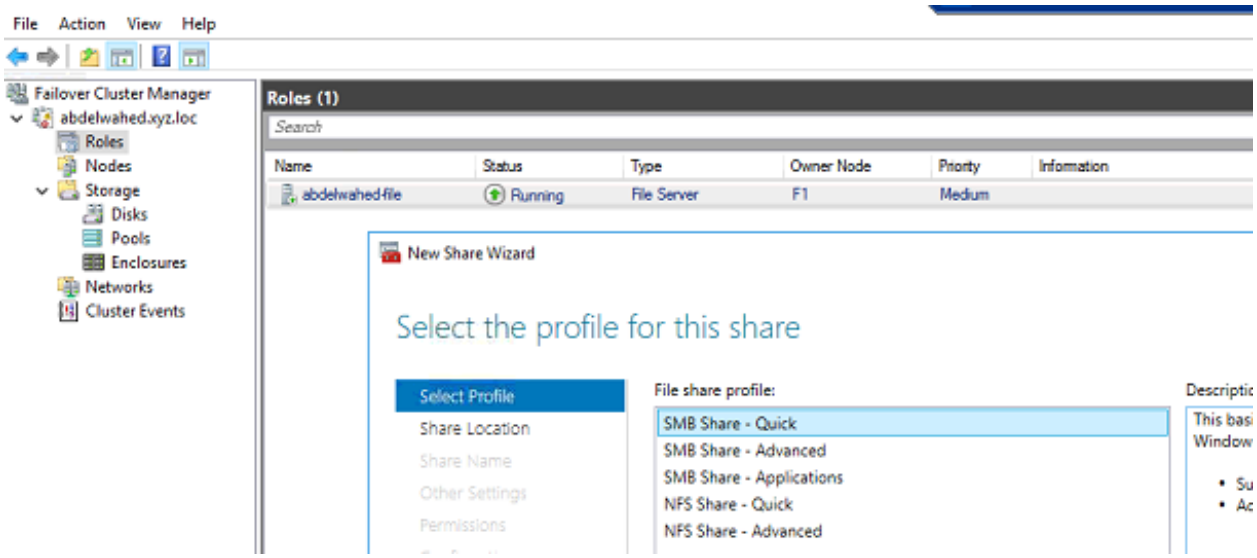

File Action View Help
Failover Cluster Manager
abdelwahed.xyz.loc
Roles
Nodes
Storage
Disks
Pools
Enclosures
Networks
Cluster Events
Roles (0)
Search
Name
Status
Type
Owner Node
Priority
Information
High Availability Wizard
Select Storage
Before You Begin
Select Role
File Server Type
Client Access Point
Select Storage
Confirmation
Configure High Availability
Summary
Select only the storage volumes that you want to assign to this clustered role.
You can assign additional storage to this clustered role after you complete this wizard.
Name
Status
Cluster Disk 1
Online
< Previous
Next >
Cancel

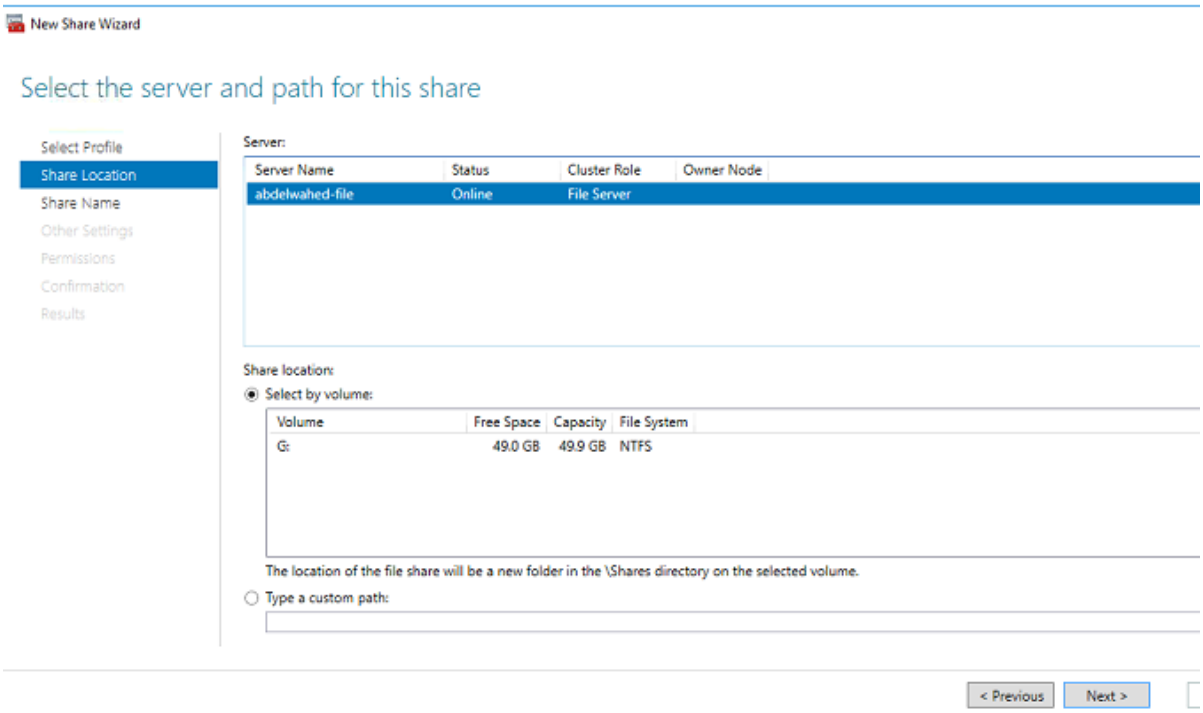

High Availability Wizard
Summary
Before You Begin
Select Role
File Server Type
Client Access Point
Select Storage
Confirmation
Configure High Availability
Summary
High availability was successfully configured for the role.
Network Name
abdelwahed-file
OU
CN=Computers,DC=xyz,DC=loc
IP Address
175.17.40.40
To view the report created by the wizard, click View Report.
To close this wizard, click Finish.
View Report...
Finish


File Action View Help
Failover Cluster Manager
abdelwahed.xyz.loc
Roles
Nodes
Storage
Disks
Pools
Enclosures
Roles (1)
Search
Name
Status
Type
Owner Node
Priority
Information
abdelwahed-file
Running
File Server
F1
Medium

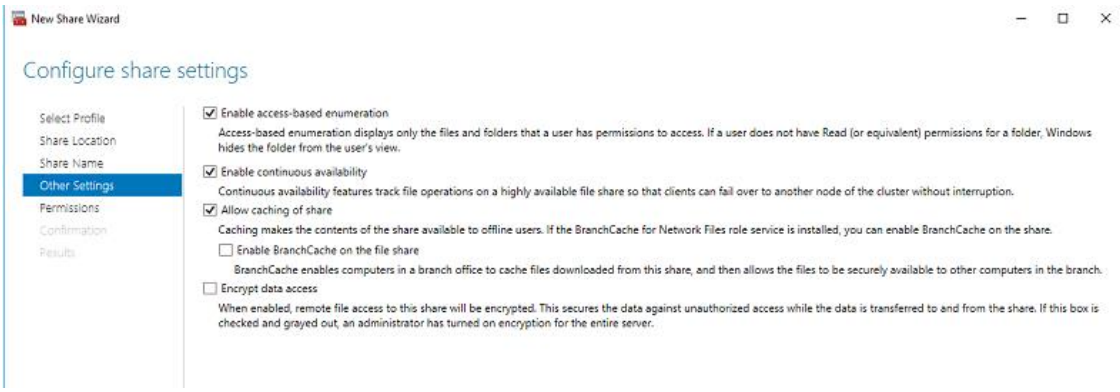
Additionally, a DNS record has been established for the file server to enable access by its name.
Testing by adding file share using cluster

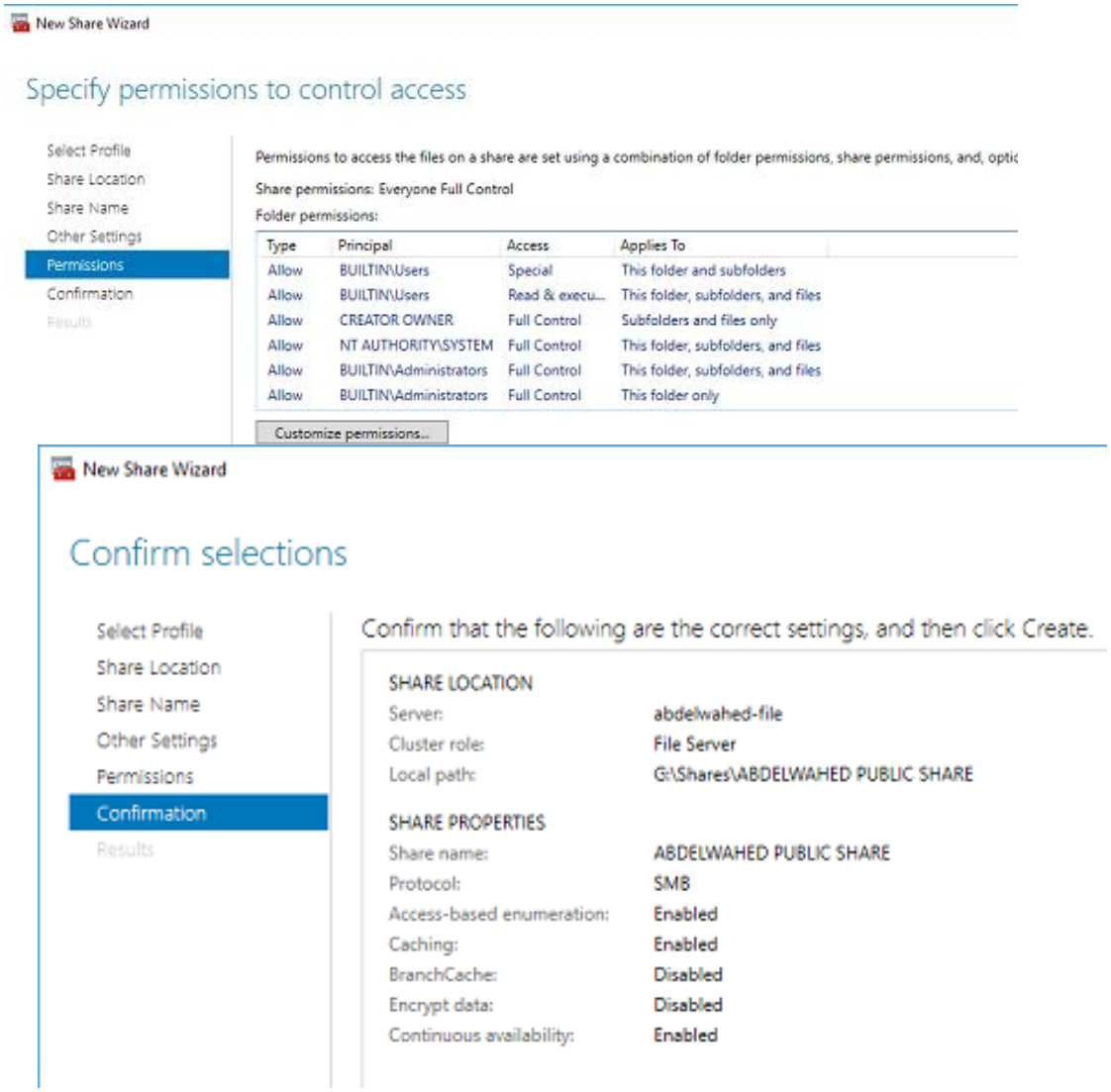




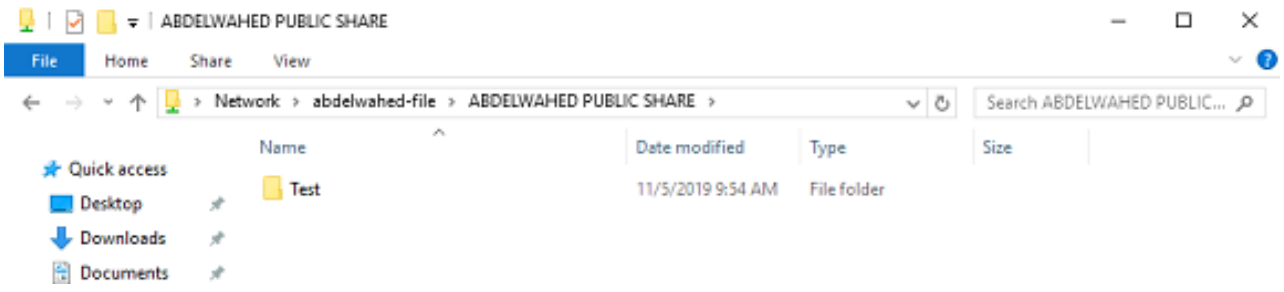


turn on the continuous availability feature.





You are now able to access files that are shared. Additionally, if you disconnect a node, you will observe that access to the shared file is maintained.



Active Directory Certification Service – ADCS

What is AD CS?

AD CS is a feature of Windows Server that simplifies the creation and management of certificates for PKI. Certificates enable secure communication and transactions by encrypting data and verifying the identity of users and computers within and outside the organization.

Overview of PKI

A public key infrastructure (PKI) is a system of software, encryption technologies, processes, and services that enables an organization to secure its communications and business transactions. PKI relies on the exchange of digital certificates between authenticated users and trusted resources. Certificates are used to encrypt data and to verify the identity of users and computers both within and outside of the organization.

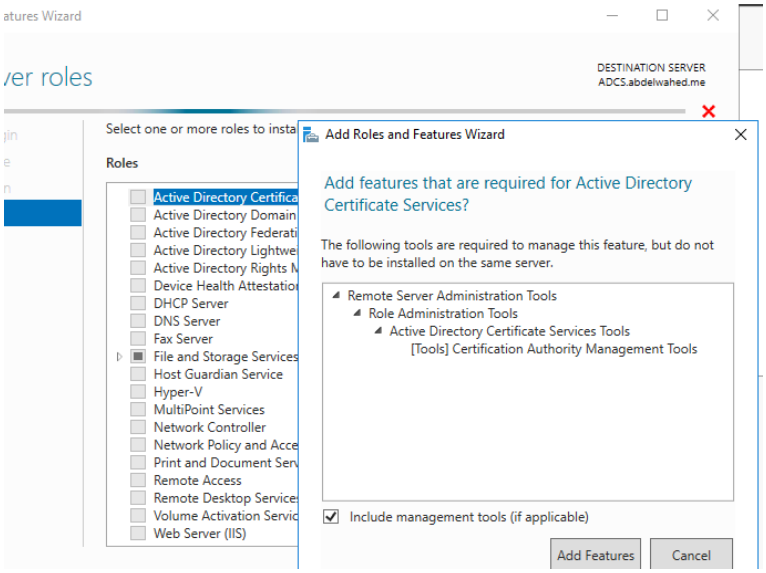
- Confidentiality – the property that ensures that data is only accessible to authorized parties and protected from unauthorized access or disclosure.
- Integrity – the property that ensures that data is accurate, complete, and consistent, and protected from unauthorized modification or corruption.
- Authenticity – the property that ensures that the identity of a user or a resource is verified and trustworthy, and that the source and destination of data are genuine.
- Nonrepudiation – the property that ensures that the origin and receipt of data are provable and undeniable, and that the parties involved in a transaction cannot dispute their participation or the validity of the data.
- Availability – the property that ensures that data and resources are accessible and usable by authorized parties when needed, and that the system can resist and recover from failures or attacks.

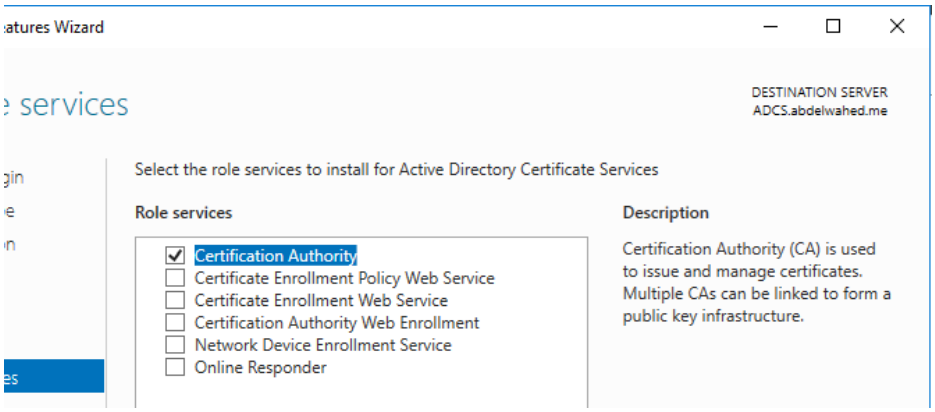
Standalone vs. Enterprise CAs

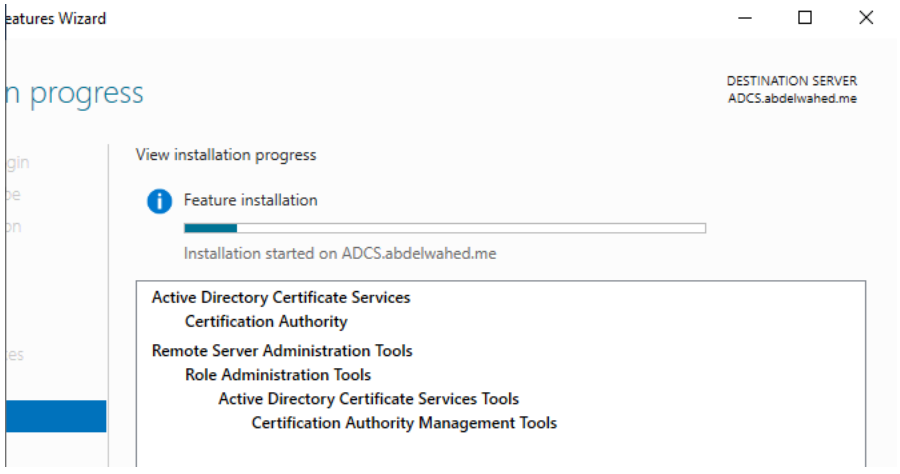
These types of CAs are not based on hierarchy, but rather on functionality and configuration storage. A standalone CA does not require AD DS and operates independently of it. An enterprise CA depends on AD DS, but it also offers several benefits, such as autoenrollment. The autoenrollment feature enables users and domain member devices to enroll for certificates automatically if you have configured automatic certificate enrollment through Group Policy.

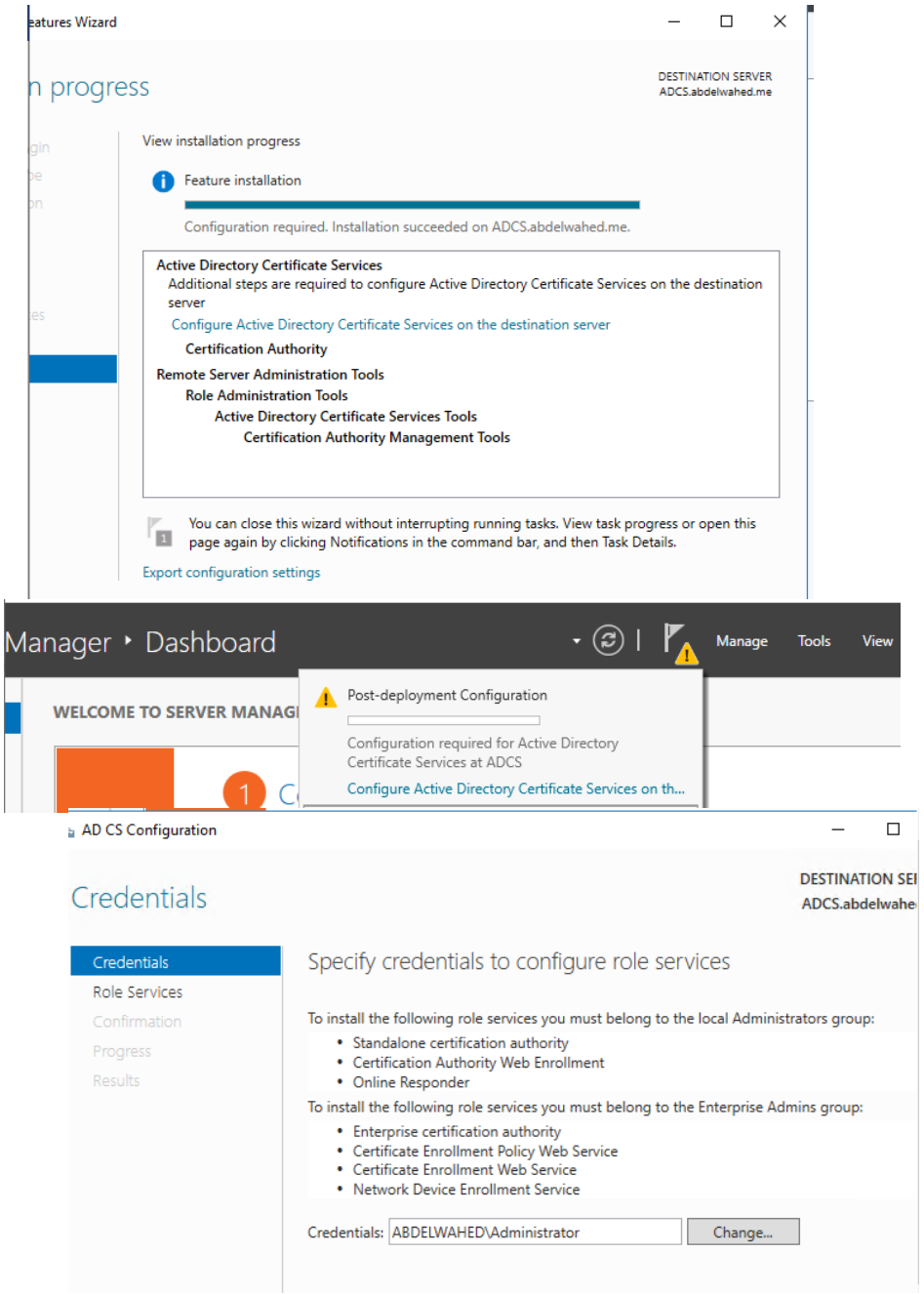
Please be aware that once AD CS is installed, the computer name and its domain affiliation are unchangeable.

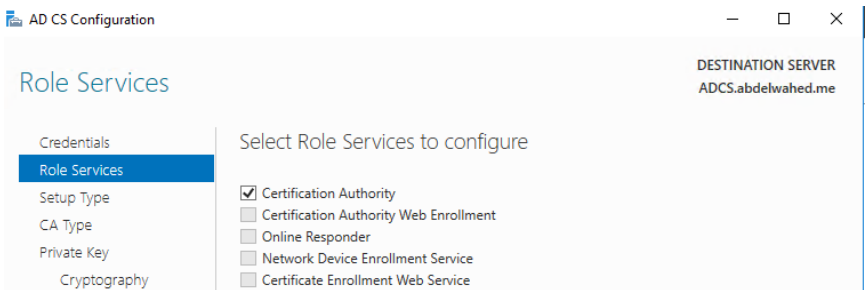
Install and Configure AD CS Role

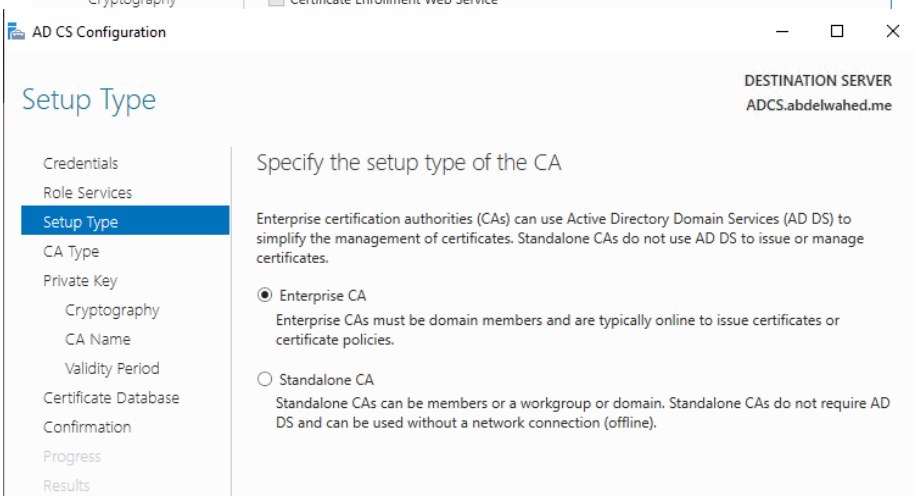


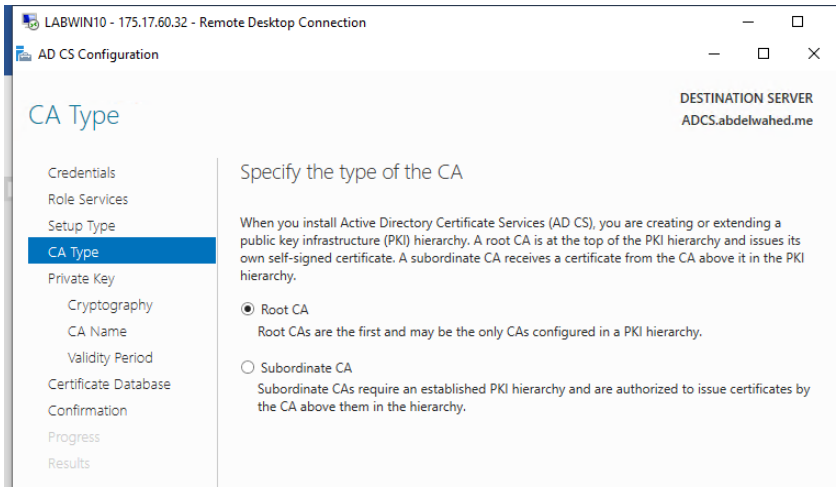


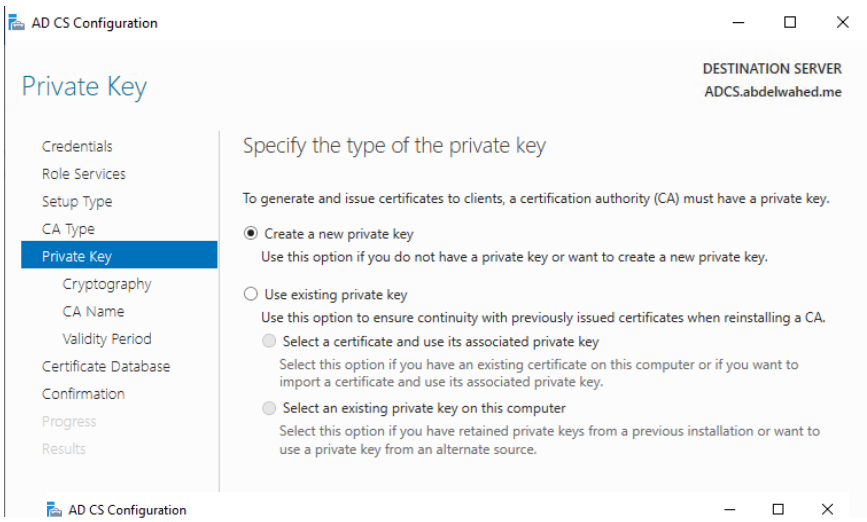


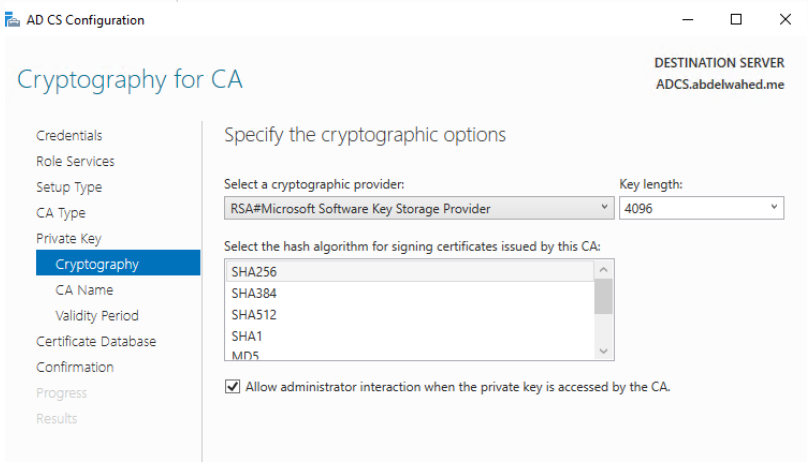

eatures Wizard
n progress
DESTINATION SERVER
ADCS.abdelwahed.me
View installation progress
Feature installation
Configuration required. Installation succeeded on ADCS.abdelwahed.me.
Active Directory Certificate Services
Additional steps are required to configure Active Directory Certificate Services on the destination server
Configure Active Directory Certificate Services on the destination server
Certification Authority
Remote Server Administration Tools
Role Administration Tools
Active Directory Certificate Services Tools
Certification Authority Management Tools
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
Manager ‣ Dashboard
Manage
Tools
View
WELCOME TO SERVER MANAGE
Post-deployment Configuration
Configuration required for Active Directory Certificate Services at ADCS
Configure Active Directory Certificate Services on th...
AD CS Configuration
Credentials
DESTINATION SE
ADCS.abdelwahe
Credentials
Role Services
Confirmation
Progress
Results
Specify credentials to configure role services
To install the following role services you must belong to the local Administrators group:
Standalone certification authority
Certification Authority Web Enrollment
Online Responder
To install the following role services you must belong to the Enterprise Admins group:
Enterprise certification authority
Certificate Enrollment Policy Web Service
Certificate Enrollment Web Service
Network Device Enrollment Service
Credentials:
ABDELWAHED\Administrator
Change...


AD CS Configuration
Role Services
DESTINATION SERVER
ADCS.abdelwahed.me
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
Select Role Services to configure
Certification Authority
Certification Authority Web Enrollment
Online Responder
Network Device Enrollment Service
Certificate Enrollment Web Service

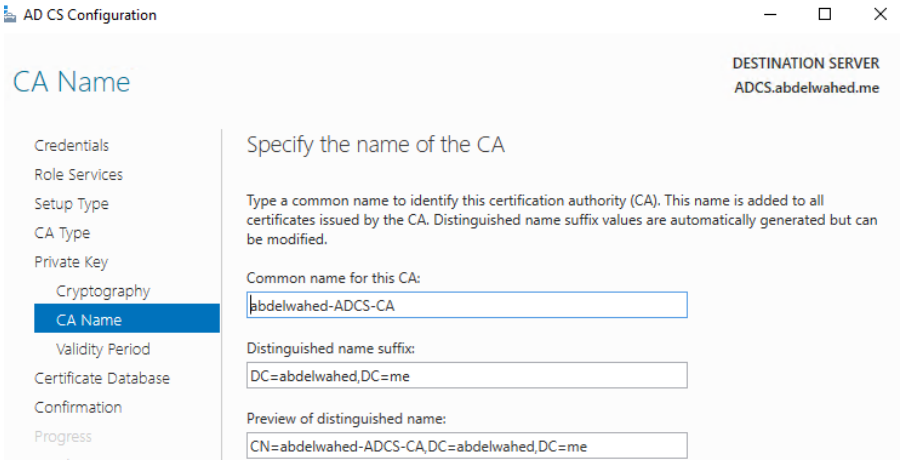

AD CS Configuration
Setup Type
DESTINATION SERVER
ADCS.abdelwahed.me
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Specify the setup type of the CA
Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.
Enterprise CA
Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.
Standalone CA
Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).


LABWIN10 - 175.17.60.32 - Remote Desktop Connection
AD CS Configuration
CA Type
DESTINATION SERVER
ADCS.abdelwahed.me
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Specify the type of the CA
When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.
Root CA
Root CAs are the first and may be the only CAs configured in a PKI hierarchy.
Subordinate CA
Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.

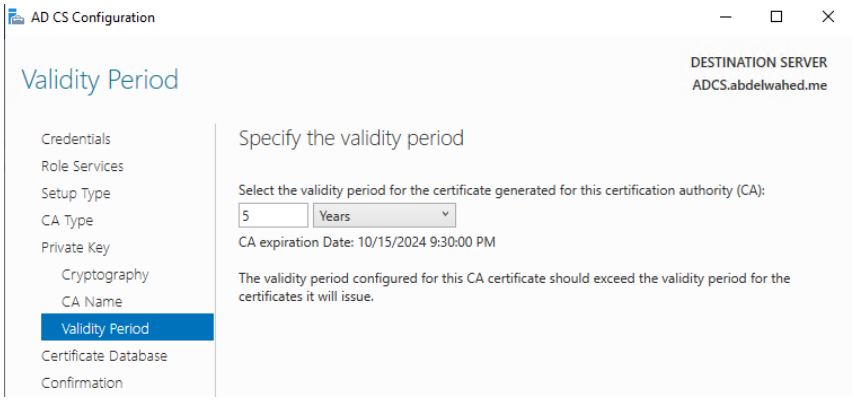


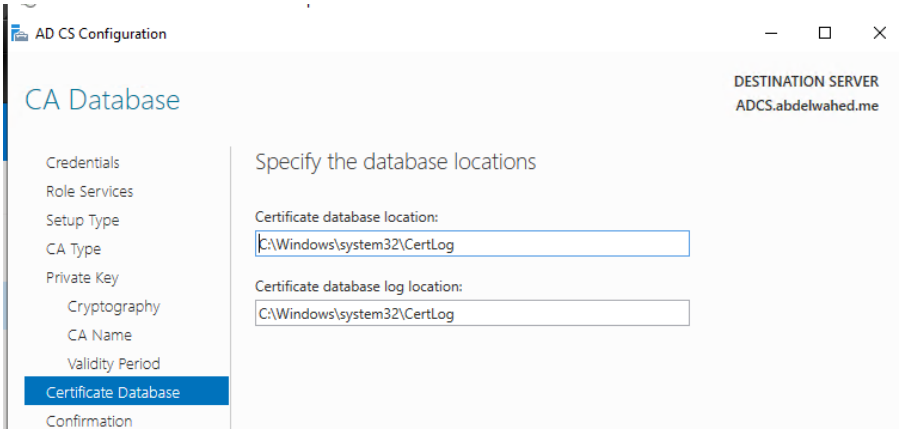


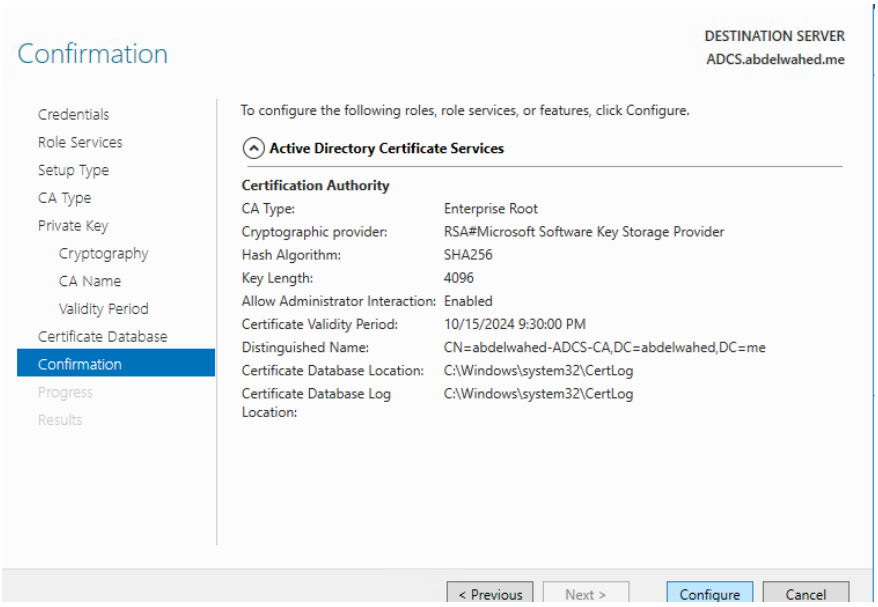
The feature permits administrators to modify the private key post-installation.



The CA certificate server is valid for 5 years, and the validity period can be extended.

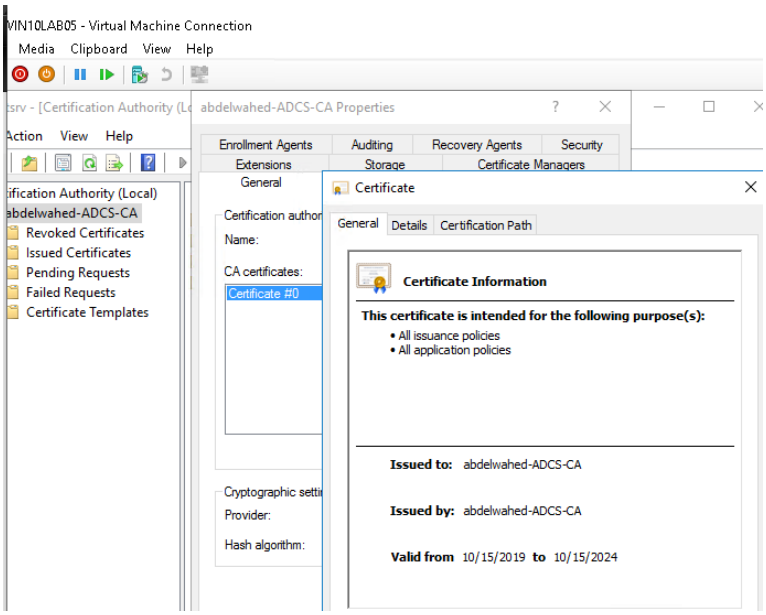


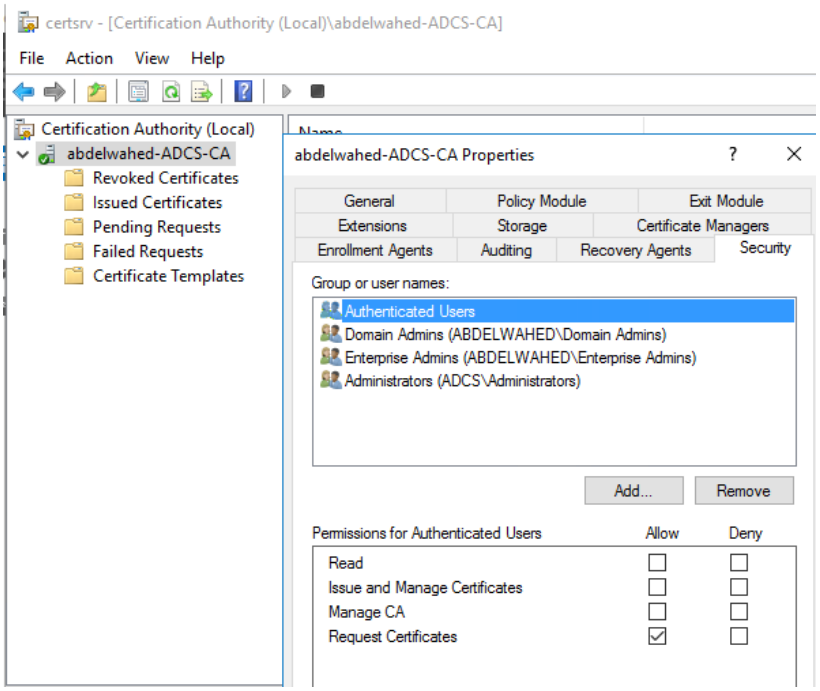




Configuring CA properties like security and Certificate Managers

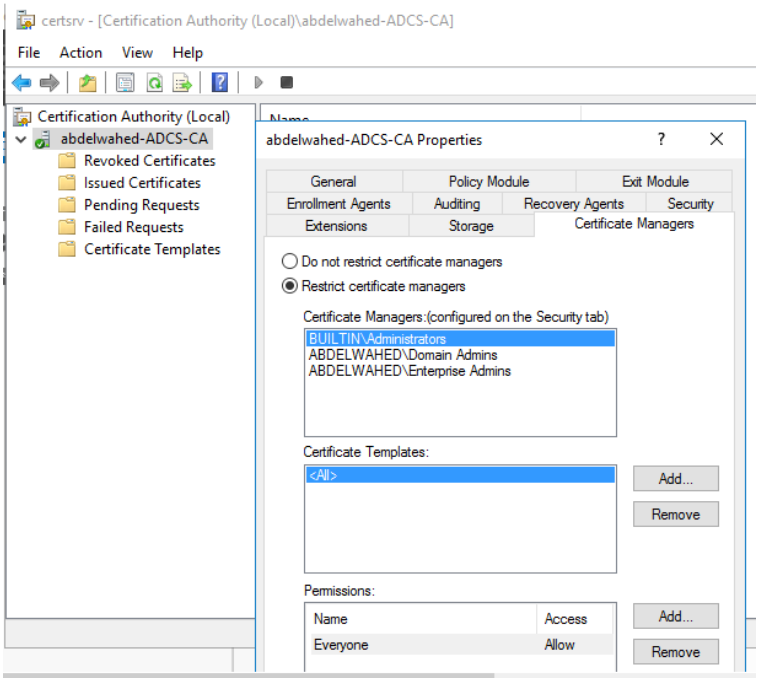
Server (CA)certificate





Restrict Certificate Managers

A certificate manager has the authority to sanction requests for certificate enrollment and revocation, distribute certificates, and oversee their administration. This responsibility can be delegated by giving a user or group the specific permission to Issue and Manage Certificates.



Troubleshooting and Maintaining CAs

Common AD CS issues

The following list describes common AD CS issues that you might encounter:

- Users or computers do not automatically enroll for certificates as expected:
  - Because you enable autoenrollment through Group Policy, you should verify that the GPOs that enable autoenrollment for users and computers are applying autoenrollment correctly and that the user or computer is not in an organizational unit (OU) where policy inheritance has been blocked or overridden by another GPO. Both the user and computer must be enabled separately, although both settings can reside in the same GPO.
  - You should verify that AD CS is publishing the certificate template to an enterprise CA that can be accessed by the computer or user.
  - You should verify that the computer or user have the Request Certificates permission on the CA and the Autoenroll permission on the certificate template in question.
  - You should verify that the requested certificate template does not require information that AD DS cannot supply automatically.
- You cannot configure autoenrollment permissions on a template. For you to configure autoenrollment against a certificate, the template must be version 2 or later. You can only add version 2 templates to a CA that is running Windows Server 2008 Enterprise or later.
- The enterprise CA option is unavailable. This occurs when a user who is not a member of the **Enterprise Admins** or **Domain Admins** group installs a CA; as such, the CA might not install as an enterprise CA. In this case, the enterprise CA option is unavailable, and information about the CA cannot automatically publish to AD DS.
- You receive an error when accessing CA web enrollment pages. This occurs while accessing CA

webpages. In this case, you should ensure that the user is a member of the **Administrators** or **Power Users** group on the client computer.
• The enrollment agent is restricted. This occurs when an enrollment agent cannot enroll on behalf of a user for a specific certificate template. This might occur because of the restrictions that were configured on the enrollment agent or the lack of enrollment permissions on the certificate template.

Troubleshooting validation issues

All certificates have a validity period. After the validity period expires, the certificate is no longer an acceptable credential. Client computers might not be able to connect to resources that require certificates if any certificate validation problems occur.

Renew a CA certificate

A CA also has its own certificate. A root CA issues a certificate for itself, a self-signed certificate, while subordinate CAs get their certificates from a root CA. Every CA certificate has a validity period. Usually, when deploying a root CA, IT administrators choose to set the validity period of the root CA certificate for five years or more. You need to renew a CA certificate when the validity period is close to the expiration date. A CA with an expired certificate cannot work, therefore, you should not let the CA certificate expire.

Moving a root CA to another computer

CAs are designed and configured to work for many years, during which time you might want to upgrade the hardware and operating system that supports the CA. Such scenarios usually require that you move a CA from one computer to another. In general, the procedure for moving a CA can be divided into two phases:
• CA backup
• CA restore

Performing a CA backup before a move

You should have a CA backup even if you are not moving a CA to another computer. A CA backup is different from ordinary backup scenarios. To perform a CA backup before moving a CA to another computer, you should perform the following procedure:
1. If you are backing up an enterprise CA, click the **Certificate Templates** item in the **Certification Authority** console, and then record the names of the listed certificate templates. These templates are in AD DS, so you do not have to back them up. You must note which templates you have published on the CA that you are moving because you will have to add them manually after you move the CA.
2. In the **Certification Authority** console, right-click the CA name, click **All Tasks**, and then click **Backup CA** to start the **Certification Authority Backup Wizard**. In the backup wizard, you have the option to make a backup of the private key and the CA certificate, as well as the certificate database and certificate database log. You also have to provide an appropriate location for the backup content. You should protect a CA private key with a password for security reasons.
3. After the backup is complete, you should open **Registry Editor**.
4. Locate and export the following registry subkey, located at:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration
Note: We recommend that you save this registry key to a file in the same folder with the CA backup from the previous step.

Before you begin the restore procedure, confirm that the *%SystemRoot%* folder of the target server matches the *%SystemRoot%* folder of the server from which you took the backup. Additionally, the location of the CA restore must match the location of the CA backup. For example, if you back up the CA from the **D:\Winnt\System32\Certlog** folder, you must restore the backup to the **D:\Winnt\System32\Certlog** folder. After you restore the backup, you can move the CA database files to a different location.

Performing a CA restore on a new computer

After you successfully finalize the backup procedure, you have to restore the CA on another computer. The new CA should have the same name as the old CA. To restore the CA, perform the following procedure:

1. Install AD CS on the target computer. Select to install **Stand-alone** or **Enterprise** depending on the type of CA that you are moving. When you come to the **Set Up Private Key** page, click **Use existing private key**, and then choose to select a certificate and use its associated private key. This will provide you with the ability to use an existing certificate from an old CA.
2. On the **Select Existing Certificate** page, click **Import**, type the path of the **.p12** file in the backup folder, type the password that you chose in the previous procedure to protect the backup file, and then click **OK**. When prompted for **Public and Private Key Pair**, verify that **Use existing keys** is selected. This is very important because you want to keep the same root CA certificate.
3. When prompted on the **Certificate Database** page, specify the same location for the certificate database and certificate database log as on the previous CA computer. After you select all of these options, wait for the CA setup to finish.
4. After the setup is complete, open the **Services** snap-in to stop the AD CS service. You do that to restore settings from the old CA.
5. Locate the registry file that you saved in the backup procedure, and then double-click it to import the registry settings.
6. After you restore the registry settings, open the **Certification Authority** console, right-click the CA name, click **All Tasks**, and then click **Restore CA**. This will start the **Certification Authority Restore Wizard**. In the wizard, select the **Private key and CA certificate** and the **Certificate database and certificate database log** check boxes. This specifies that you want to restore these objects from a backup. Next, provide a backup folder location, and then verify the settings for the restore. The **Issued Log** and **Pending Requests** settings should display.
7. When the restore process completes, choose to restart the AD CS service.
8. If you restored an enterprise CA, restore the certificate templates from AD DS that you recorded in the previous procedure

Monitoring CA operations

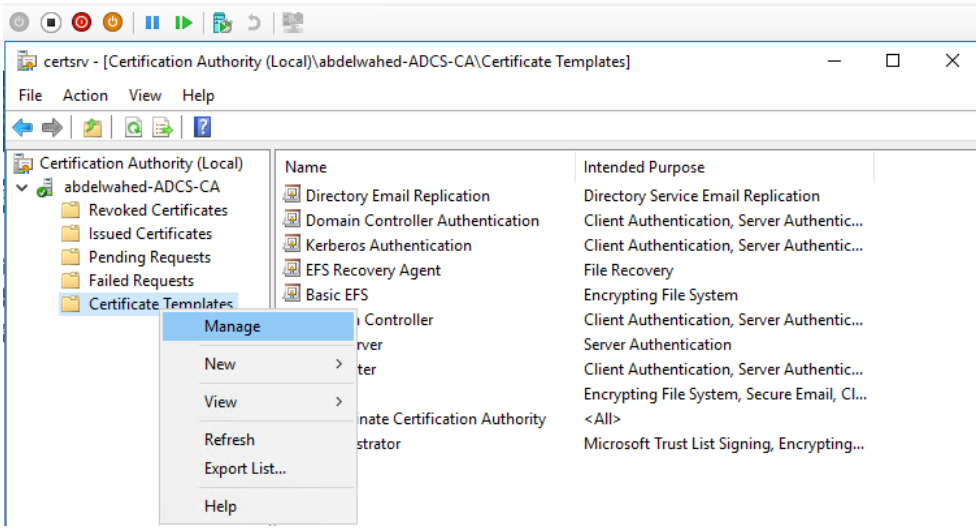
through **PKIView** console this tool installed by default when we install CS.

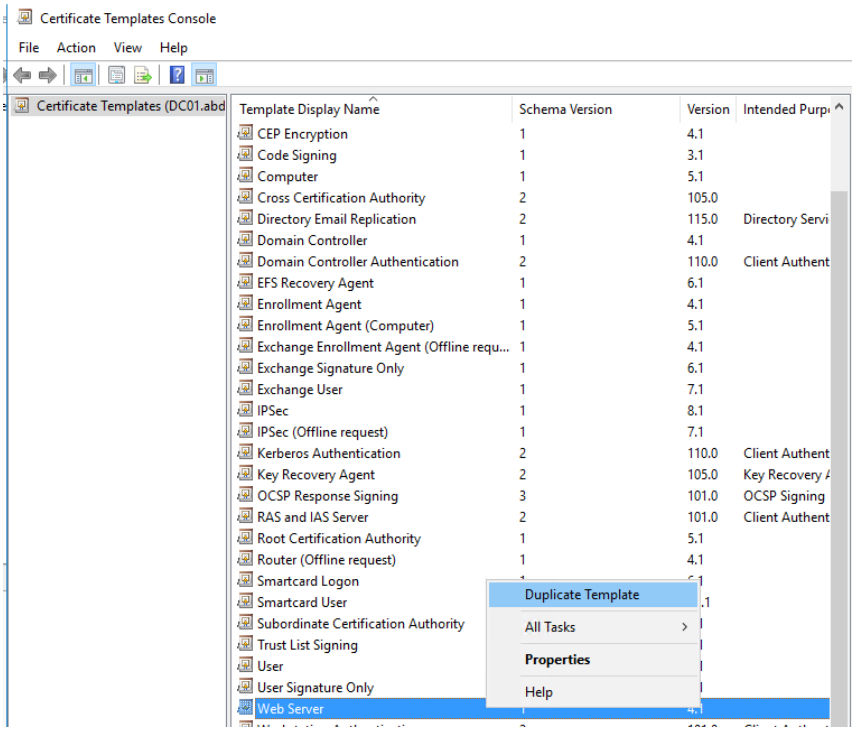
Auditing CA events

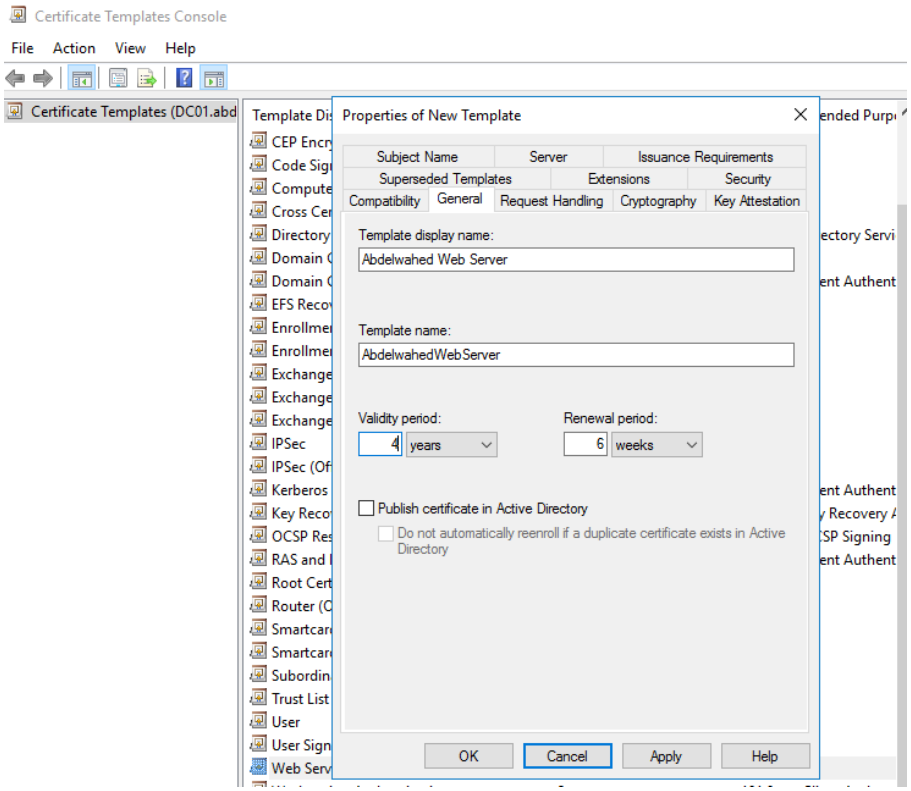
Through CA properties then select audit tab.

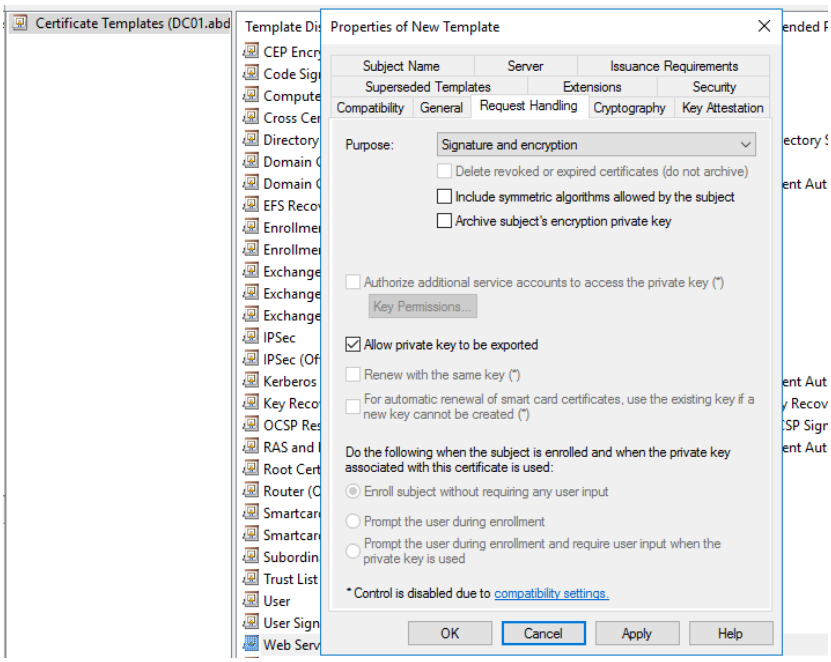
Certificate Templates (Create create for web server) so computers can request it

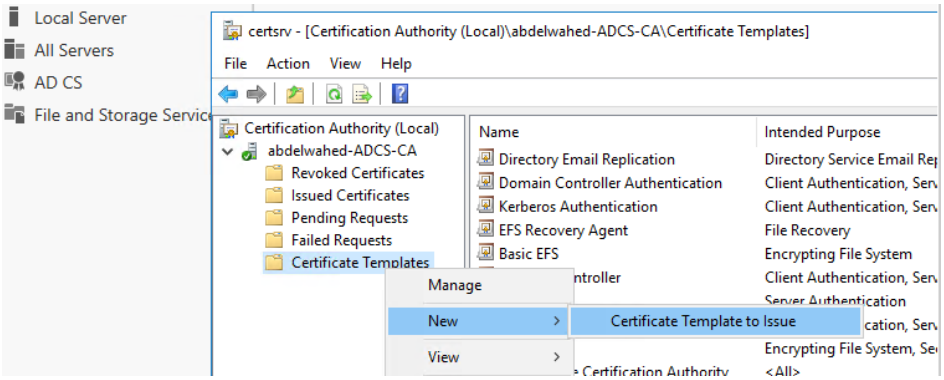
Certificate Template

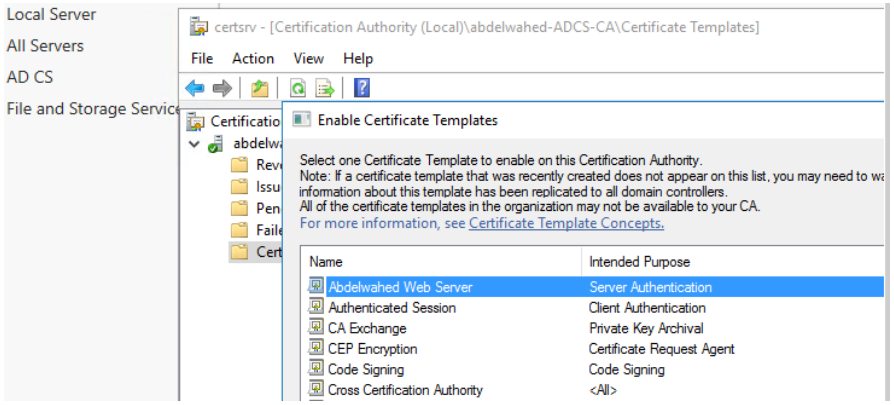


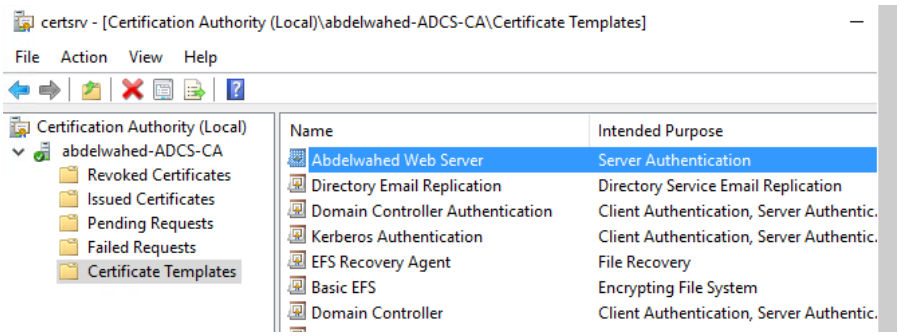



Certificate Templates Console
File Action View Help
Certificate Templates (DC01.abd
Properties of New Template
Subject Name Server Issuance Requirements
Superseded Templates Extensions Security
Compatibility General Request Handling Cryptography Key Attestation
Template display name:
Abdelwahed Web Server
Template name:
AbdelwahedWebServer
Validity period:
4 years
Renewal period:
6 weeks
Publish certificate in Active Directory
Do not automatically reenroll if a duplicate certificate exists in Active Directory
OK Cancel Apply Help

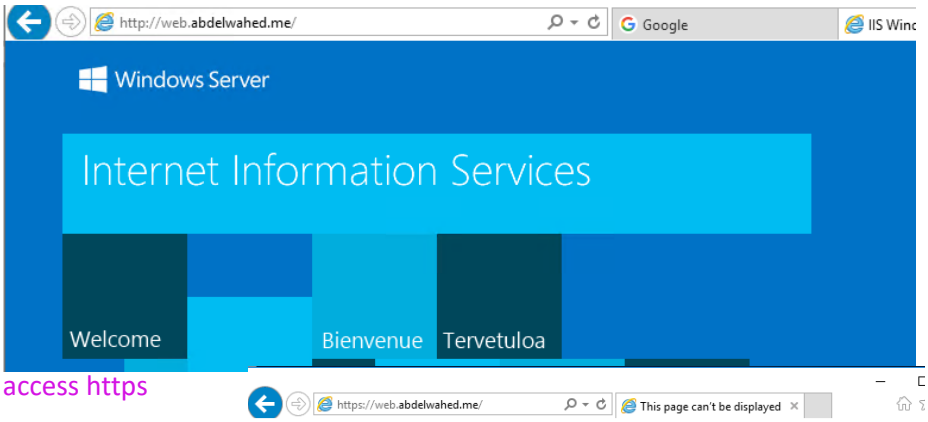

Certificate Templates (DC01.abd
Properties of New Template
Subject Name Server Issuance Requirements
Superseded Templates Extensions Security
Compatibility General Request Handling Cryptography Key Attestation
Purpose: Signature and encryption
Delete revoked or expired certificates (do not archive)
Include symmetric algorithms allowed by the subject
Archive subject's encryption private key
Authorize additional service accounts to access the private key (*)
Key Permissions...
Allow private key to be exported
Renew with the same key (*)
For automatic renewal of smart card certificates, use the existing key if a new key cannot be created (*)
Do the following when the subject is enrolled and when the private key associated with this certificate is used:
Enroll subject without requiring any user input
Prompt the user during enrollment
Prompt the user during enrollment and require user input when the private key is used
* Control is disabled due to compatibility settings.
OK Cancel Apply Help







Now we can test this certificate by requesting it from another IIS Server as demonstrated below.

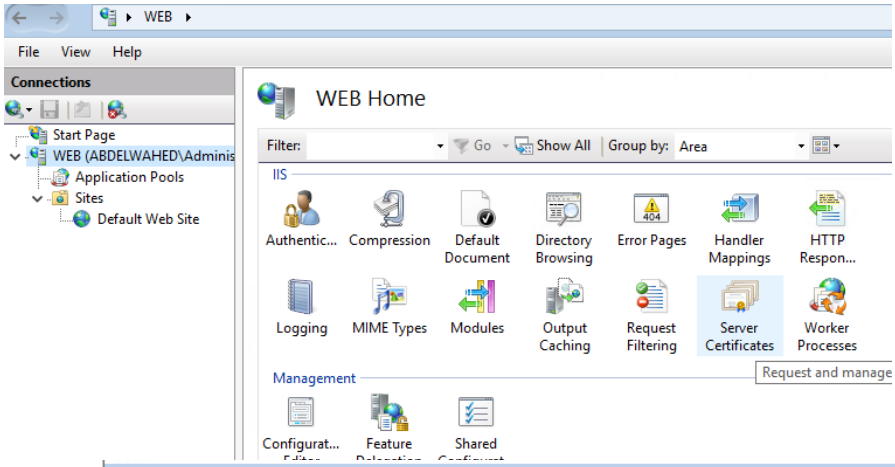


If you try to access https

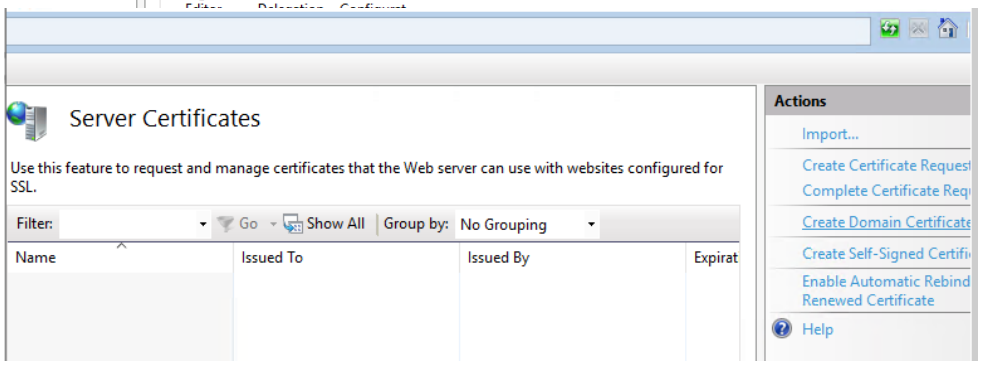
This page can't be displayed

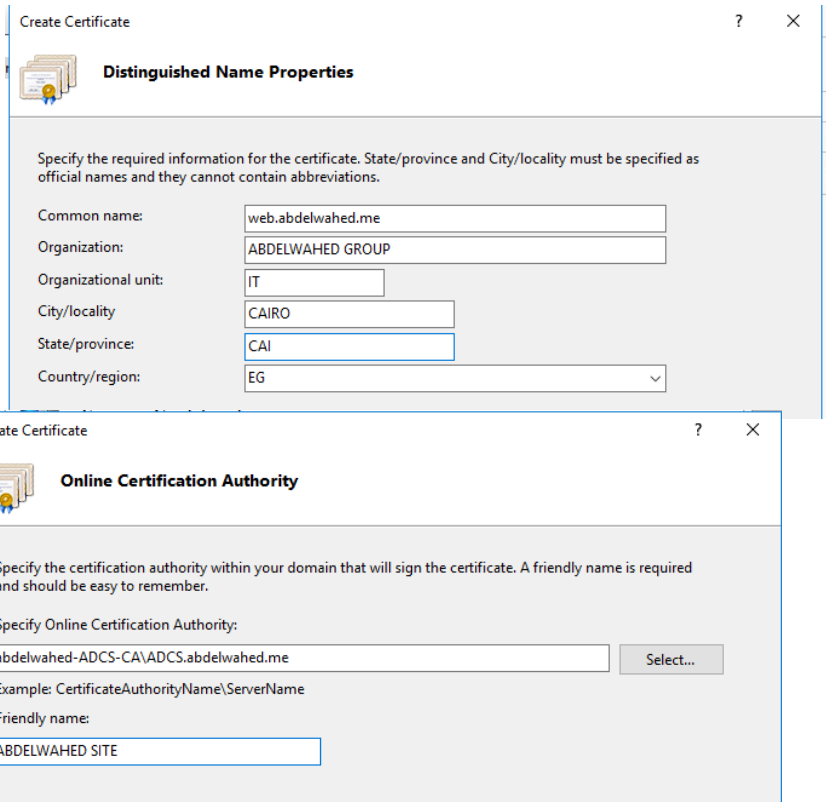
- Make sure the web address https://web.abdelwahed.me is correct.
- Look for the page with your search engine.
- Refresh the page in a few minutes.

Go to IIS

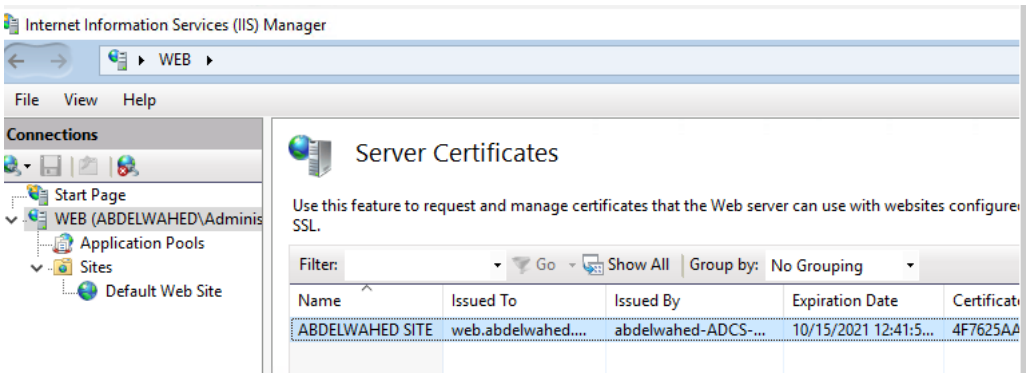


Next, choose 'Create Domain Certificate' from the right panel.

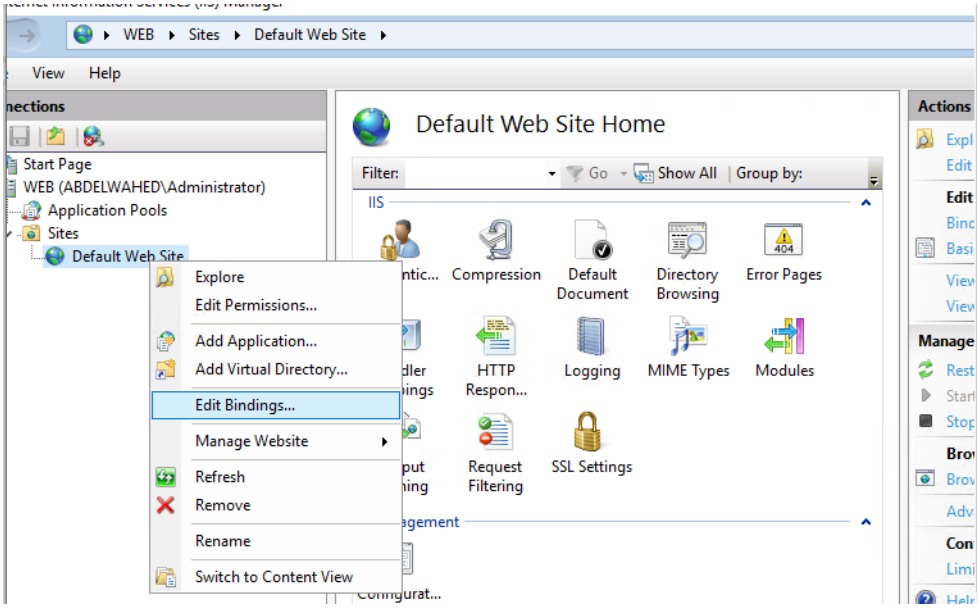


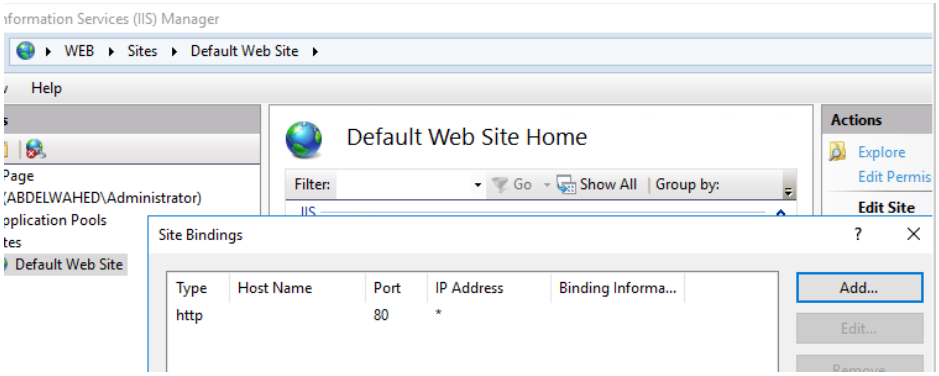


NOW CERTIFICATE ISSUED TO THE WEB SERVER AS SHOWN DOWN

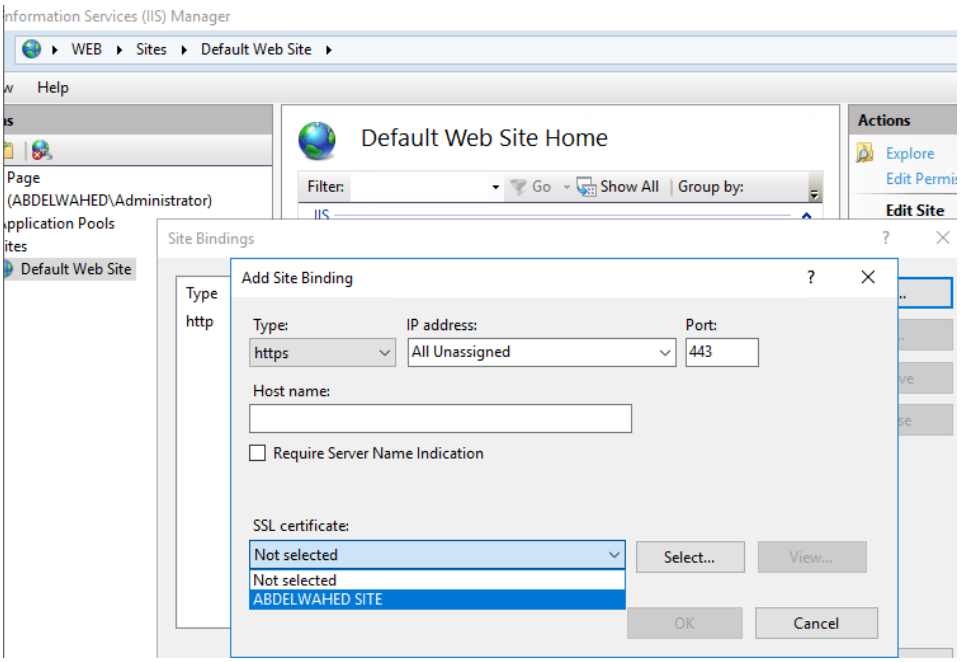


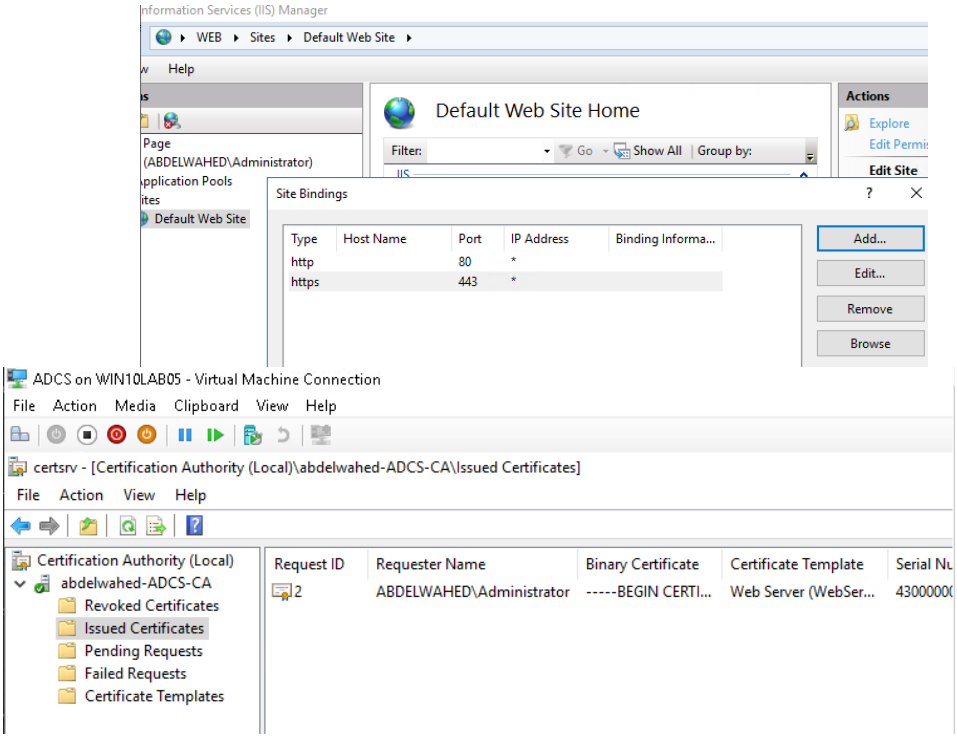
NOW CONFIGURE HTTPS OPTIONS TO THE SITE





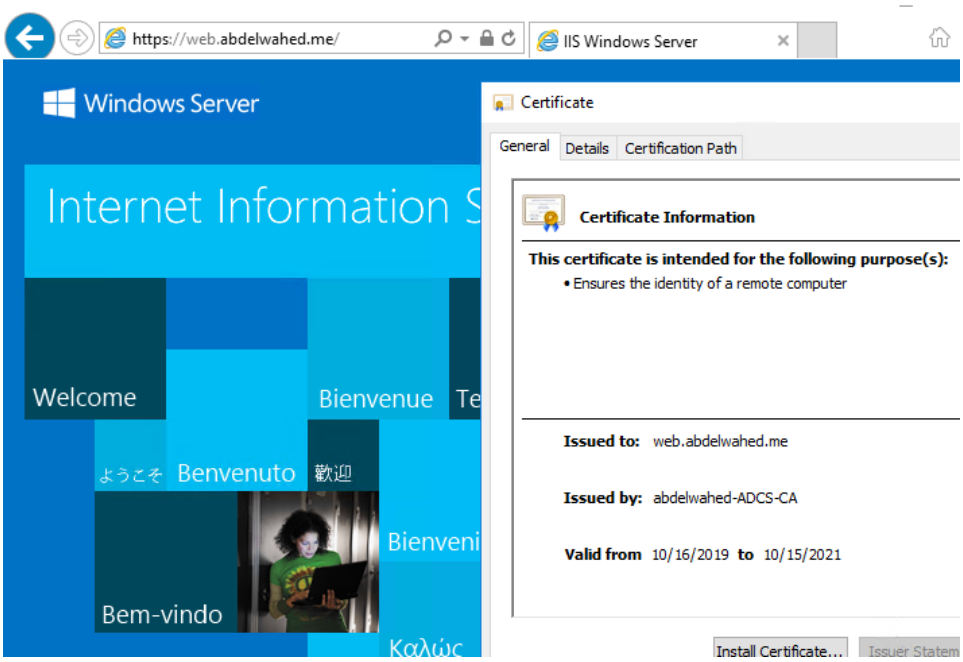
SELECT ADD THEN SELECT CERTIFICATE WE JUST REQUESTED

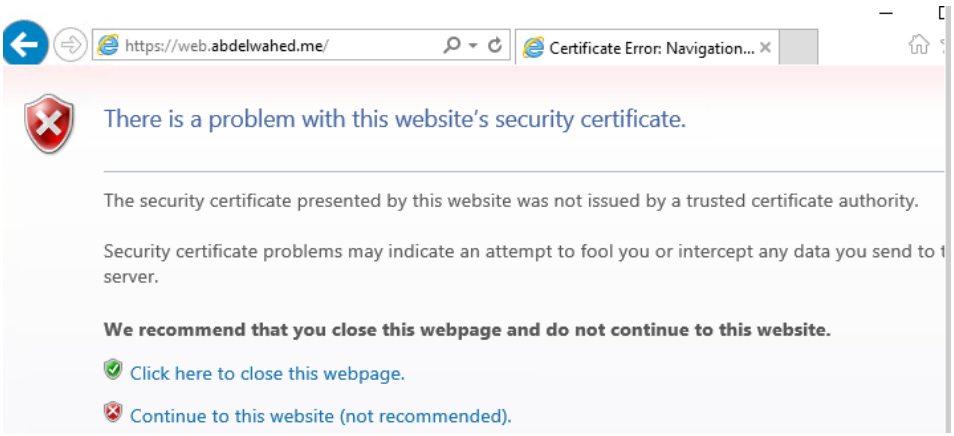




NOW WE CAN ACCESS THE WEB SERVER THROUGH HTTPS – FROM THE SAME SERVER-

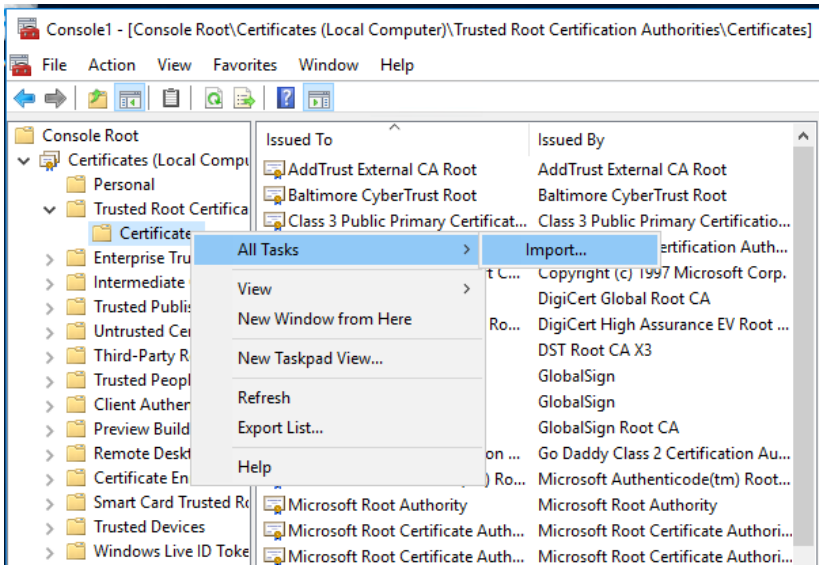
---

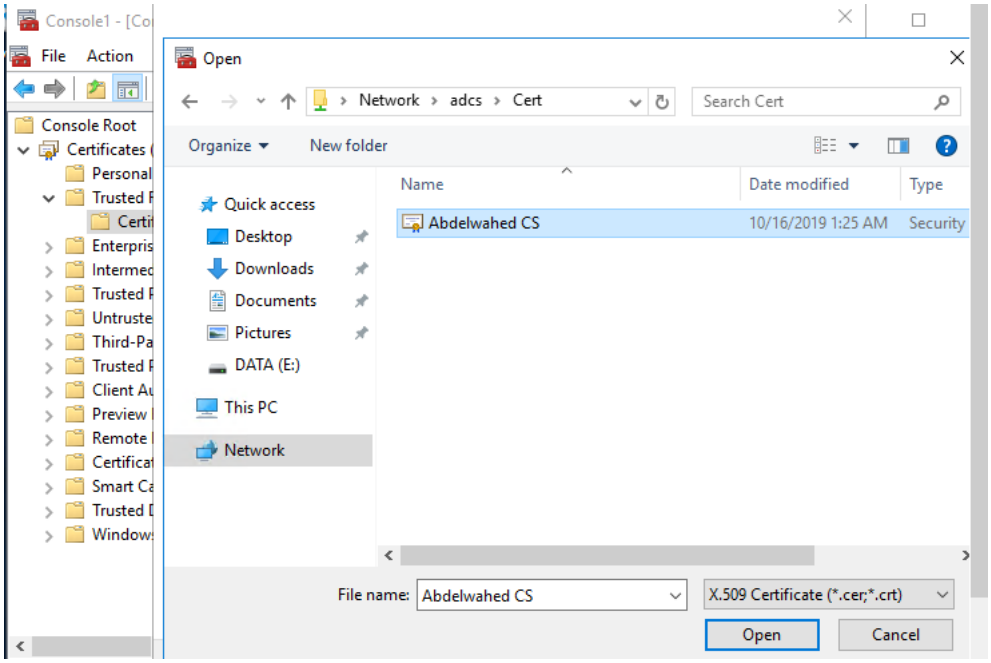

https://web.abdelwahed.me/
IIS Windows Server
Windows Server
Internet Information S
Welcome
Bienvenue
Te
ようこそ
Benvenuto
歡迎
Bienveni
Bem-vindo
Καλώς
Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer
Issued to: web.abdelwahed.me
Issued by: abdelwahed-ADCS-CA
Valid from 10/16/2019 to 10/15/2021
Install Certificate...
Issuer Statem

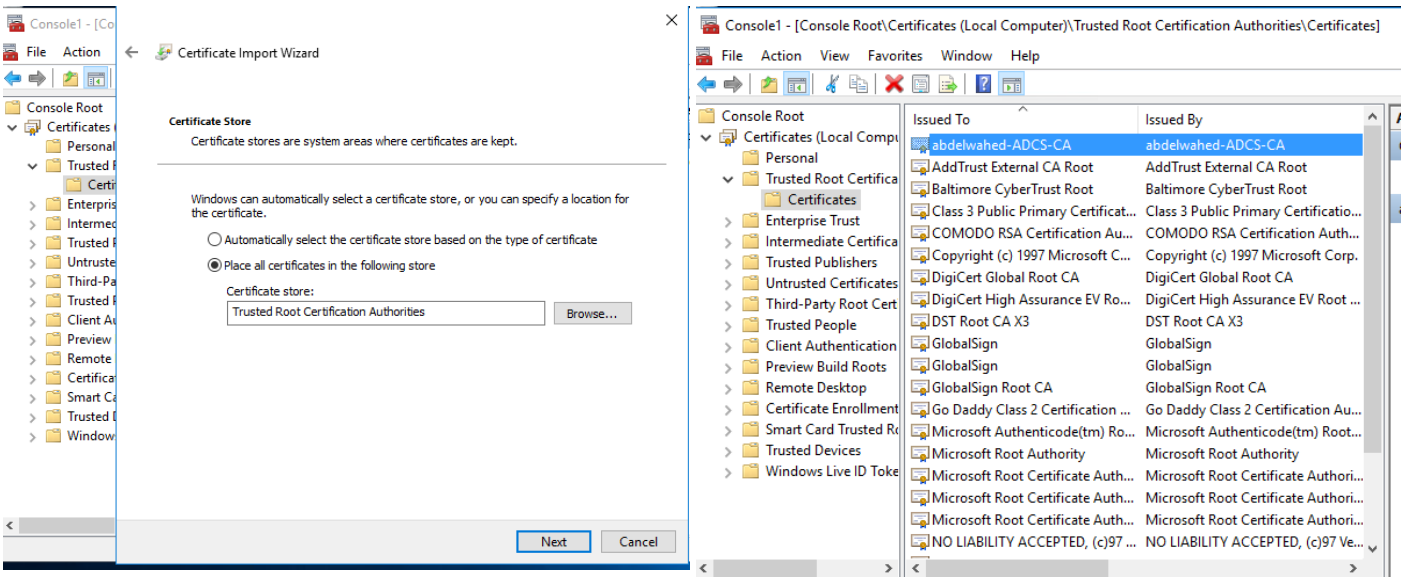

https://web.abdelwahed.me/
Certificate Error: Navigation...
There is a problem with this website's security certificate.
The security certificate presented by this website was not issued by a trusted certificate authority.
Security certificate problems may indicate an attempt to fool you or intercept any data you send to t
server.
We recommend that you close this webpage and do not continue to this website.
Click here to close this webpage.
Continue to this website (not recommended).

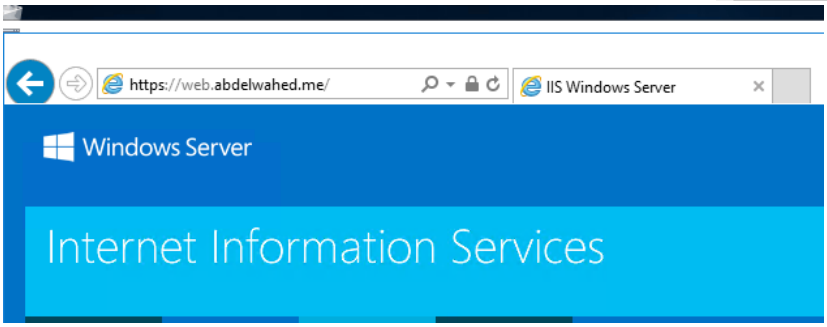
Add our AD CS server as trusted root CA

First you must export AD CS certificate and share it so you can access it from another server





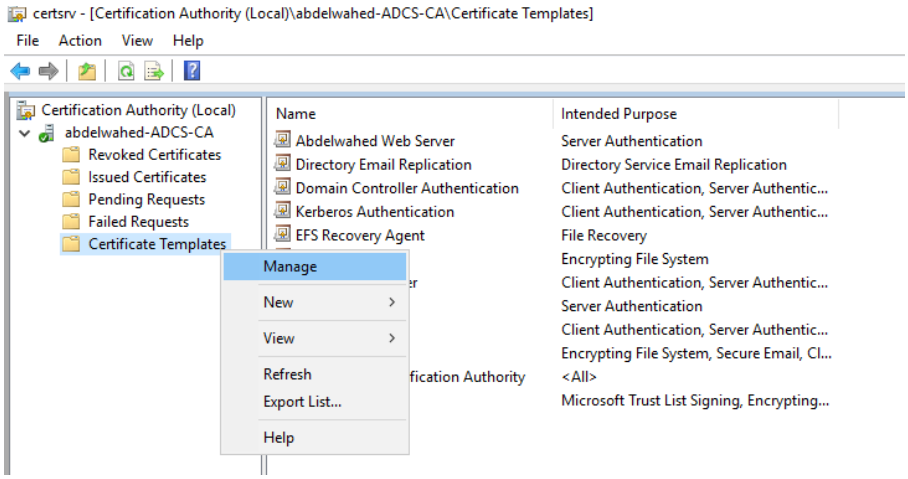


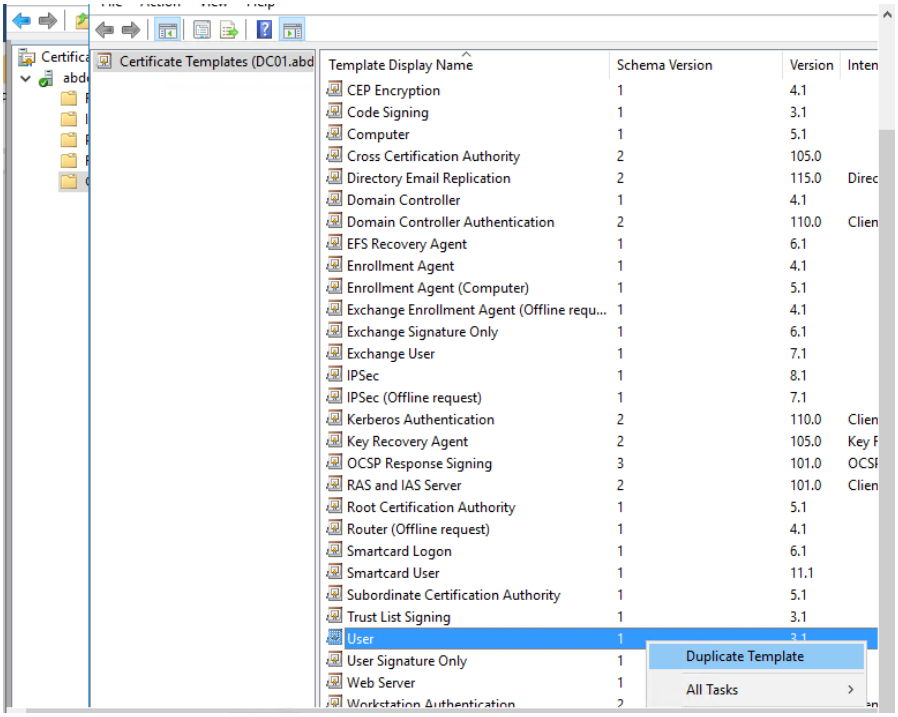


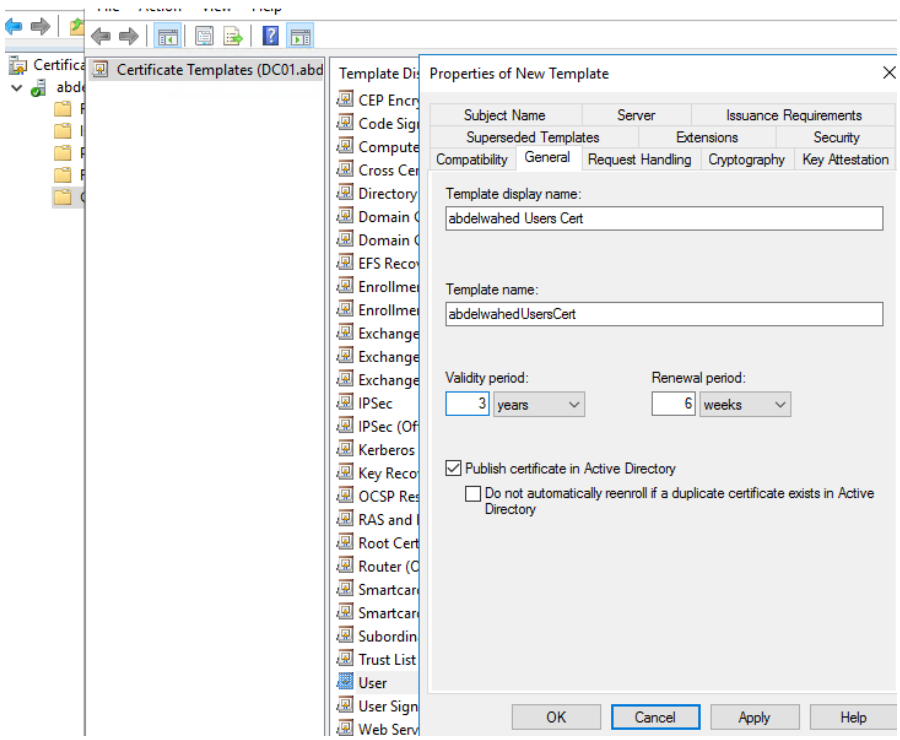
Now there are no error messages.

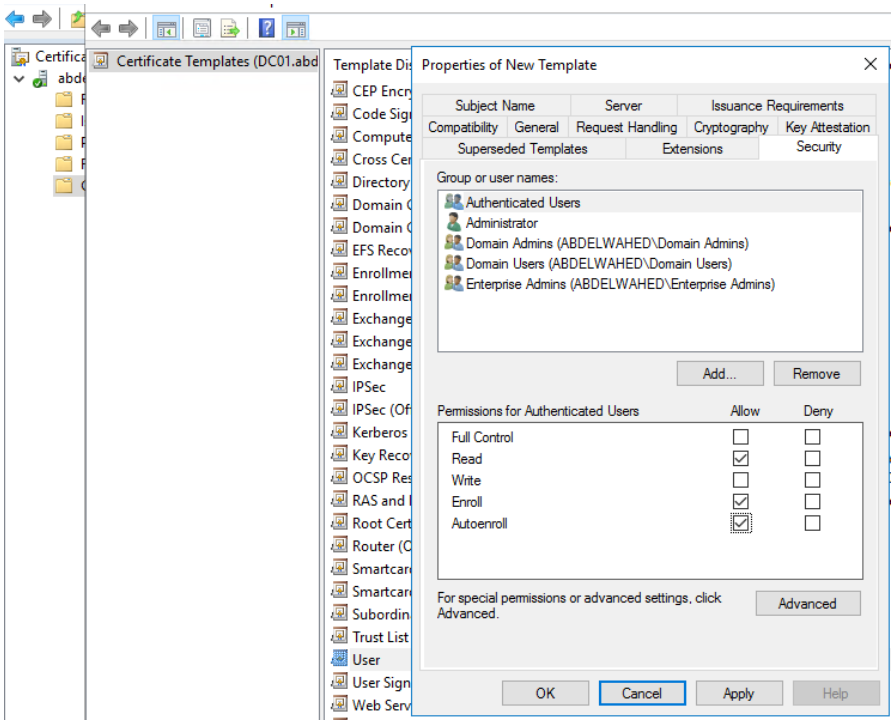
Set up automatic certificate enrollment for users.

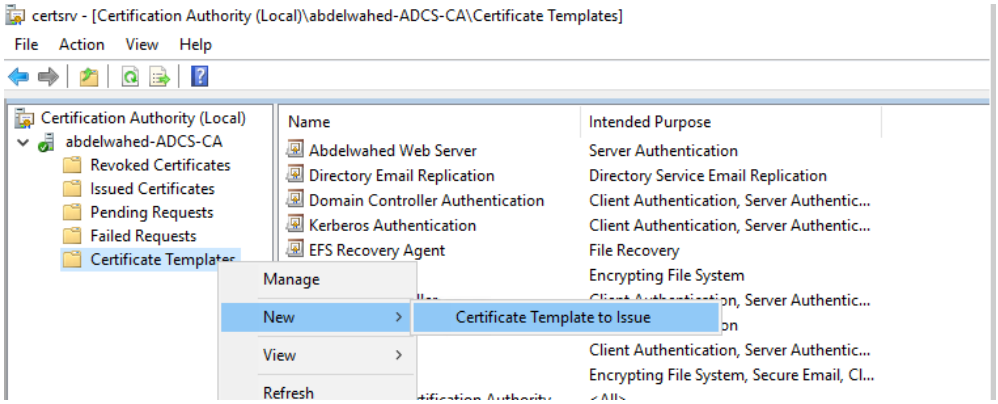
Initially, generate a user certificate template in the Certification Authority.

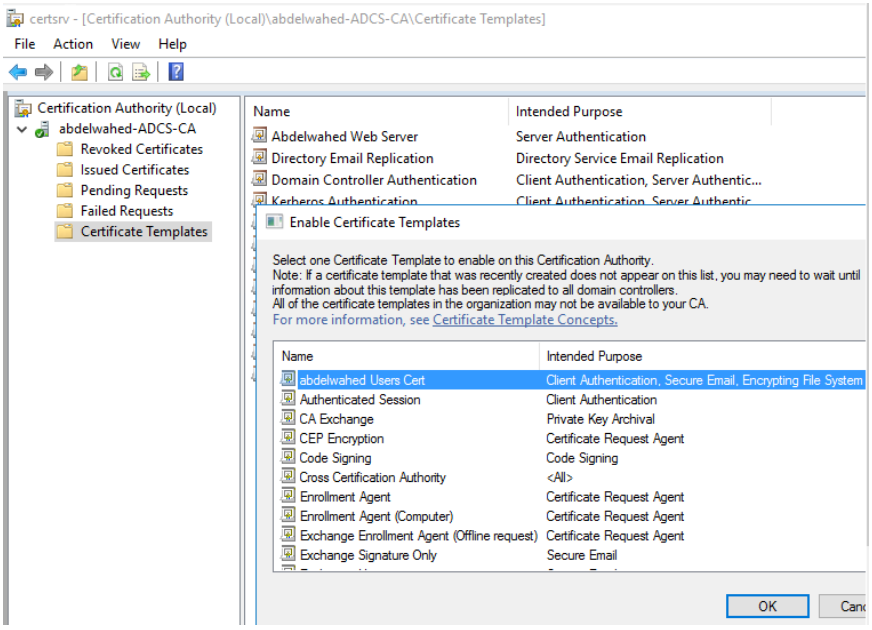


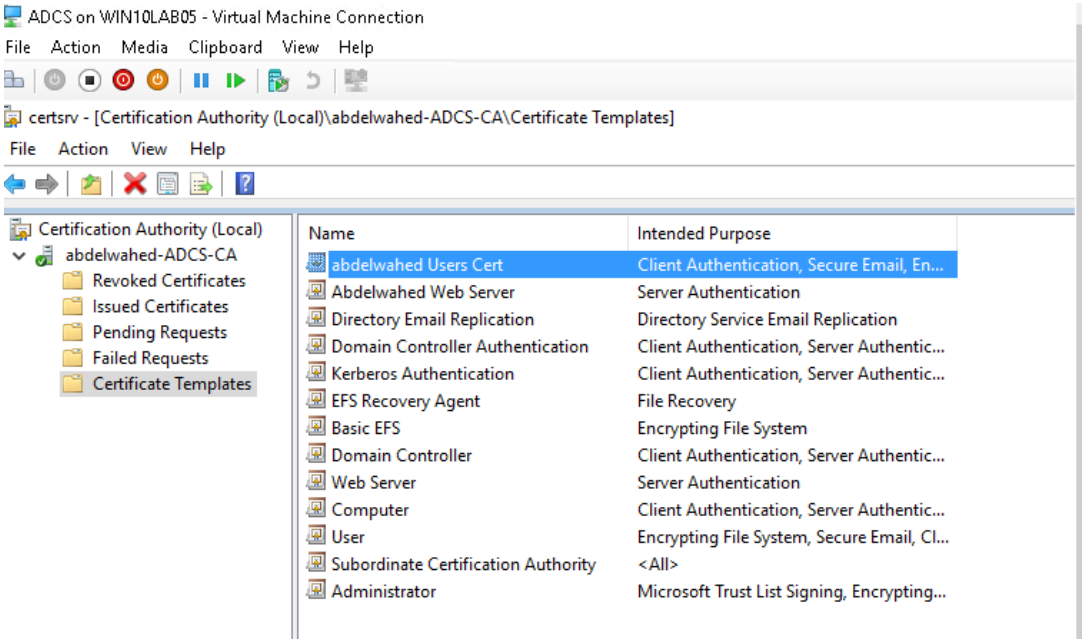

Certificate Templates (DC01.abd
Template Display Name
Schema Version
Version
CEP Encryption 1 4.1
Code Signing 1 3.1
Computer 1 5.1
Cross Certification Authority 2 105.0
Directory Email Replication 2 115.0
Domain Controller 1 4.1
Domain Controller Authentication 2 110.0
EFS Recovery Agent 1 6.1
Enrollment Agent 1 4.1
Enrollment Agent (Computer) 1 5.1
Exchange Enrollment Agent (Offline requ... 1 4.1
Exchange Signature Only 1 6.1
Exchange User 1 7.1
IPSec 1 8.1
IPSec (Offline request) 1 7.1
Kerberos Authentication 2 110.0
Key Recovery Agent 2 105.0
OCSP Response Signing 3 101.0
RAS and IAS Server 2 101.0
Root Certification Authority 1 5.1
Router (Offline request) 1 4.1
Smartcard Logon 1 6.1
Smartcard User 1 11.1
Subordinate Certification Authority 1 5.1
Trust List Signing 1 3.1
User 1
User Signature Only 1
Web Server 1
Duplicate Template
All Tasks


Certificate Templates (DC01.abd
Properties of New Template
Subject Name
Server
Issuance Requirements
Superseded Templates
Extensions
Security
Compatibility
General
Request Handling
Cryptography
Key Attestation
Template display name:
abdelwahed Users Cert
Template name:
abdelwahedUsersCert
Validity period:
3
years
Renewal period:
6
weeks
Publish certificate in Active Directory
Do not automatically reenroll if a duplicate certificate exists in Active Directory
OK
Cancel
Apply
Help


Certificate Templates (DC01.abd
Template Dis
Properties of New Template
Subject Name
Server
Issuance Requirements
Compatibility
General
Request Handling
Cryptography
Key Attestation
Superseded Templates
Extensions
Security
Group or user names:
Authenticated Users
Administrator
Domain Admins (ABDELWAHED\Domain Admins)
Domain Users (ABDELWAHED\Domain Users)
Enterprise Admins (ABDELWAHED\Enterprise Admins)
Add...
Remove
Permissions for Authenticated Users
Allow
Deny
Full Control
Read
Write
Enroll
Autoenroll
For special permissions or advanced settings, click Advanced.
Advanced
OK
Cancel
Apply
Help

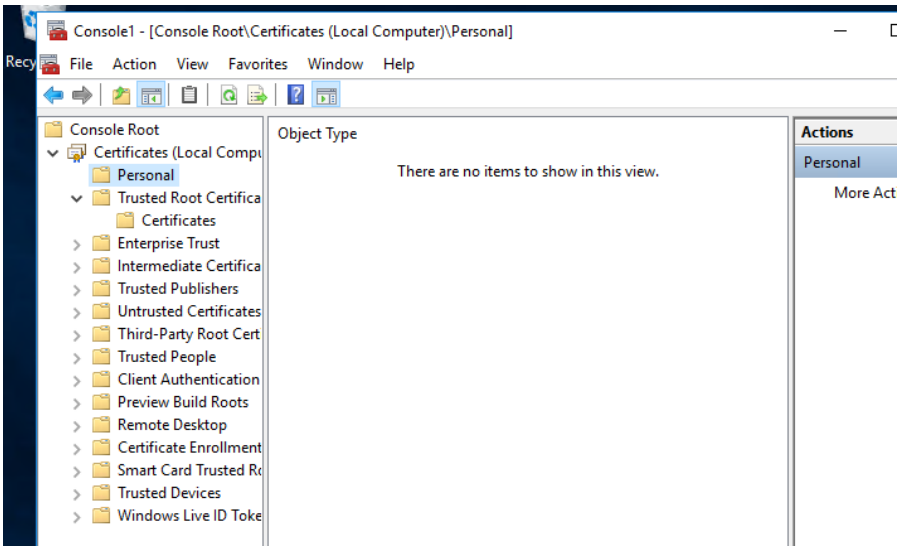

certsrv - [Certification Authority (Local)\abdelwahed-ADCS-CA\Certificate Templates]
File
Action
View
Help
Certification Authority (Local)
abdelwahed-ADCS-CA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
Name
Intended Purpose
Abdelwahed Web Server
Server Authentication
Directory Email Replication
Directory Service Email Replication
Domain Controller Authentication
Client Authentication, Server Authentic...
Kerberos Authentication
Client Authentication, Server Authentic...
EFS Recovery Agent
File Recovery
Encrypting File System
Manage
New
Certificate Template to Issue
View
Refresh
Client Authentication, Server Authentic...
Encrypting File System, Secure Email, Cl...

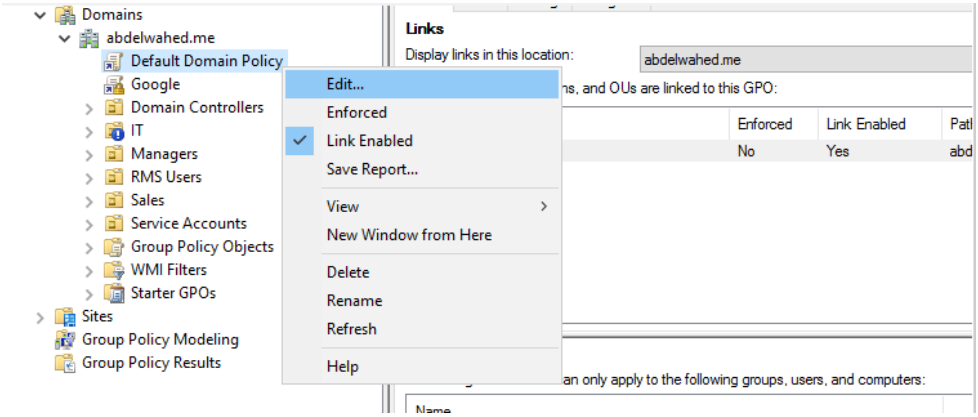

certsrv - [Certification Authority (Local)\abdelwahed-ADCS-CA\Certificate Templates]
File Action View Help
Certification Authority (Local)
abdelwahed-ADCS-CA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
Name
Intended Purpose
Abdelwahed Web Server
Server Authentication
Directory Email Replication
Directory Service Email Replication
Domain Controller Authentication
Client Authentication, Server Authentic...
Enable Certificate Templates
Select one Certificate Template to enable on this Certification Authority.
Note: If a certificate template that was recently created does not appear on this list, you may need to wait until information about this template has been replicated to all domain controllers.
All of the certificate templates in the organization may not be available to your CA.
For more information, see Certificate Template Concepts.
Name
Intended Purpose
abdelwahed Users Cert
Client Authentication, Secure Email, Encrypting File System
Authenticated Session
Client Authentication
CA Exchange
Private Key Archival
CEP Encryption
Certificate Request Agent
Code Signing
Code Signing
Cross Certification Authority
<All>
Enrollment Agent
Certificate Request Agent
Enrollment Agent (Computer)
Certificate Request Agent
Exchange Enrollment Agent (Offline request)
Certificate Request Agent
Exchange Signature Only
Secure Email
OK

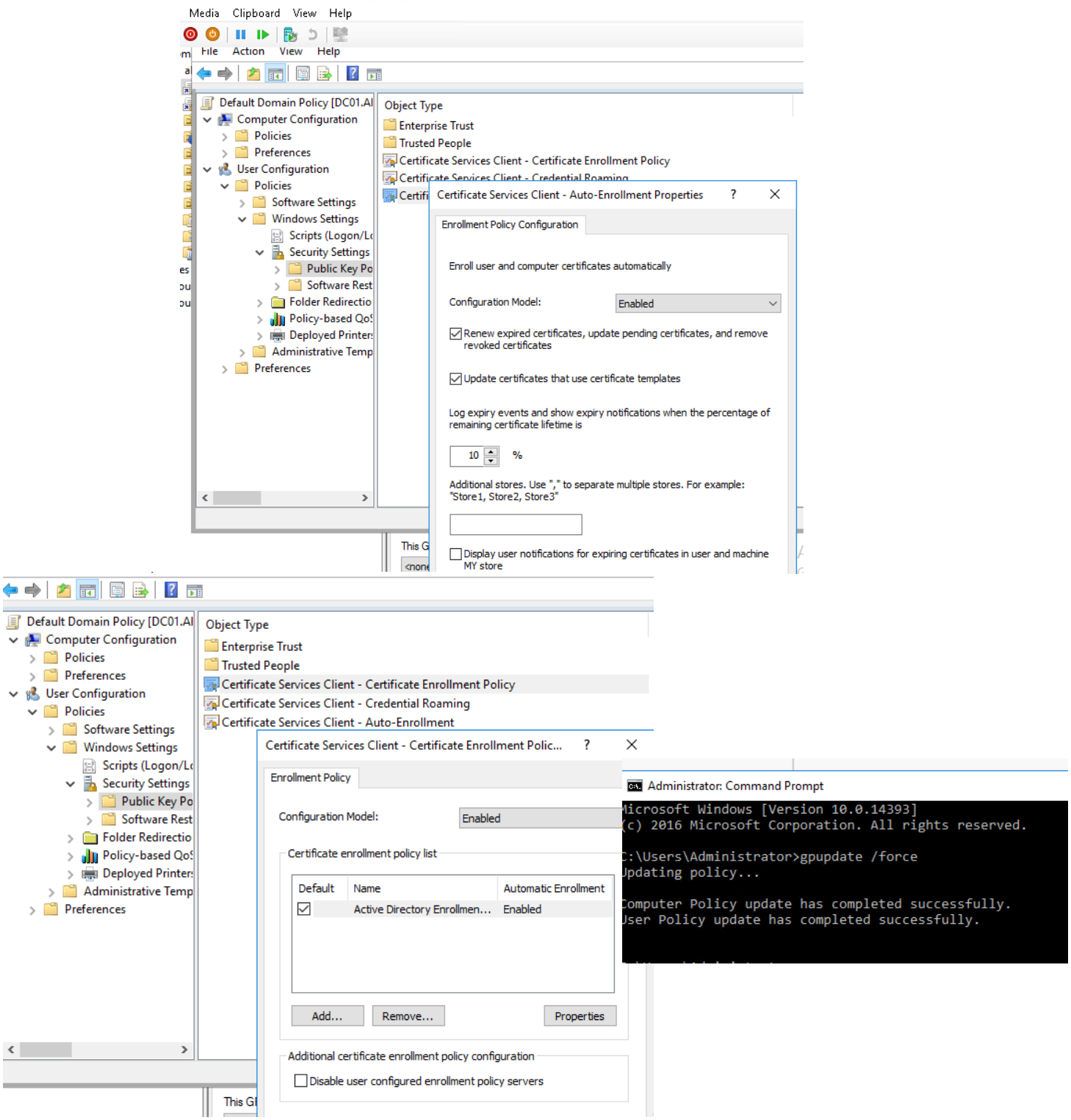

ADCS on WIN10LAB05 - Virtual Machine Connection
File Action Media Clipboard View Help
certsrv - [Certification Authority (Local)\abdelwahed-ADCS-CA\Certificate Templates]
File Action View Help
Certification Authority (Local)
abdelwahed-ADCS-CA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
Name
Intended Purpose
abdelwahed Users Cert
Client Authentication, Secure Email, En...
Abdelwahed Web Server
Server Authentication
Directory Email Replication
Directory Service Email Replication
Domain Controller Authentication
Client Authentication, Server Authentic...
Kerberos Authentication
Client Authentication, Server Authentic...
EFS Recovery Agent
File Recovery
Basic EFS
Encrypting File System
Domain Controller
Client Authentication, Server Authentic...
Web Server
Server Authentication
Computer
Client Authentication, Server Authentic...
User
Encrypting File System, Secure Email, Cl...
Subordinate Certification Authority
<All>
Administrator
Microsoft Trust List Signing, Encrypting...

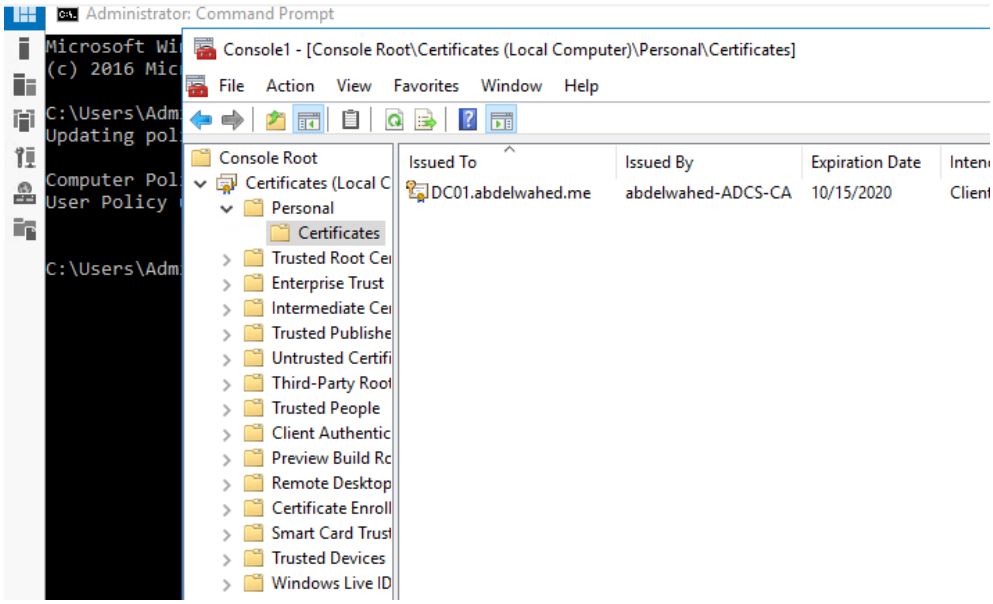
Proceed to group policy settings to set up automatic enrollment.

Initially, verify any certificates that have been issued to the administrator user on an Active Directory computer.

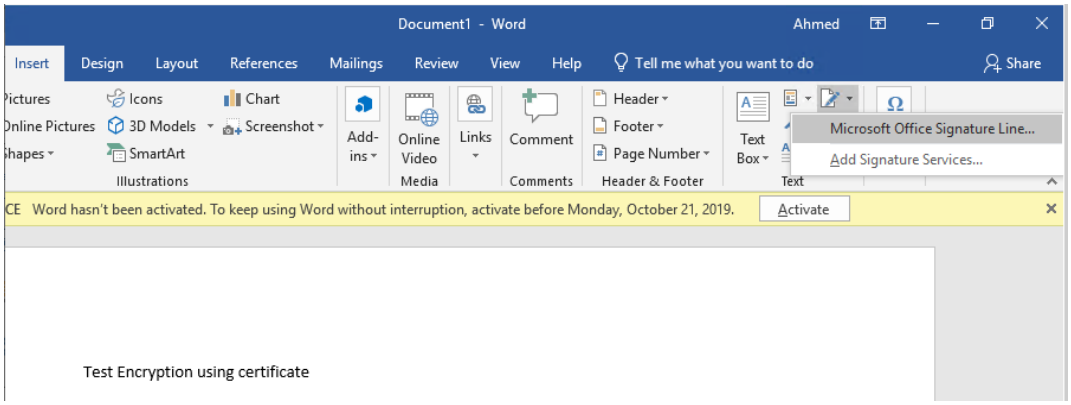


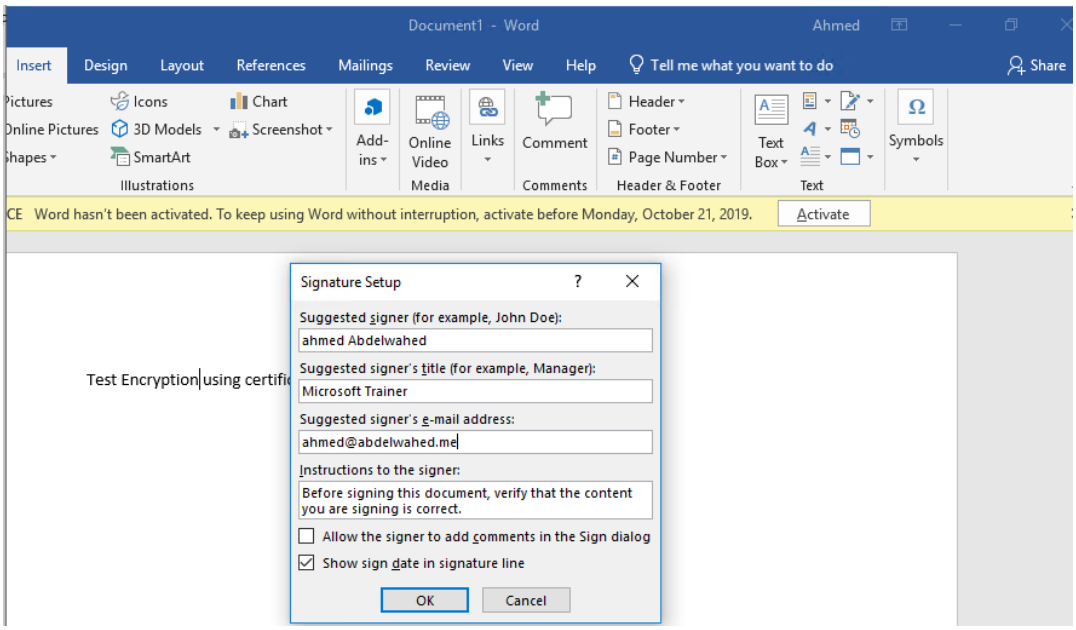


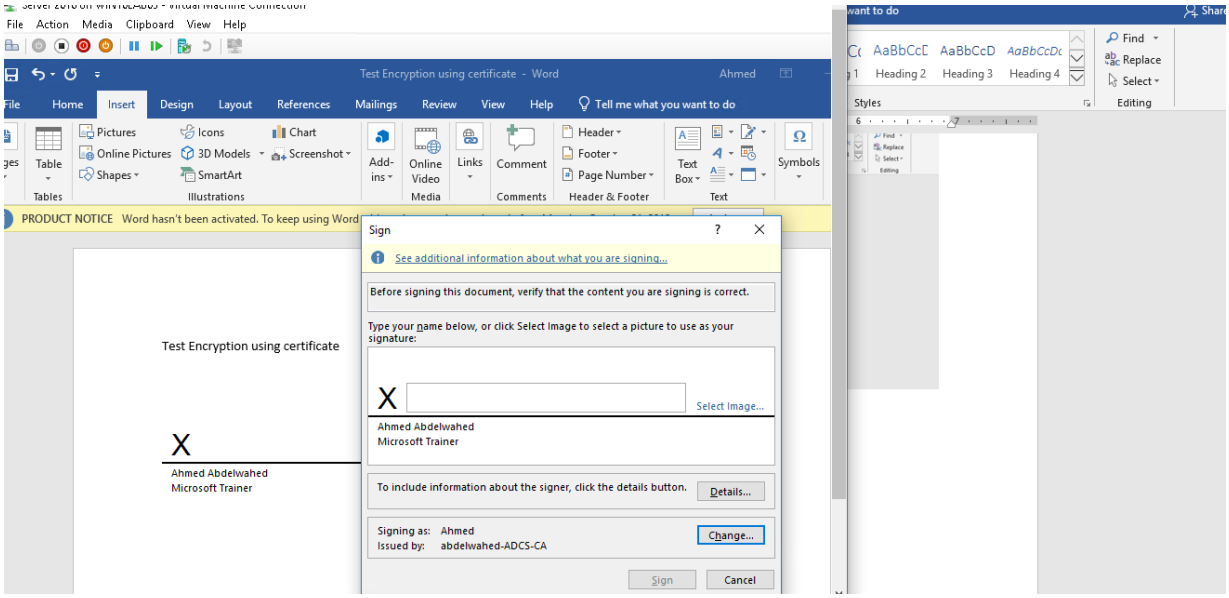

Media Clipboard View Help
File Action View Help
Default Domain Policy [DC01.Al
Computer Configuration
Policies
Preferences
User Configuration
Policies
Software Settings
Windows Settings
Scripts (Logon/Lo
Security Settings
Public Key Po
Software Rest
Folder Redirectio
Policy-based QoS
Deployed Printers
Administrative Temp
Preferences
Object Type
Enterprise Trust
Trusted People
Certificate Services Client - Certificate Enrollment Policy
Certificate Services Client - Credential Roaming
Certificate Services Client - Auto-Enrollment
Certificate Services Client - Auto-Enrollment Properties
Enrollment Policy Configuration
Enroll user and computer certificates automatically
Configuration Model:
Enabled
Renew expired certificates, update pending certificates, and remove revoked certificates
Update certificates that use certificate templates
Log expiry events and show expiry notifications when the percentage of remaining certificate lifetime is
10
%
Additional stores. Use "," to separate multiple stores. For example: "Store1, Store2, Store3"
Display user notifications for expiring certificates in user and machine MY store
Certificate Services Client - Certificate Enrollment Polic...
Enrollment Policy
Configuration Model:
Enabled
Certificate enrollment policy list
Default
Name
Automatic Enrollment
Active Directory Enrollmen...
Enabled
Add...
Remove...
Properties
Additional certificate enrollment policy configuration
Disable user configured enrollment policy servers
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>gpupdate /force
Updating policy...
Computer Policy update has completed successfully.
User Policy update has completed successfully.



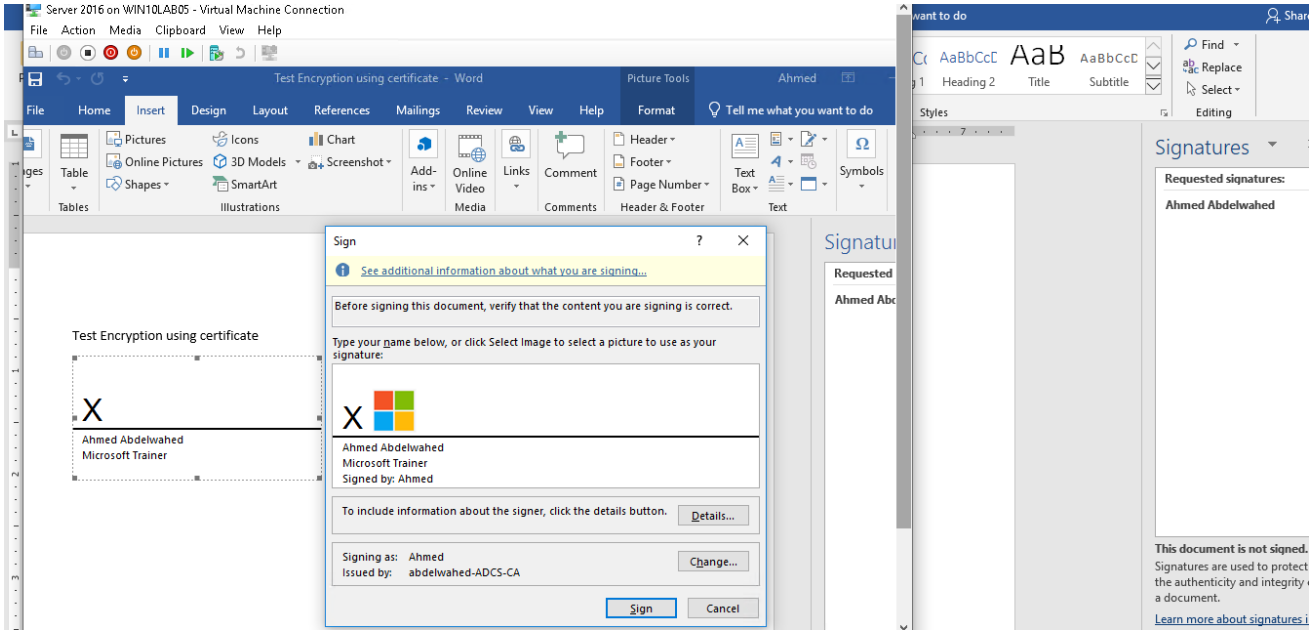
Secure a Word document with a Certificate for integrity and authenticity.



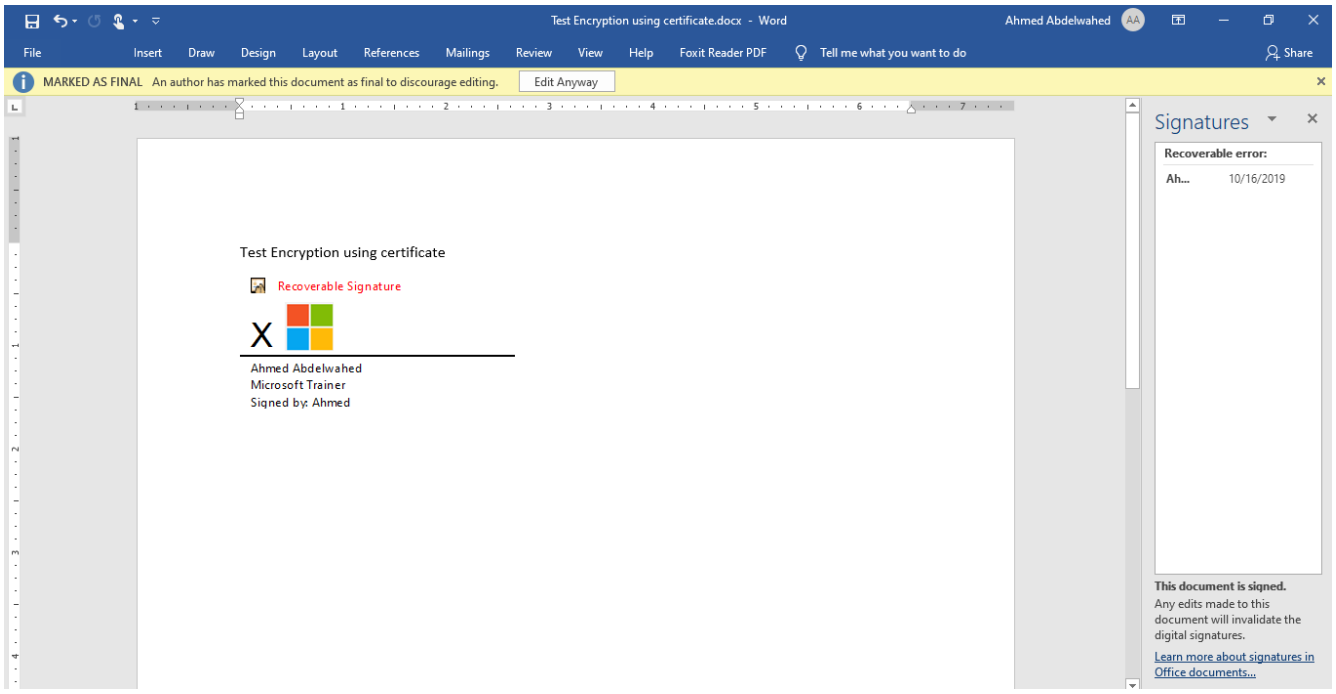




Be aware that our CA, abdelwahed-ADCS-CA, issues the certificate.



Attempting to edit the file now is impossible as it is designated a final copy with a signature, ensuring its integrity and authenticity. This means the file hasn't been altered in transit because editing would require removing the signed signature first.

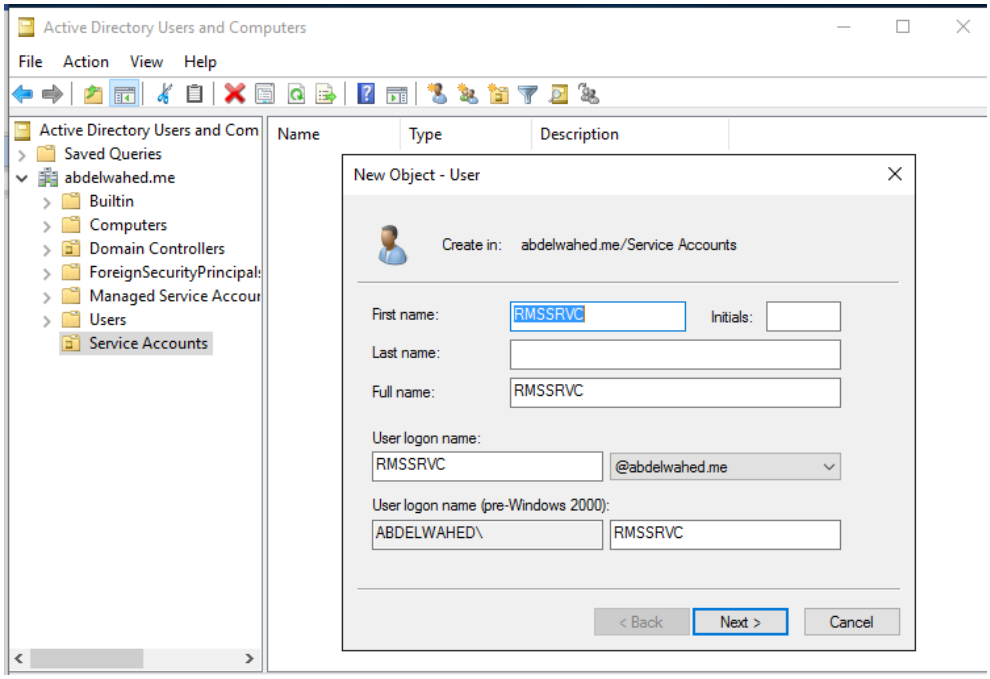


Active Directory Rights Management

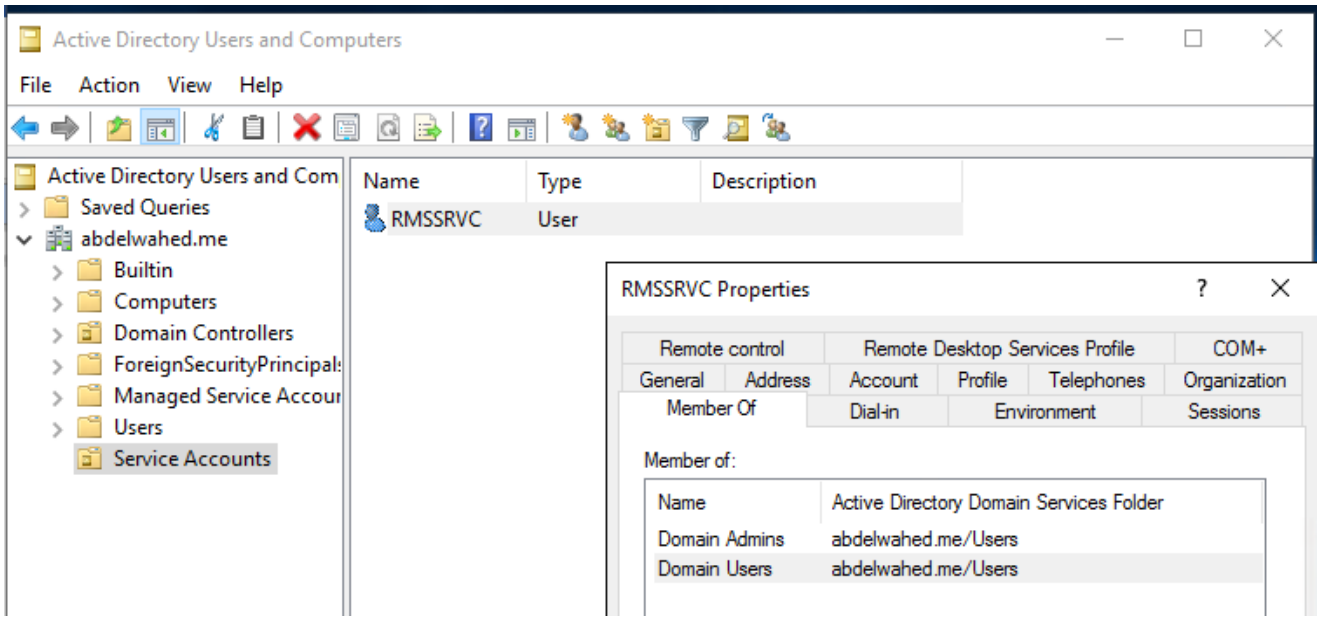
Preparation and Installation

Active Directory Configuration

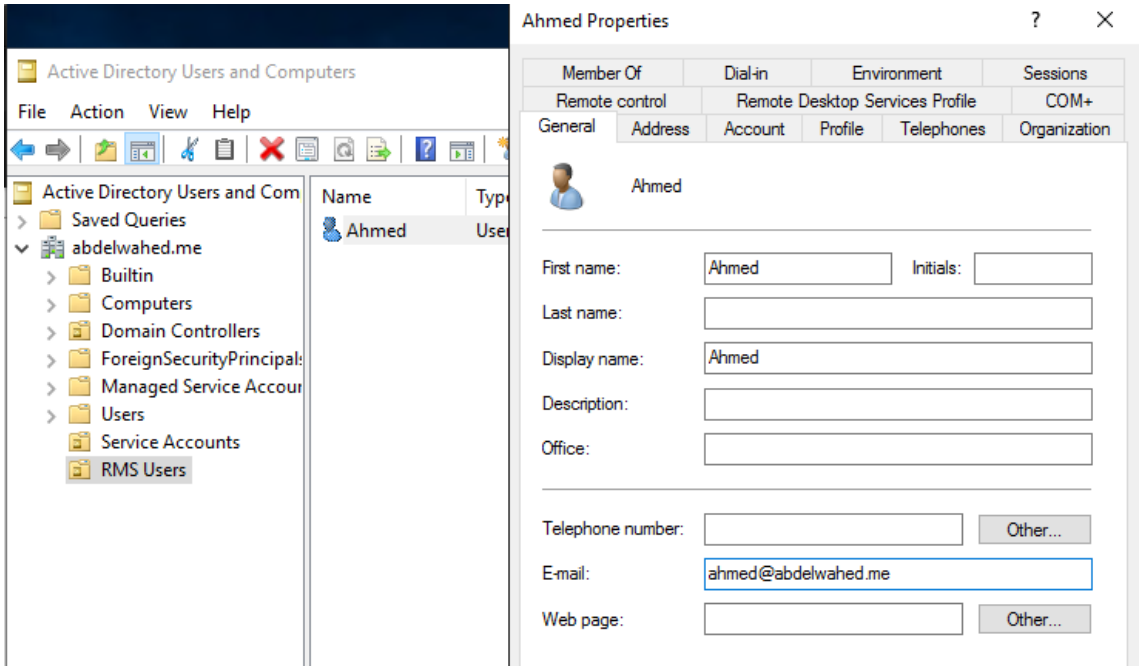
Creating **AD RMS Service Account on Domain Server and create users for testing**

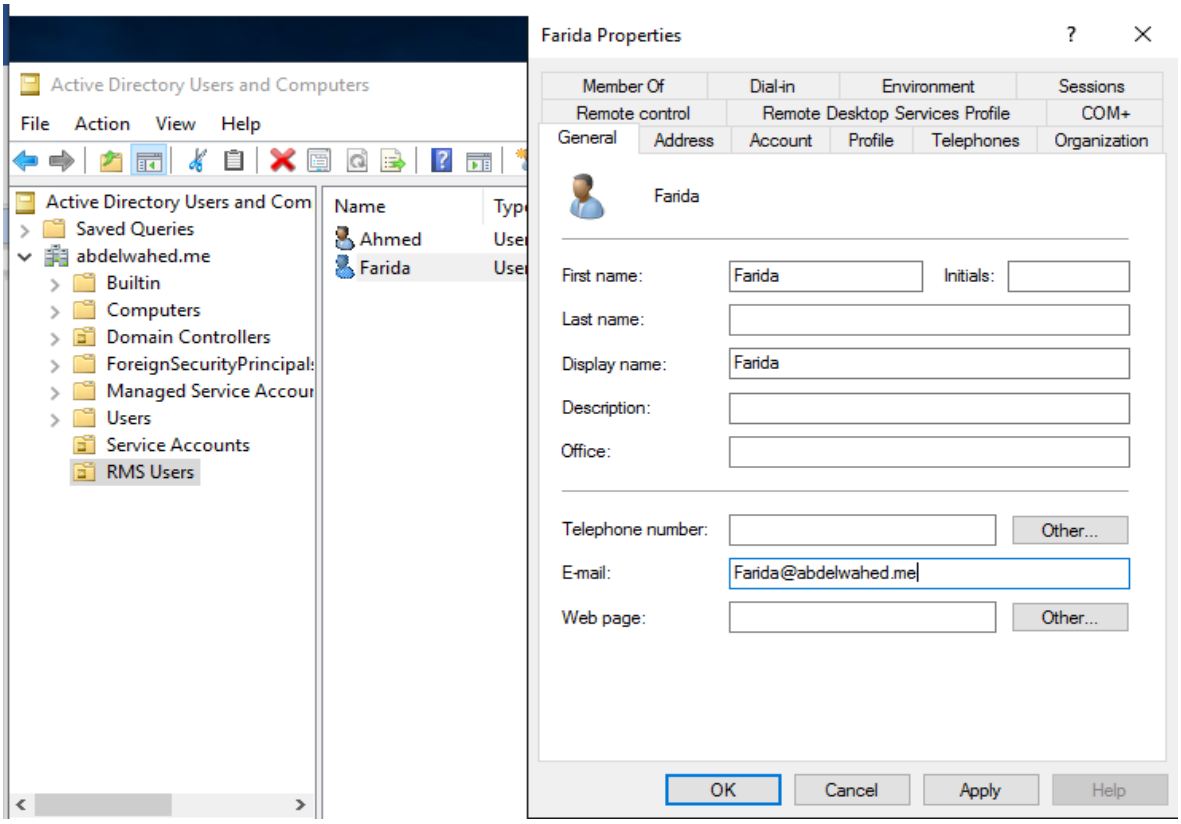


Remember, it's unnecessary to include the RMSerivce user in the admin group; instead, we can make them a member of the RM Server's local admin group.



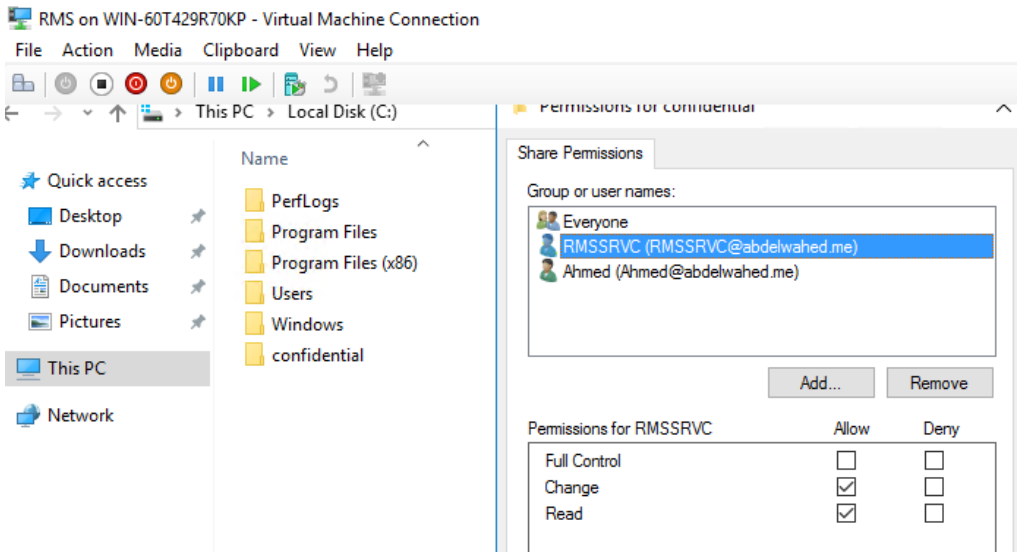
Create two users in the active directory for testing purposes and provide information to the users via email.



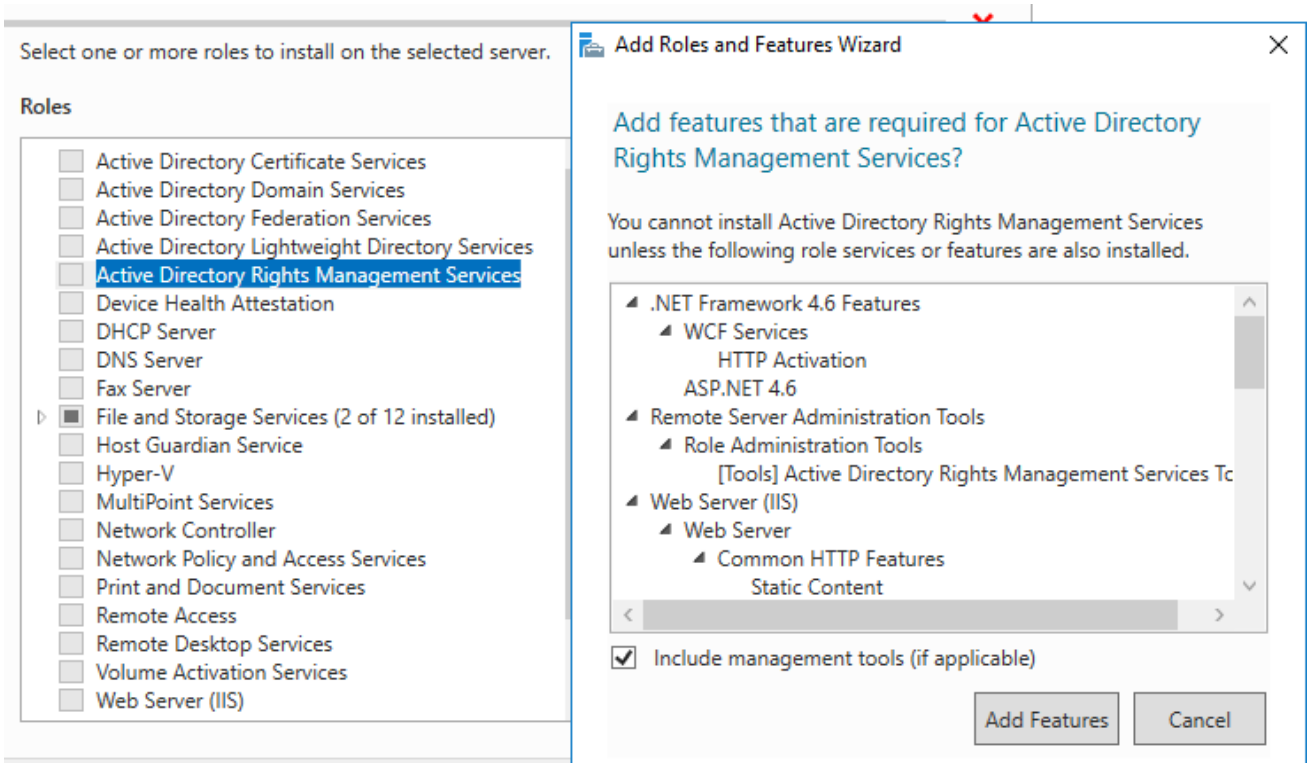


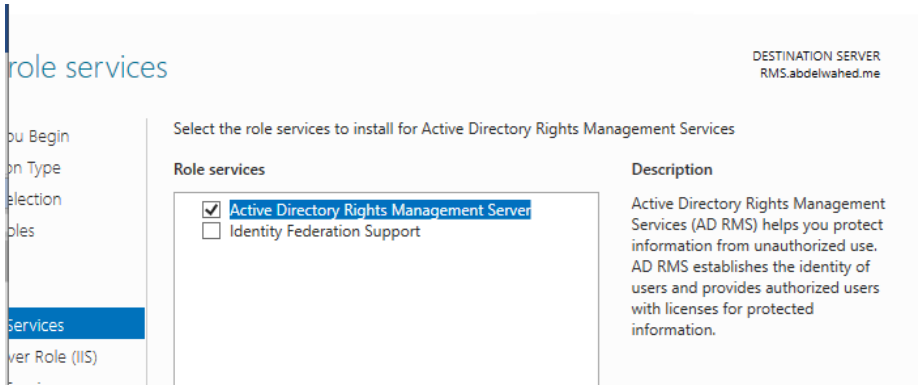
Create Shared Distribution Point (SDP) used to save policy template

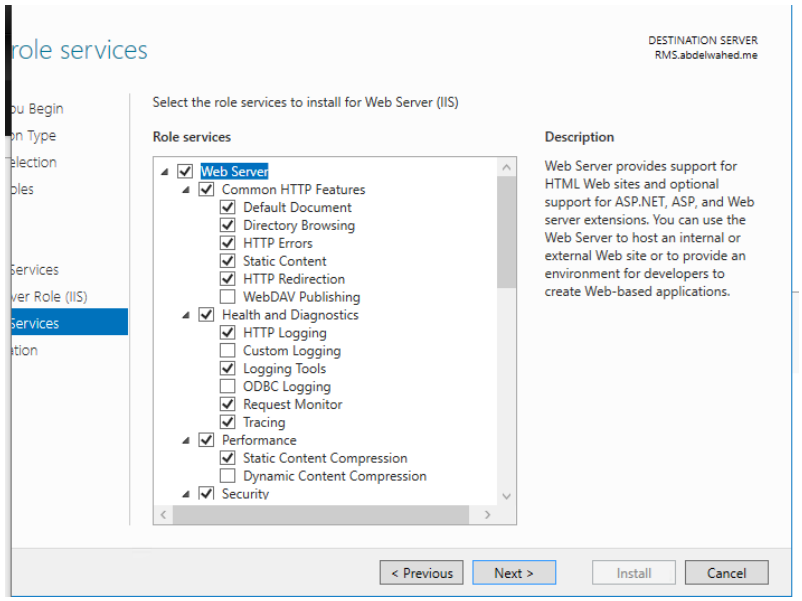
Set up a Shared Distribution Point (SDP) called 'confidential' and grant Read/Write access to users Ahmed and RMSRVC using a domain member server that will also serve as an RMS Server.

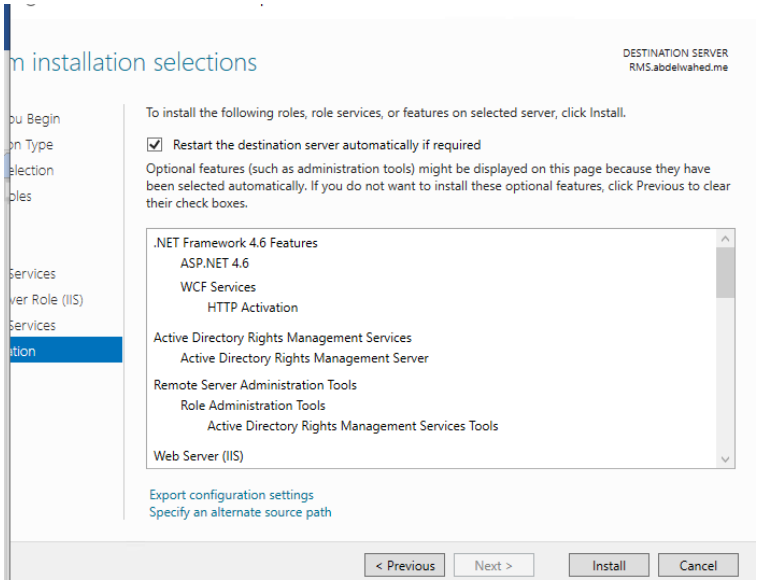


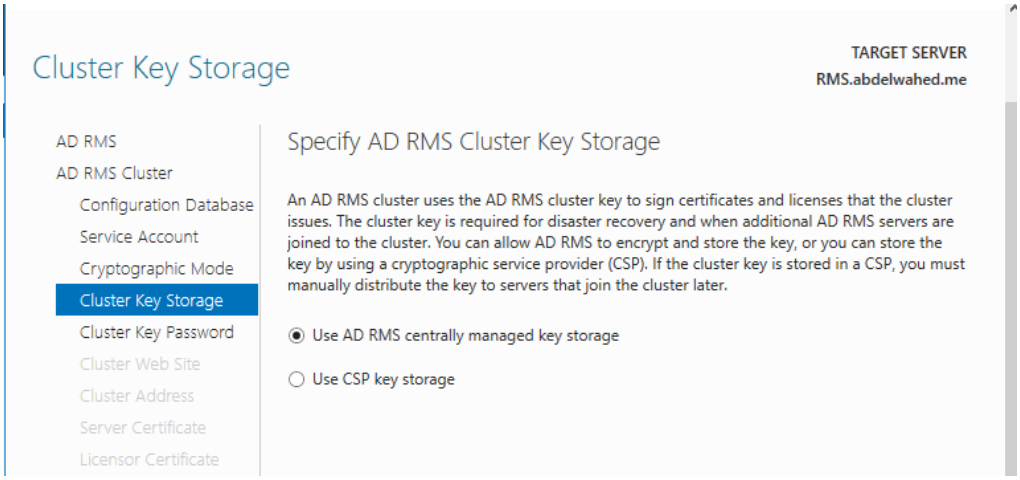
AD RMS Installation using domain joined member server (RMS)




role services
DESTINATION SERVER
RMS.abdelwahed.me
Select the role services to install for Active Directory Rights Management Services
Role services
Active Directory Rights Management Server
Identity Federation Support
Description
Active Directory Rights Management Services (AD RMS) helps you protect information from unauthorized use. AD RMS establishes the identity of users and provides authorized users with licenses for protected information.

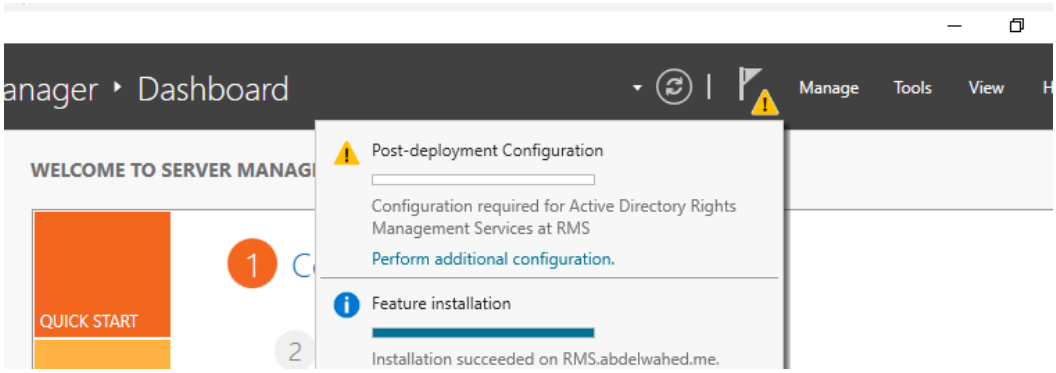

role services
DESTINATION SERVER
RMS.abdelwahed.me
Select the role services to install for Web Server (IIS)
Role services
Web Server
Common HTTP Features
Default Document
Directory Browsing
HTTP Errors
Static Content
HTTP Redirection
WebDAV Publishing
Health and Diagnostics
HTTP Logging
Custom Logging
Logging Tools
ODBC Logging
Request Monitor
Tracing
Performance
Static Content Compression
Dynamic Content Compression
Security
Description
Web Server provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web-based applications.
< Previous
Next >
Install
Cancel

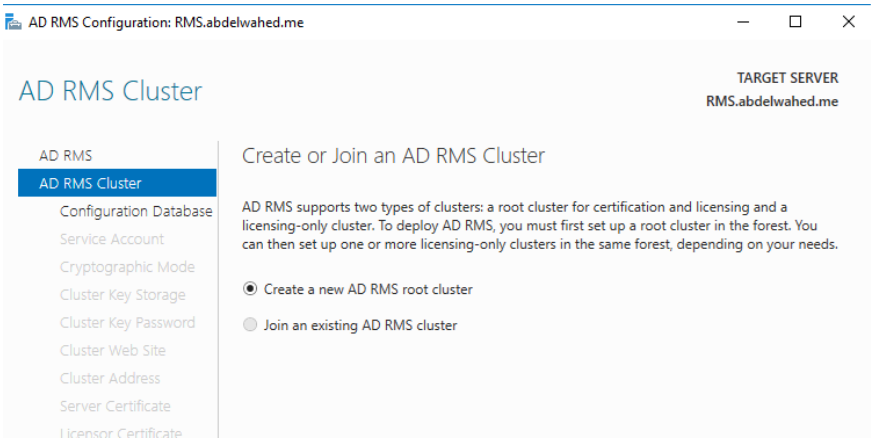

m installation selections
DESTINATION SERVER
RMS.abdelwahed.me
To install the following roles, role services, or features on selected server, click Install.
Restart the destination server automatically if required
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.
.NET Framework 4.6 Features
ASP.NET 4.6
WCF Services
HTTP Activation
Active Directory Rights Management Services
Active Directory Rights Management Server
Remote Server Administration Tools
Role Administration Tools
Active Directory Rights Management Services Tools
Web Server (IIS)
Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel

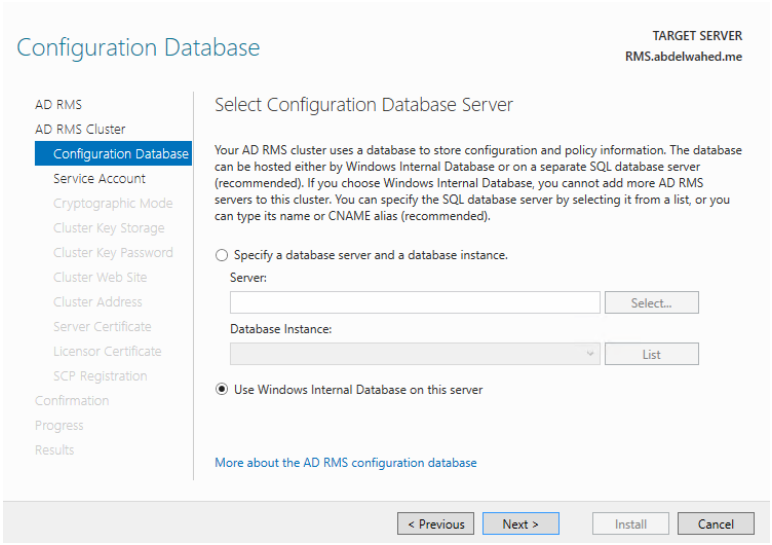


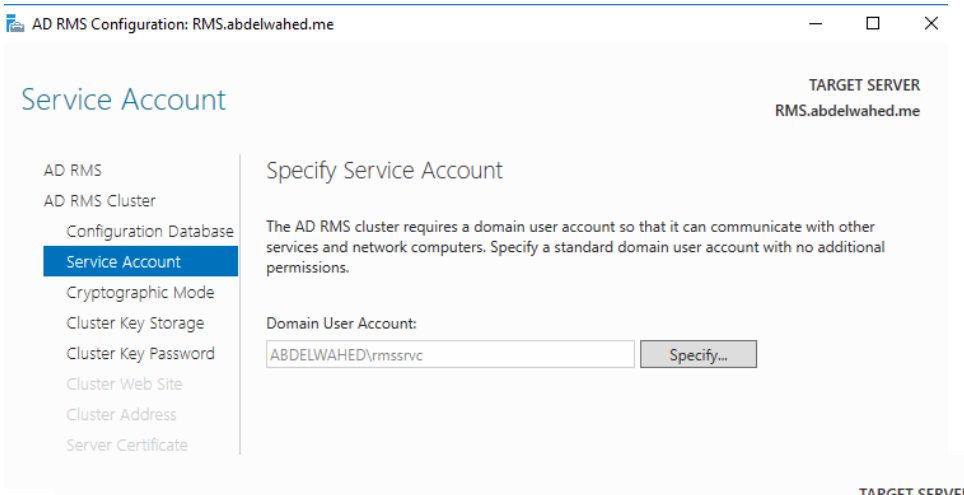
Post installation configuration

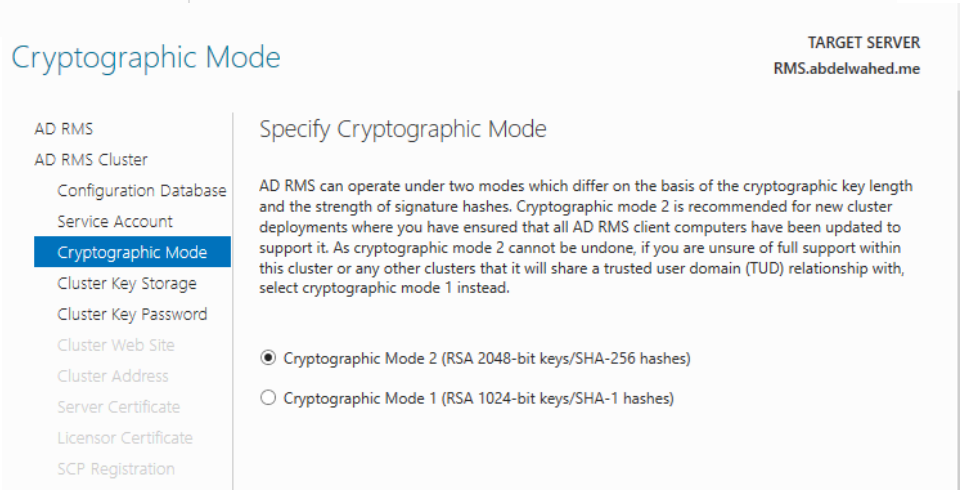
add AD RMS Cluster

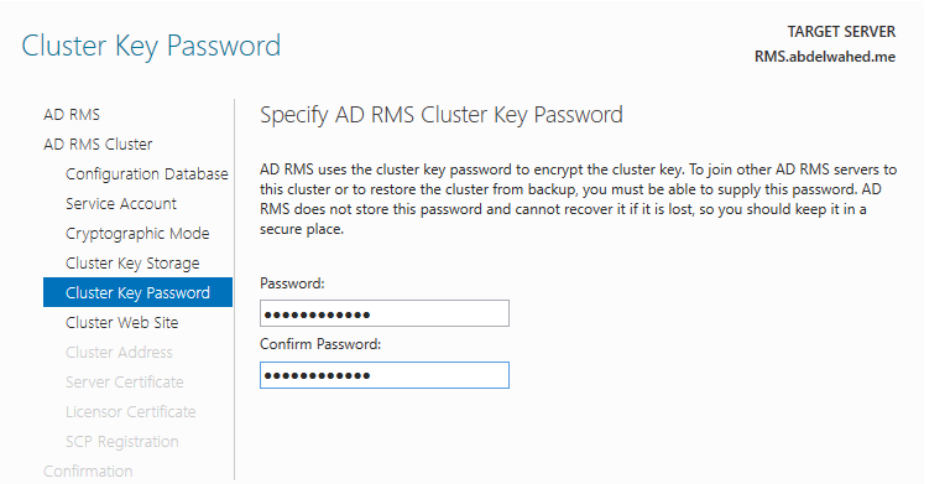


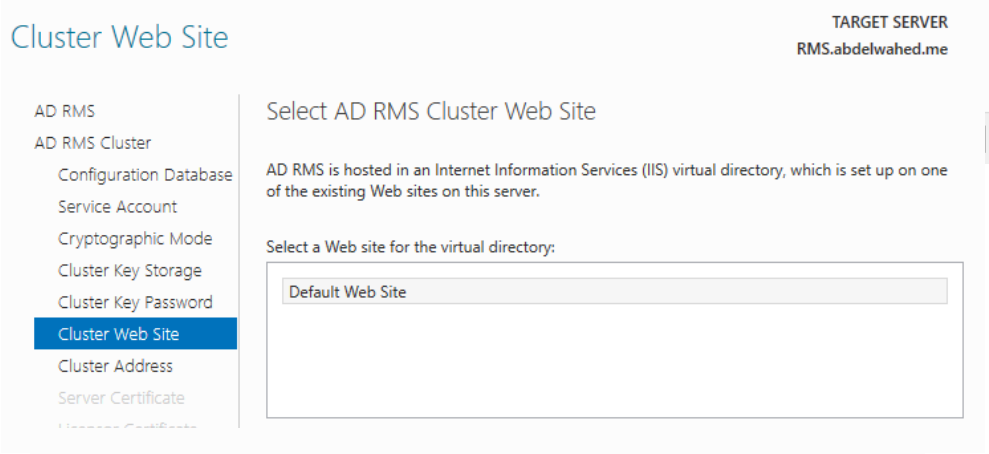


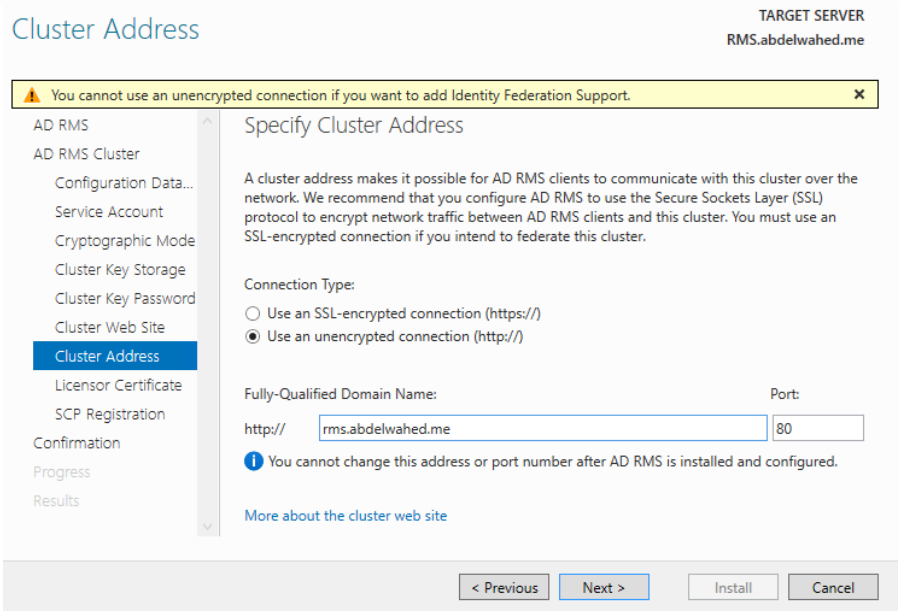

Configuration Database
TARGET SERVER
RMS.abdelwahed.me
AD RMS
AD RMS Cluster
Configuration Database
Service Account
Cryptographic Mode
Cluster Key Storage
Cluster Key Password
Cluster Web Site
Cluster Address
Server Certificate
Licensor Certificate
SCP Registration
Confirmation
Progress
Results
Select Configuration Database Server
Your AD RMS cluster uses a database to store configuration and policy information. The database can be hosted either by Windows Internal Database or on a separate SQL database server (recommended). If you choose Windows Internal Database, you cannot add more AD RMS servers to this cluster. You can specify the SQL database server by selecting it from a list, or you can type its name or CNAME alias (recommended).
Specify a database server and a database instance.
Server:
Select...
Database Instance:
List
Use Windows Internal Database on this server
More about the AD RMS configuration database
< Previous
Next >
Install
Cancel

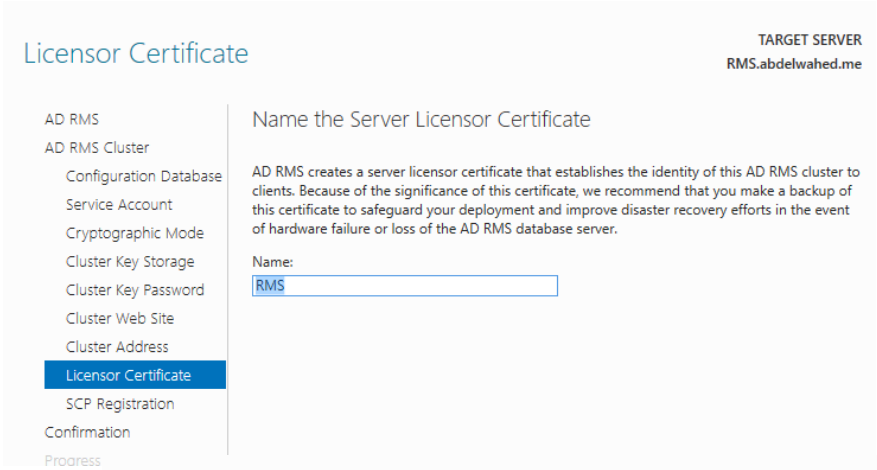

AD RMS Configuration: RMS.abdelwahed.me
Service Account
TARGET SERVER
RMS.abdelwahed.me
AD RMS
AD RMS Cluster
Configuration Database
Service Account
Cryptographic Mode
Cluster Key Storage
Cluster Key Password
Cluster Web Site
Cluster Address
Server Certificate
Specify Service Account
The AD RMS cluster requires a domain user account so that it can communicate with other services and network computers. Specify a standard domain user account with no additional permissions.
Domain User Account:
ABDELWAHED\rmssrvc
Specify...

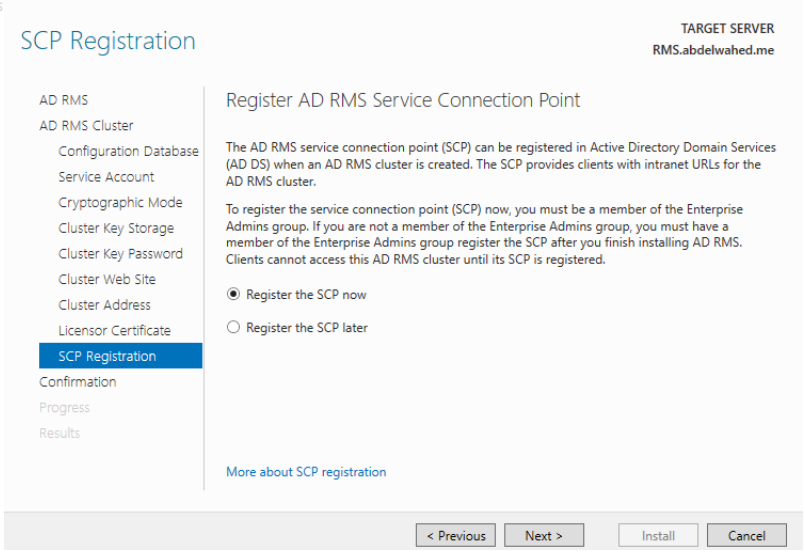

Cryptographic Mode
TARGET SERVER
RMS.abdelwahed.me
AD RMS
AD RMS Cluster
Configuration Database
Service Account
Cryptographic Mode
Cluster Key Storage
Cluster Key Password
Cluster Web Site
Cluster Address
Server Certificate
Licensor Certificate
SCP Registration
Specify Cryptographic Mode
AD RMS can operate under two modes which differ on the basis of the cryptographic key length and the strength of signature hashes. Cryptographic mode 2 is recommended for new cluster deployments where you have ensured that all AD RMS client computers have been updated to support it. As cryptographic mode 2 cannot be undone, if you are unsure of full support within this cluster or any other clusters that it will share a trusted user domain (TUD) relationship with, select cryptographic mode 1 instead.
Cryptographic Mode 2 (RSA 2048-bit keys/SHA-256 hashes)
Cryptographic Mode 1 (RSA 1024-bit keys/SHA-1 hashes)

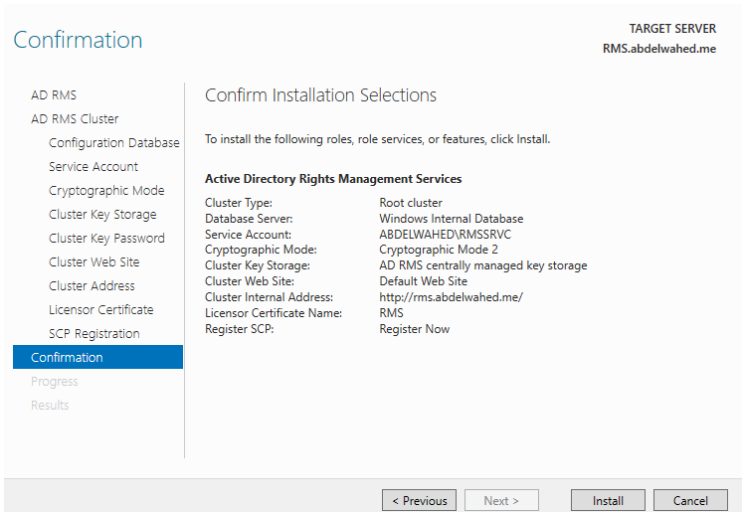

Cluster Key Password
TARGET SERVER
RMS.abdelwahed.me
AD RMS
AD RMS Cluster
Configuration Database
Service Account
Cryptographic Mode
Cluster Key Storage
Cluster Key Password
Cluster Web Site
Cluster Address
Server Certificate
Licensor Certificate
SCP Registration
Confirmation
Specify AD RMS Cluster Key Password
AD RMS uses the cluster key password to encrypt the cluster key. To join other AD RMS servers to this cluster or to restore the cluster from backup, you must be able to supply this password. AD RMS does not store this password and cannot recover it if it is lost, so you should keep it in a secure place.
Password:
Confirm Password:

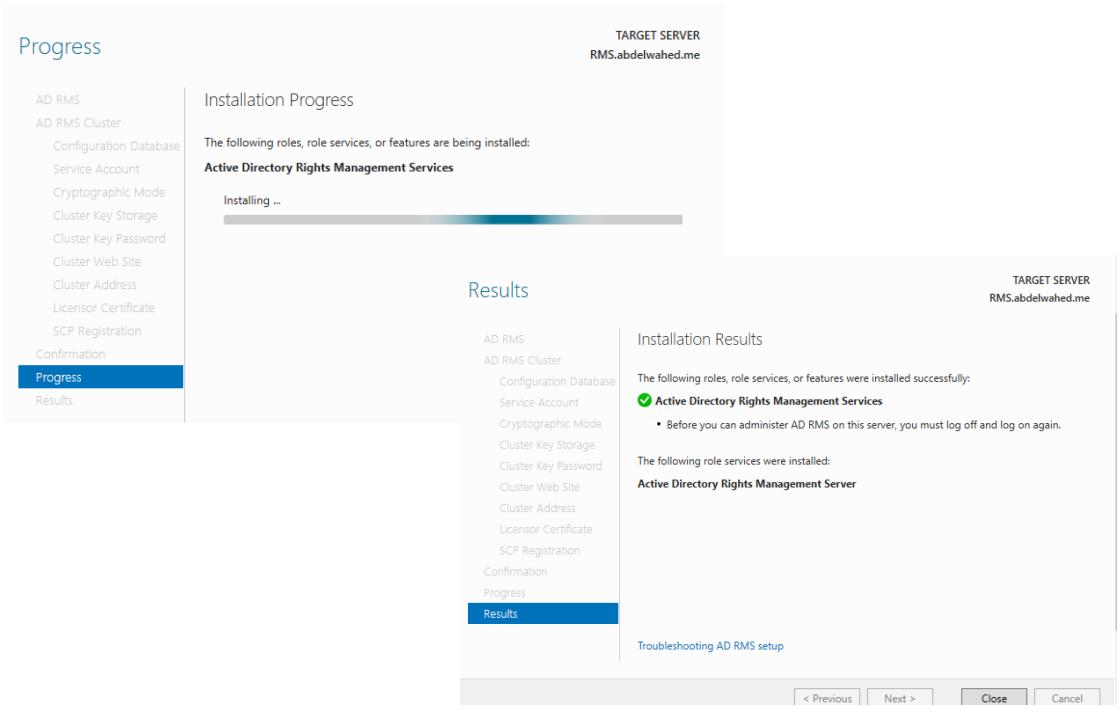

Cluster Web Site
TARGET SERVER
RMS.abdelwahed.me
AD RMS
AD RMS Cluster
Configuration Database
Service Account
Cryptographic Mode
Cluster Key Storage
Cluster Key Password
Cluster Web Site
Cluster Address
Server Certificate
Select AD RMS Cluster Web Site
AD RMS is hosted in an Internet Information Services (IIS) virtual directory, which is set up on one of the existing Web sites on this server.
Select a Web site for the virtual directory:
Default Web Site


Cluster Address
TARGET SERVER
RMS.abdelwahed.me
You cannot use an unencrypted connection if you want to add Identity Federation Support.
AD RMS
AD RMS Cluster
Configuration Data...
Service Account
Cryptographic Mode
Cluster Key Storage
Cluster Key Password
Cluster Web Site
Cluster Address
Licensor Certificate
SCP Registration
Confirmation
Progress
Results
Specify Cluster Address
A cluster address makes it possible for AD RMS clients to communicate with this cluster over the network. We recommend that you configure AD RMS to use the Secure Sockets Layer (SSL) protocol to encrypt network traffic between AD RMS clients and this cluster. You must use an SSL-encrypted connection if you intend to federate this cluster.
Connection Type:
Use an SSL-encrypted connection (https://)
Use an unencrypted connection (http://)
Fully-Qualified Domain Name:
Port:
http://
rms.abdelwahed.me
80
You cannot change this address or port number after AD RMS is installed and configured.
More about the cluster web site
< Previous
Next >
Install
Cancel

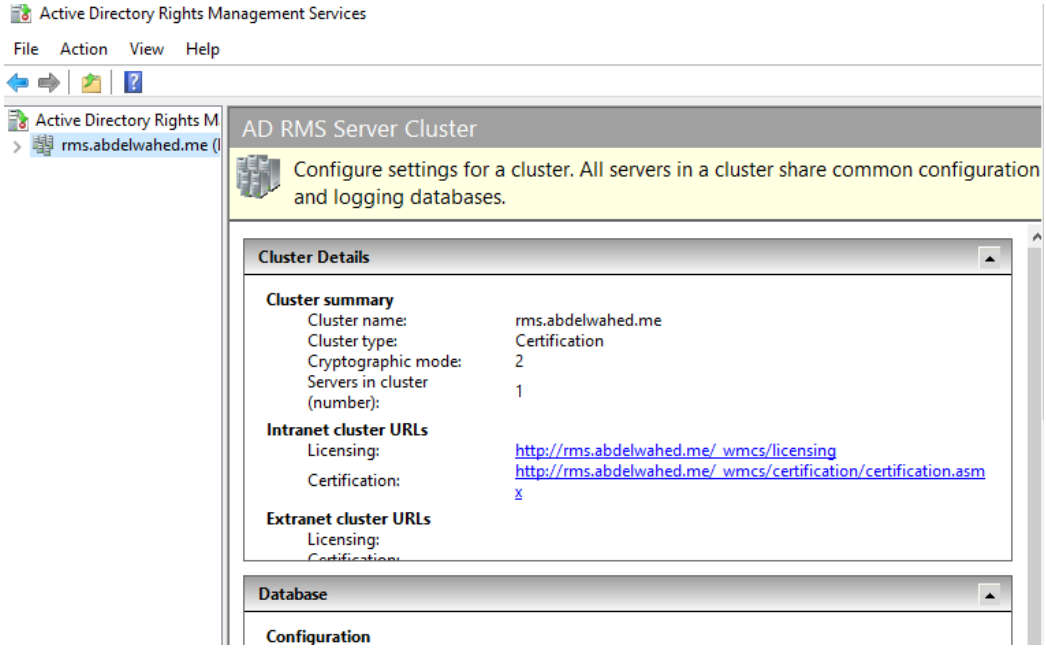

Licensor Certificate
TARGET SERVER
RMS.abdelwahed.me
AD RMS
AD RMS Cluster
Configuration Database
Service Account
Cryptographic Mode
Cluster Key Storage
Cluster Key Password
Cluster Web Site
Cluster Address
Licensor Certificate
SCP Registration
Confirmation
Progress
Name the Server Licensor Certificate
AD RMS creates a server licensor certificate that establishes the identity of this AD RMS cluster to clients. Because of the significance of this certificate, we recommend that you make a backup of this certificate to safeguard your deployment and improve disaster recovery efforts in the event of hardware failure or loss of the AD RMS database server.
Name:
RMS


SCP Registration
TARGET SERVER
RMS.abdelwahed.me
AD RMS
AD RMS Cluster
Configuration Database
Service Account
Cryptographic Mode
Cluster Key Storage
Cluster Key Password
Cluster Web Site
Cluster Address
Licensor Certificate
SCP Registration
Confirmation
Progress
Results
Register AD RMS Service Connection Point
The AD RMS service connection point (SCP) can be registered in Active Directory Domain Services (AD DS) when an AD RMS cluster is created. The SCP provides clients with intranet URLs for the AD RMS cluster.
To register the service connection point (SCP) now, you must be a member of the Enterprise Admins group. If you are not a member of the Enterprise Admins group, you must have a member of the Enterprise Admins group register the SCP after you finish installing AD RMS. Clients cannot access this AD RMS cluster until its SCP is registered.
Register the SCP now
Register the SCP later
More about SCP registration
< Previous
Next >
Install
Cancel

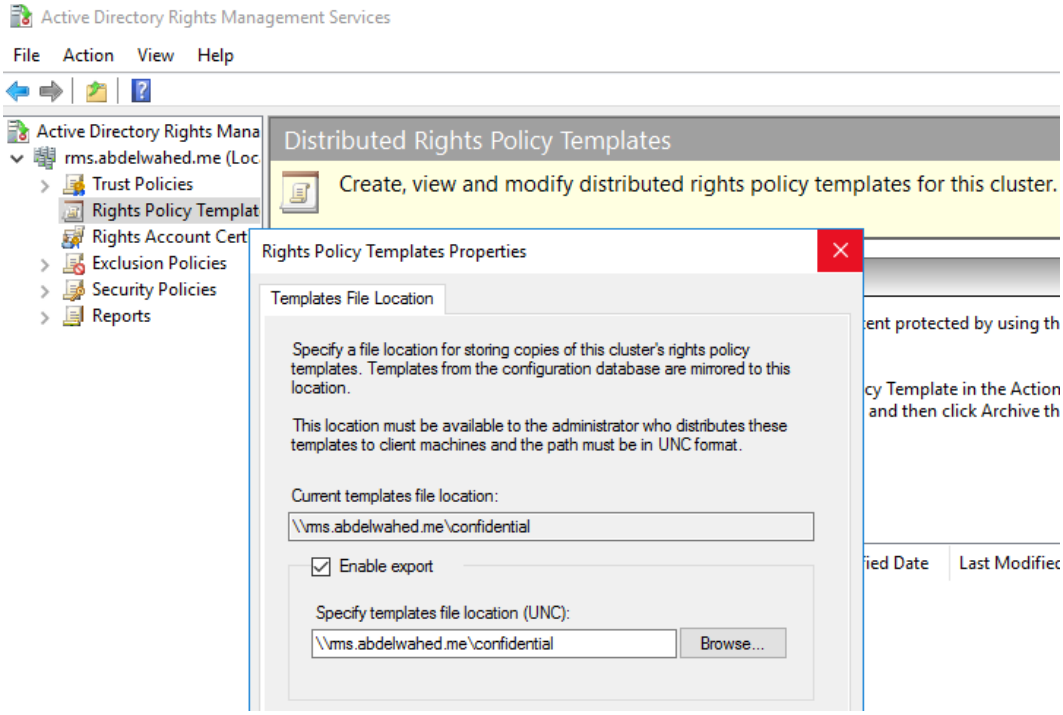

Confirmation
TARGET SERVER
RMS.abdelwahed.me
AD RMS
AD RMS Cluster
Configuration Database
Service Account
Cryptographic Mode
Cluster Key Storage
Cluster Key Password
Cluster Web Site
Cluster Address
Licensor Certificate
SCP Registration
Confirmation
Progress
Results
Confirm Installation Selections
To install the following roles, role services, or features, click Install.
Active Directory Rights Management Services
Cluster Type: Root cluster
Database Server: Windows Internal Database
Service Account: ABDELWAHED\RMSSRVC
Cryptographic Mode: Cryptographic Mode 2
Cluster Key Storage: AD RMS centrally managed key storage
Cluster Web Site: Default Web Site
Cluster Internal Address: http://rms.abdelwahed.me/
Licensor Certificate Name: RMS
Register SCP: Register Now
< Previous
Next >
Install
Cancel



Access AD RMS by utilizing the rmssrvc service account credentials (log into the RMS Server with the rms service account).

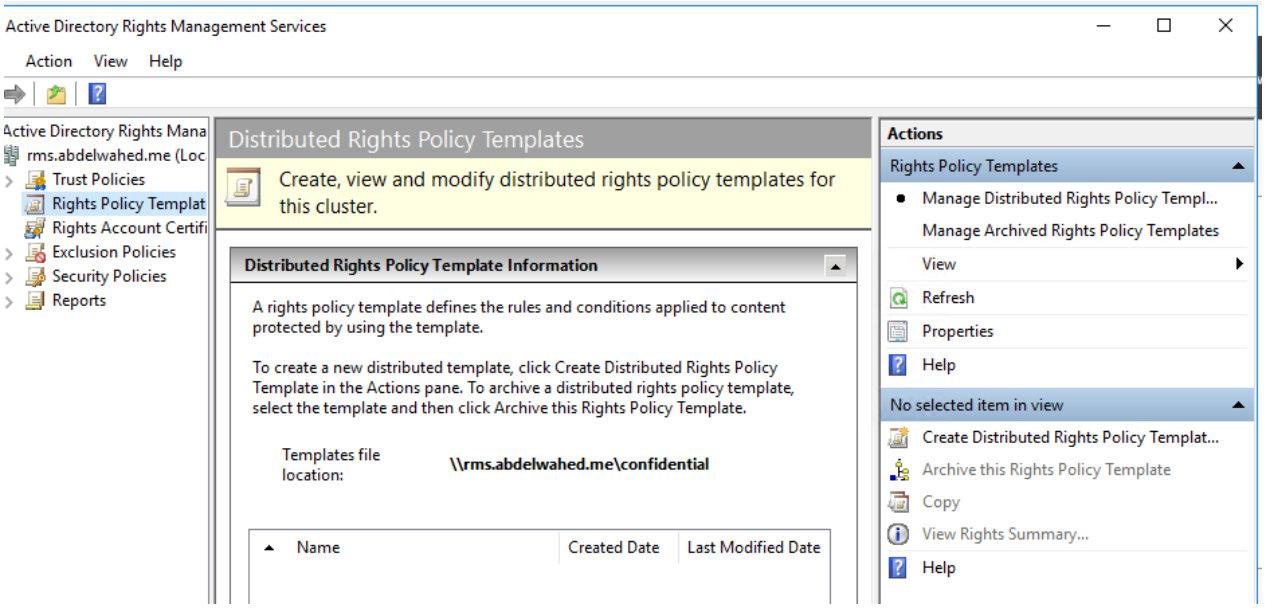


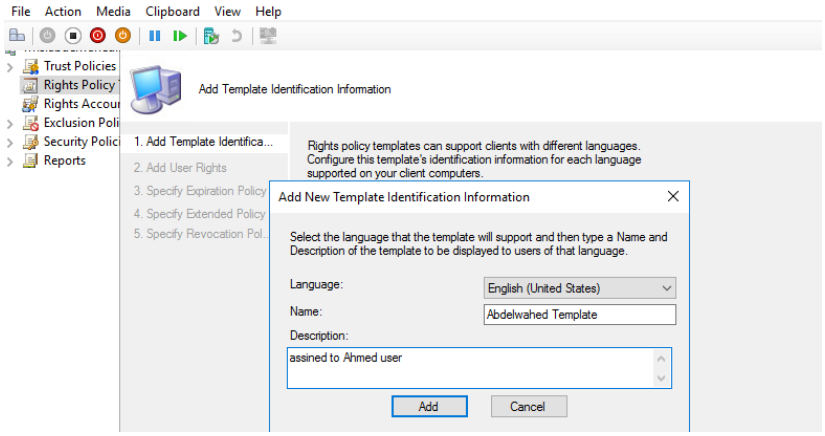
Configure RMS Template

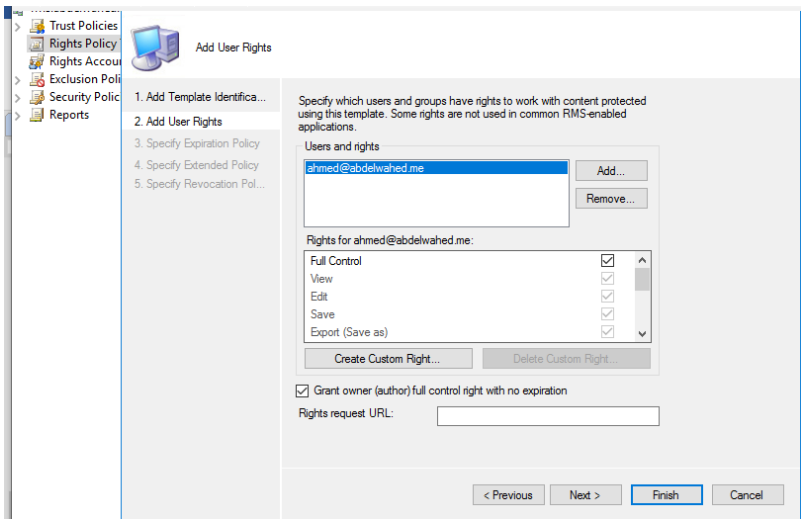


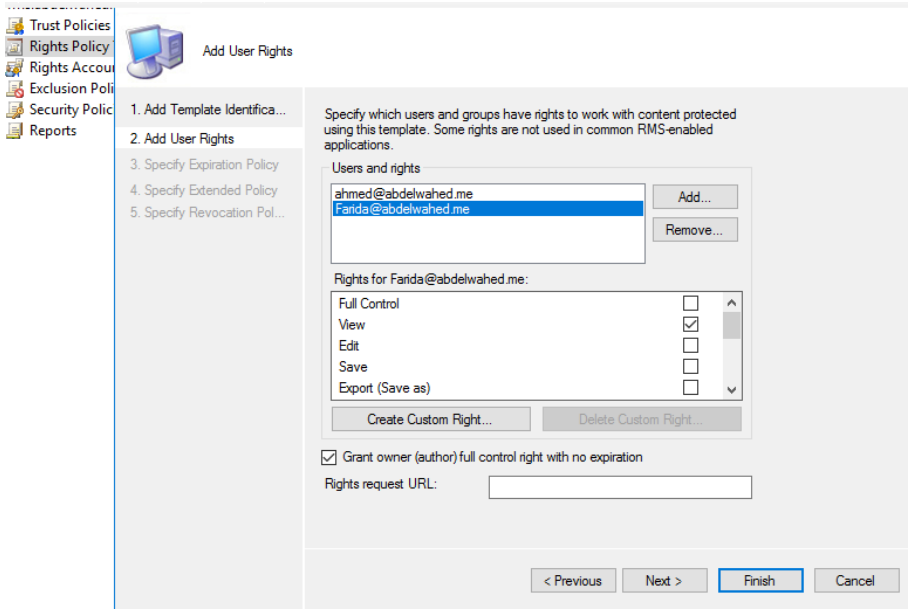
Create distributed rights policy template

Thus, users are able to apply security measures to their documents using this feature.

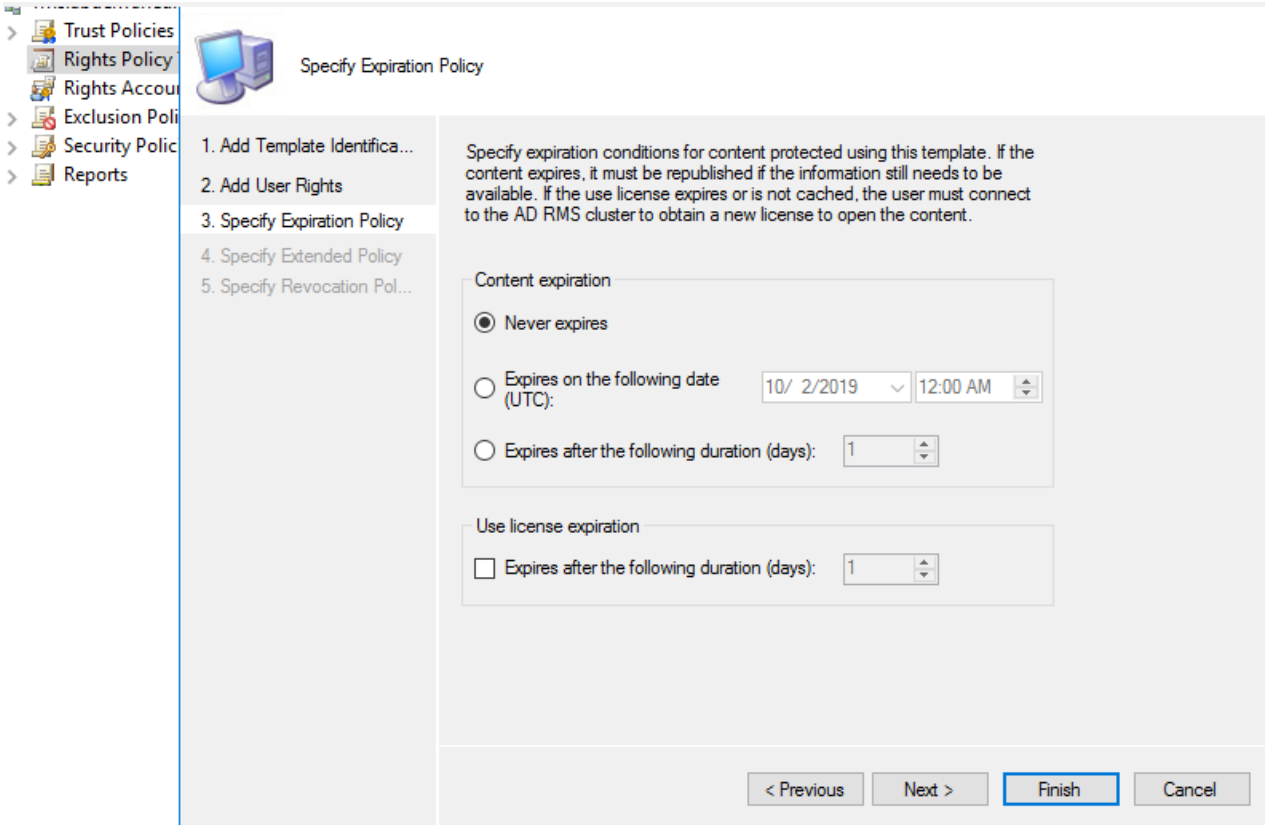


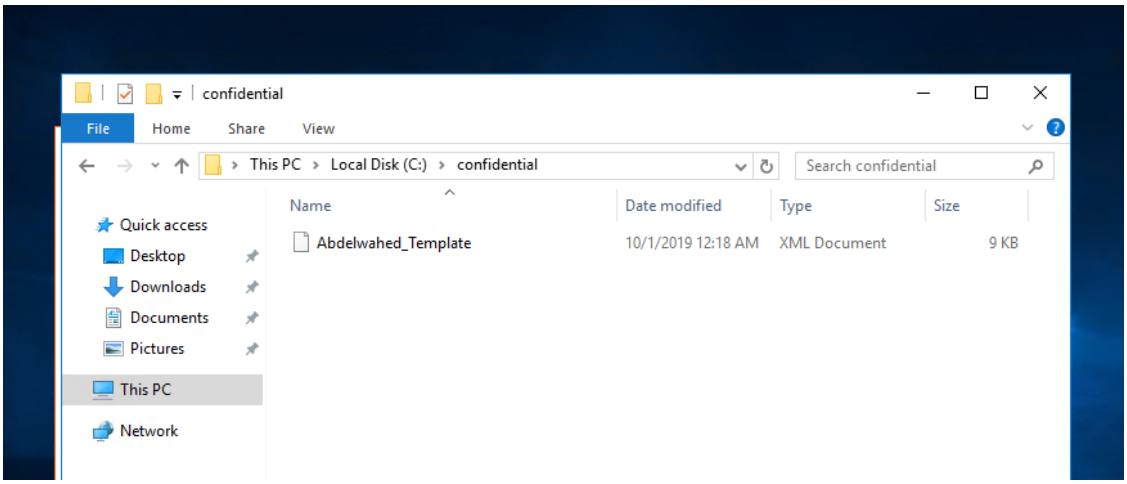

File Action Media Clipboard View Help
Trust Policies
Rights Policy
Rights Accou
Exclusion Poli
Security Polici
Reports
Add Template Identification Information
1. Add Template Identifica...
2. Add User Rights
3. Specify Expiration Policy
4. Specify Extended Policy
5. Specify Revocation Pol...
Rights policy templates can support clients with different languages. Configure this template's identification information for each language supported on your client computers.
Add New Template Identification Information
Select the language that the template will support and then type a Name and Description of the template to be displayed to users of that language.
Language:
English (United States)
Name:
Abdelwahed Template
Description:
assined to Ahmed user
Add
Cancel


Trust Policies
Rights Policy
Rights Accou
Exclusion Poli
Security Polic
Reports
Add User Rights
1. Add Template Identifica...
2. Add User Rights
3. Specify Expiration Policy
4. Specify Extended Policy
5. Specify Revocation Pol...
Specify which users and groups have rights to work with content protected using this template. Some rights are not used in common RMS-enabled applications.
Users and rights
ahmed@abdelwahed.me
Add...
Remove...
Rights for ahmed@abdelwahed.me:
Full Control
View
Edit
Save
Export (Save as)
Create Custom Right...
Delete Custom Right...
Grant owner (author) full control right with no expiration
Rights request URL:
< Previous
Next >
Finish
Cancel


Trust Policies
Rights Policy
Rights Accou
Exclusion Poli
Security Polic
Reports
Add User Rights
1. Add Template Identifica...
2. Add User Rights
3. Specify Expiration Policy
4. Specify Extended Policy
5. Specify Revocation Pol...
Specify which users and groups have rights to work with content protected using this template. Some rights are not used in common RMS-enabled applications.
Users and rights
ahmed@abdelwahed.me
Farida@abdelwahed.me
Add...
Remove...
Rights for Farida@abdelwahed.me:
Full Control
View
Edit
Save
Export (Save as)
Create Custom Right...
Delete Custom Right...
Grant owner (author) full control right with no expiration
Rights request URL:
< Previous
Next >
Finish
Cancel

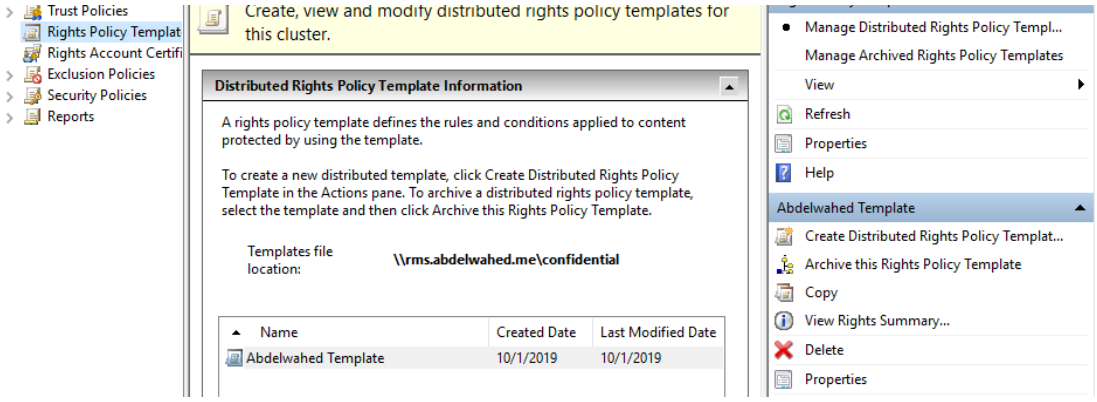
You can set expire date for this policy

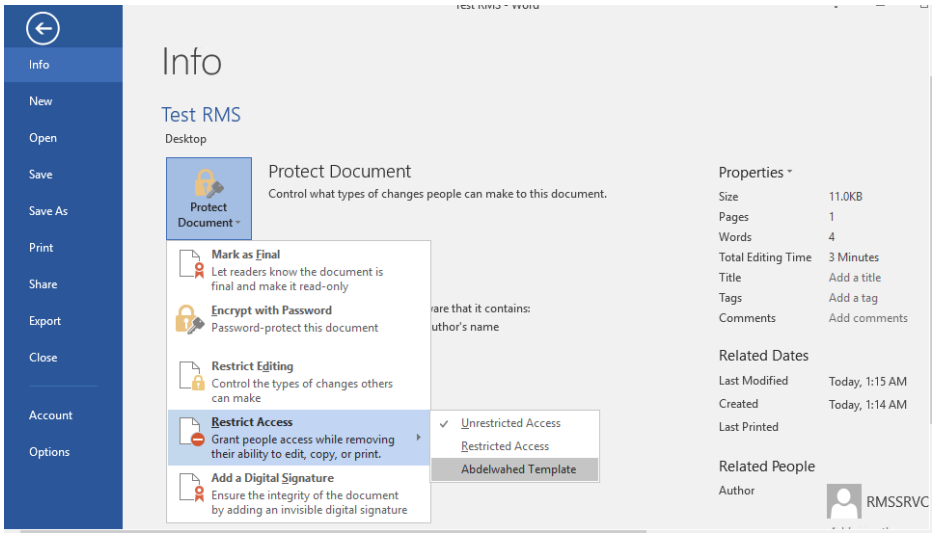


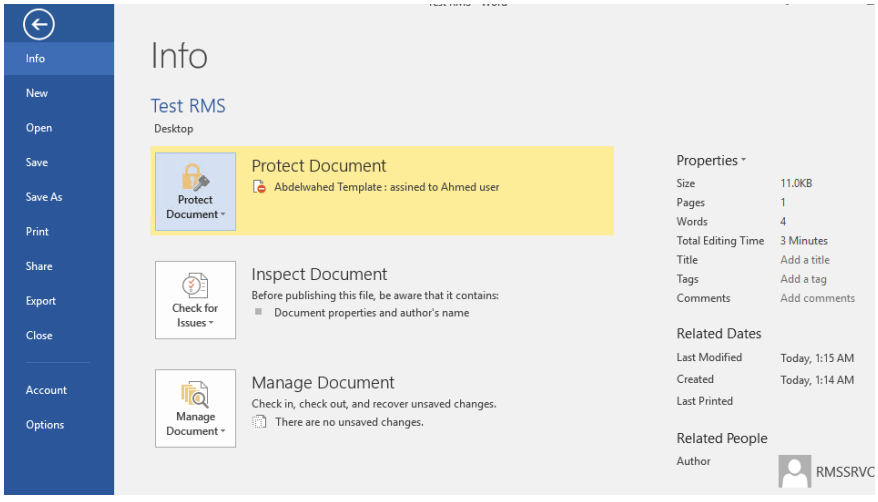


Testing

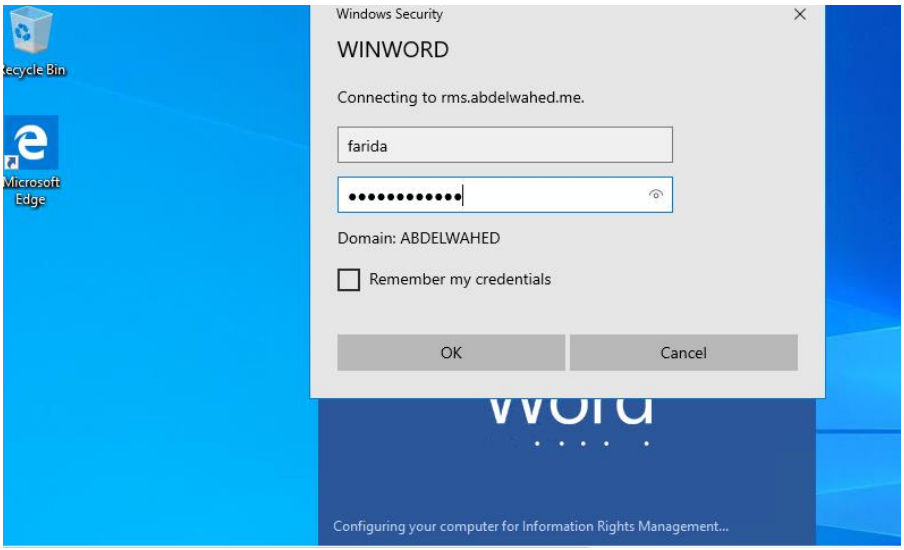
After creating and preparing the Policy, for testing purposes, generate a Word document and apply the newly established policy template (Abdelwahed Template) to it. Then, transfer this file to the Windows 10 client where the Farida User is signed in to verify the permitted permissions.



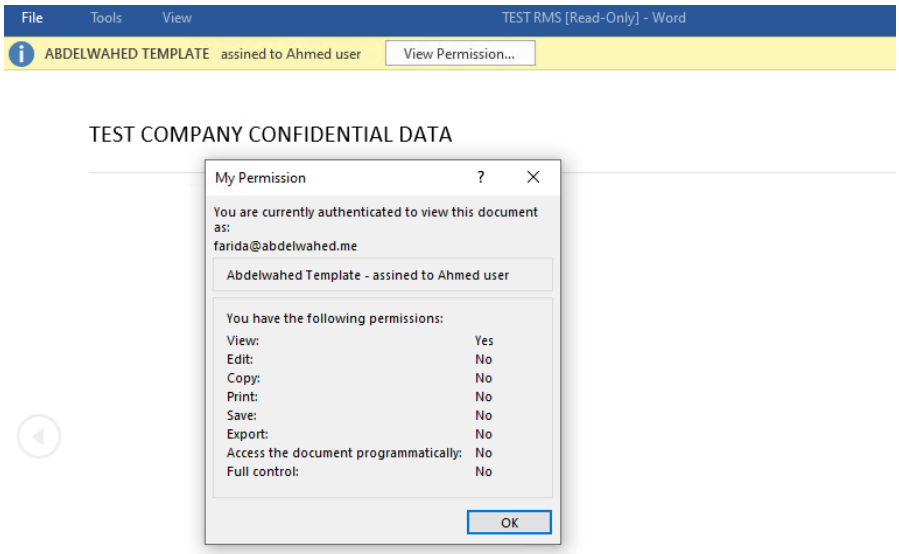




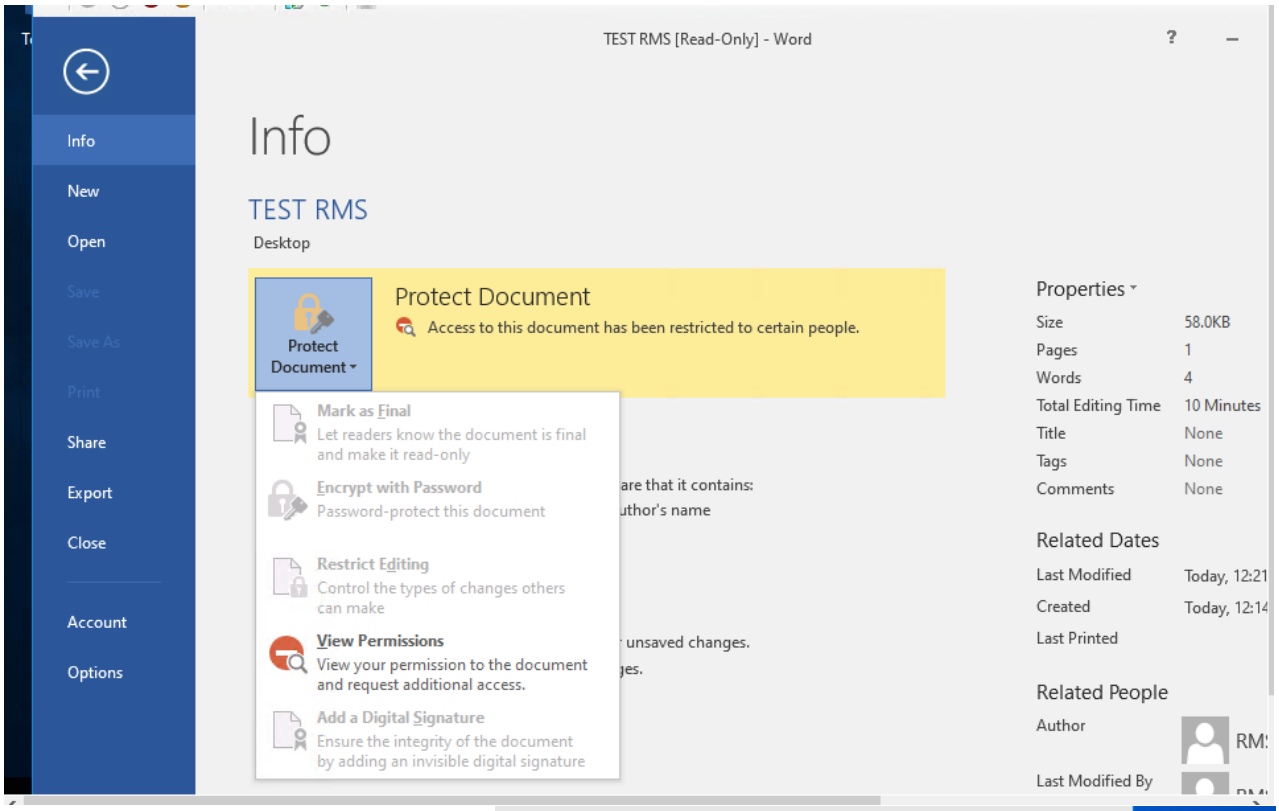
When attempting to open the file on a client computer after logging in as user Farida, it prompts for credentials.



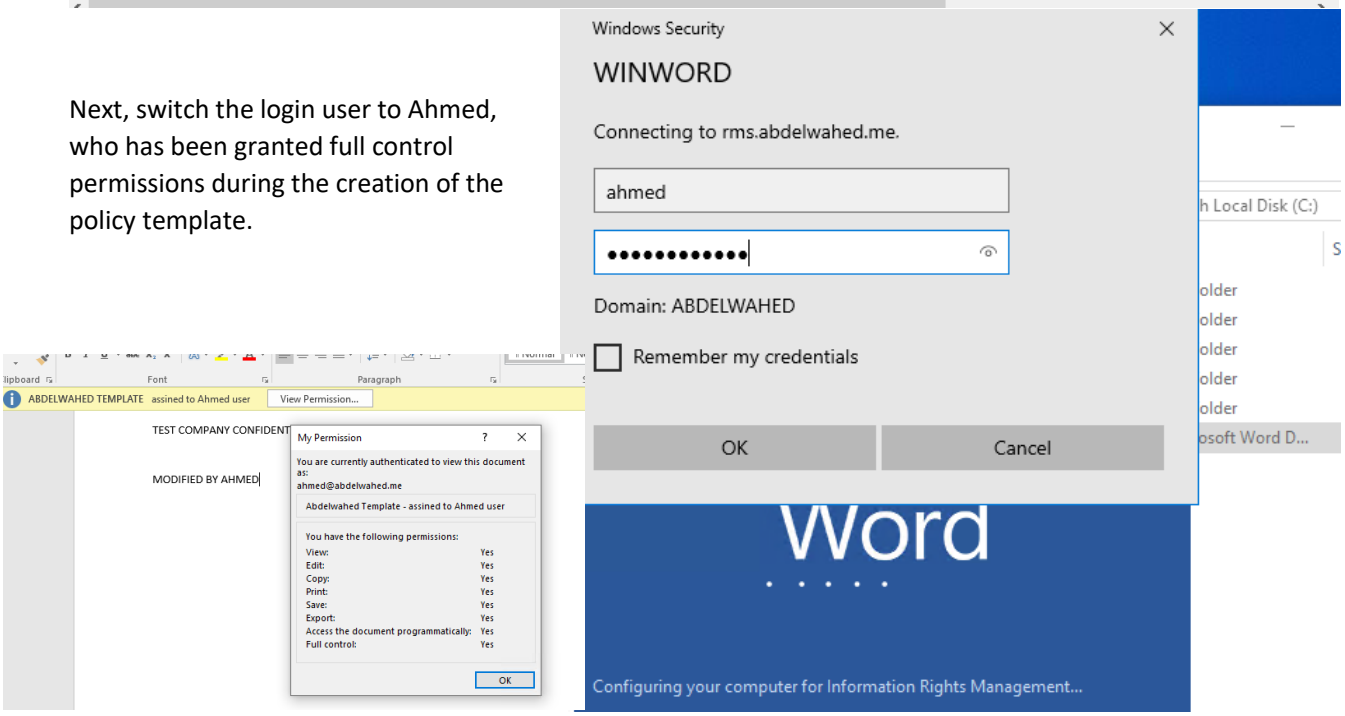
view permission to check your allowed actions to this file



Additionally, you're not able to modify file permission settings.



Next, switch the login user to Ahmed, who has been granted full control permissions during the creation of the policy template.

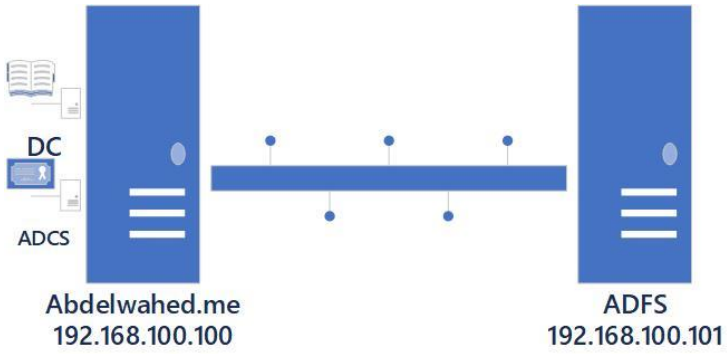


Active Directory Federation Services

Installation Prerequisites and Installation

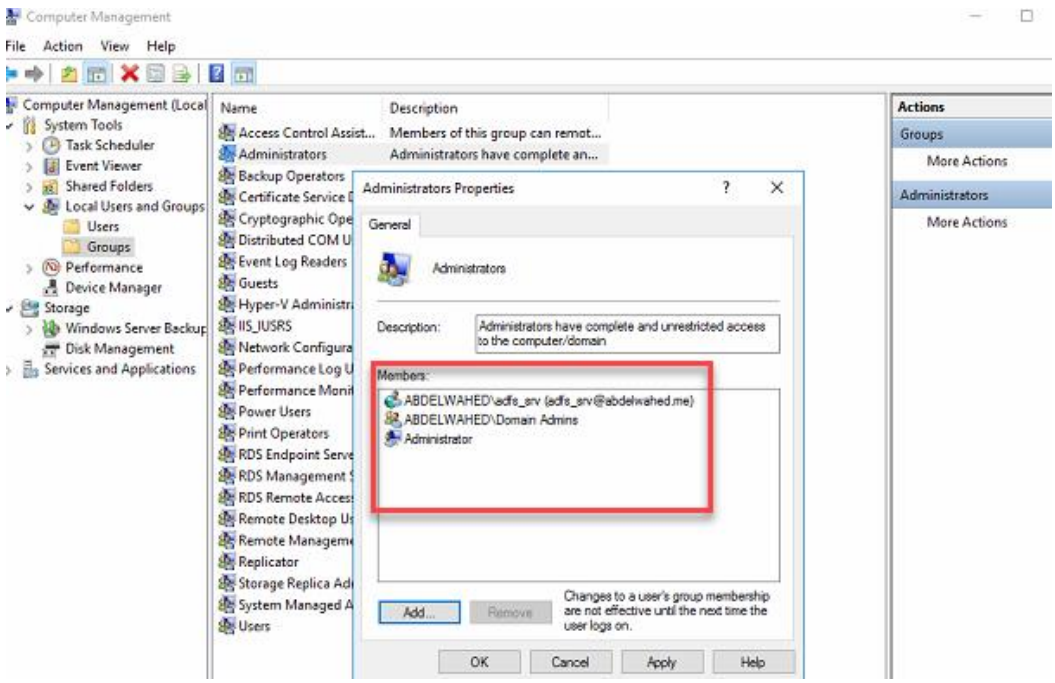
1- Joined Domain
2- SQL or WID
3- SSL Certificate (to secure chanel between DFS)
4- Enterprise administrator
5- Add domain admins as local admin group member
6- ADFS user service

Current environment

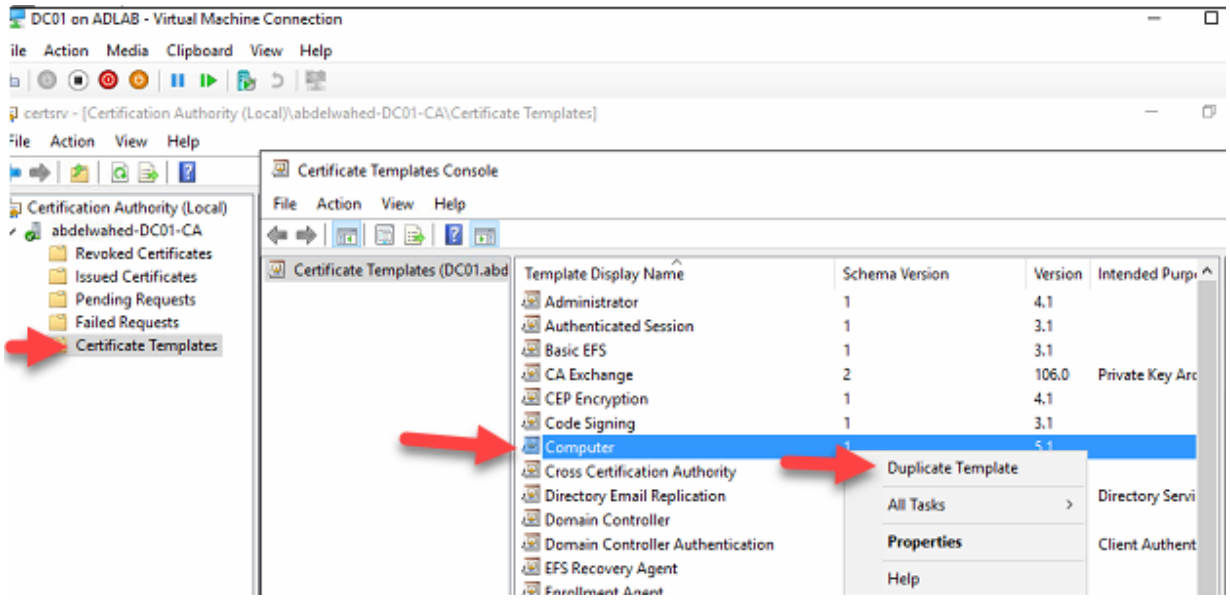


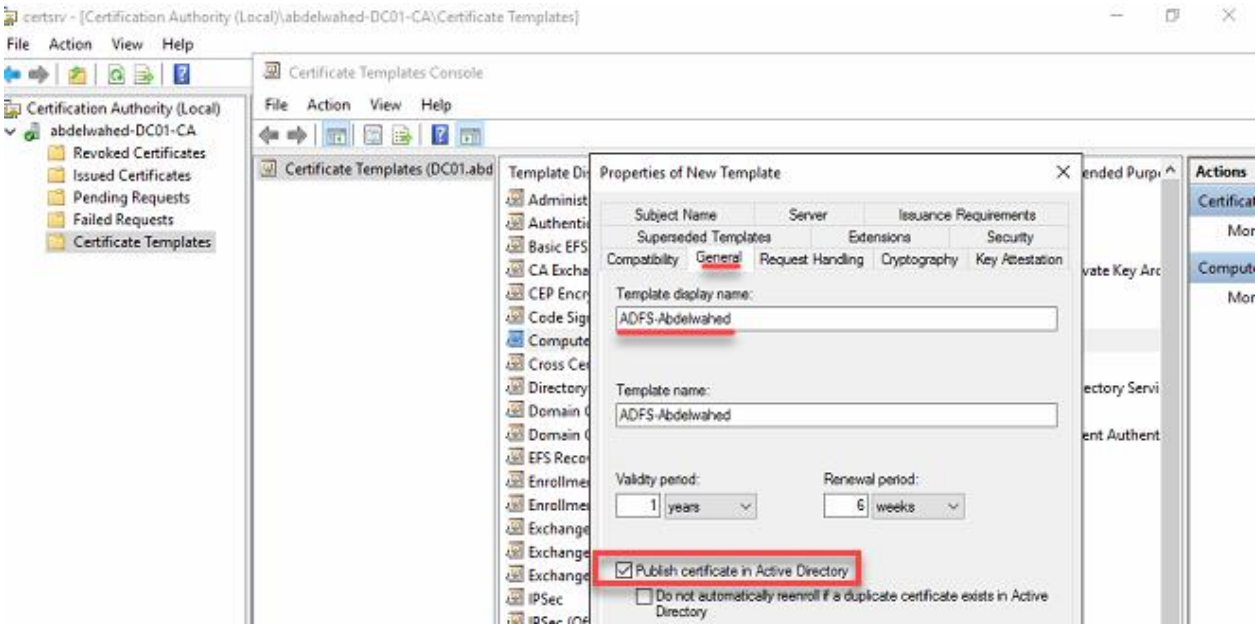
Installation:

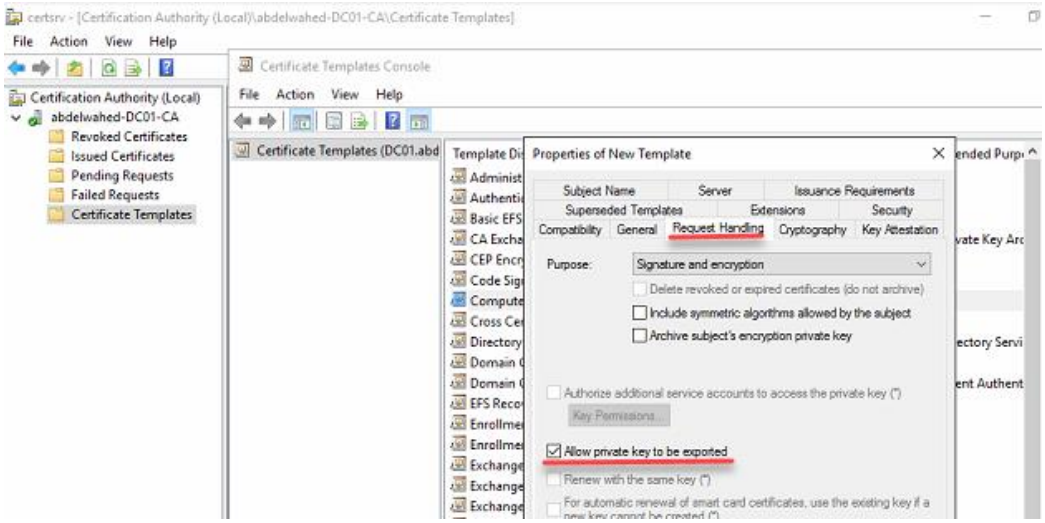
Add domain admins to ADFS local admin group and ADFS service account

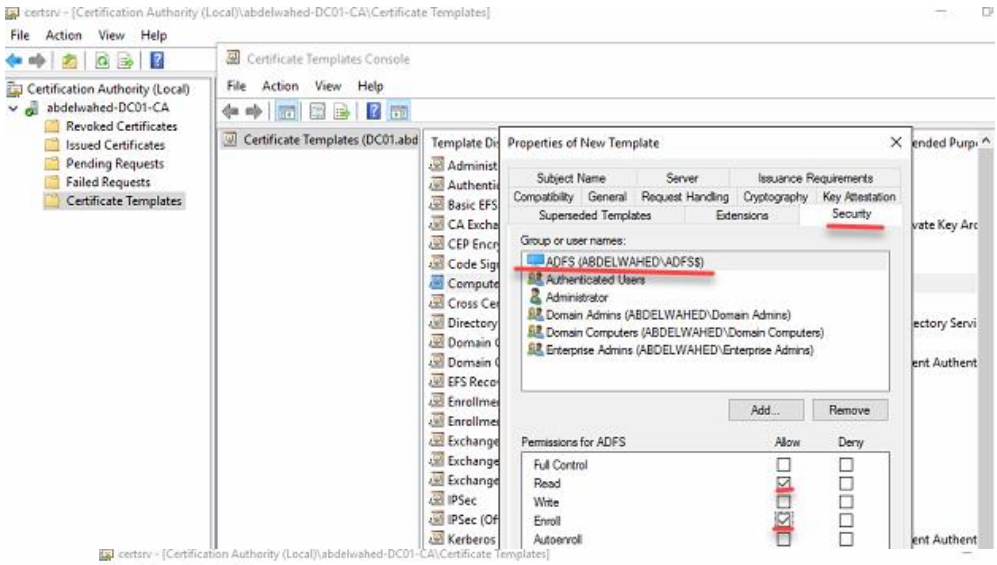


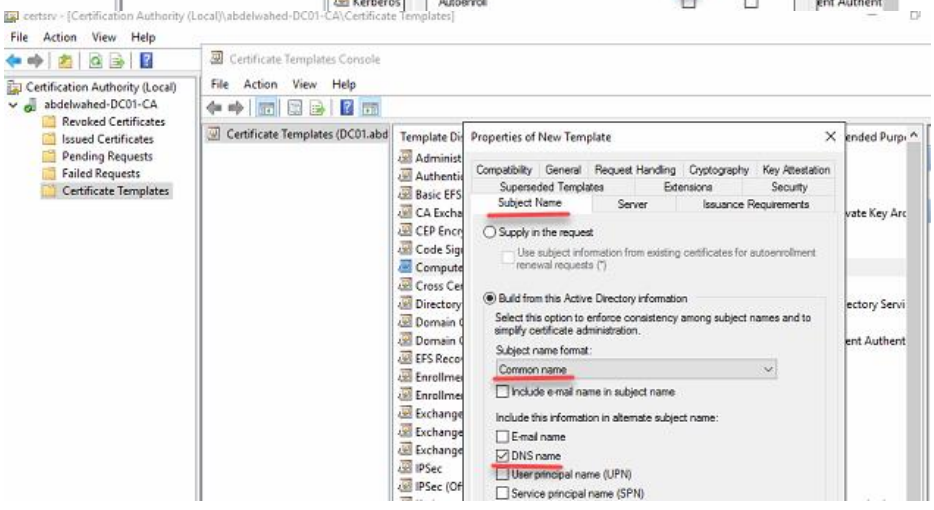
Create SSL Computer certificate from ADCS for ADFS



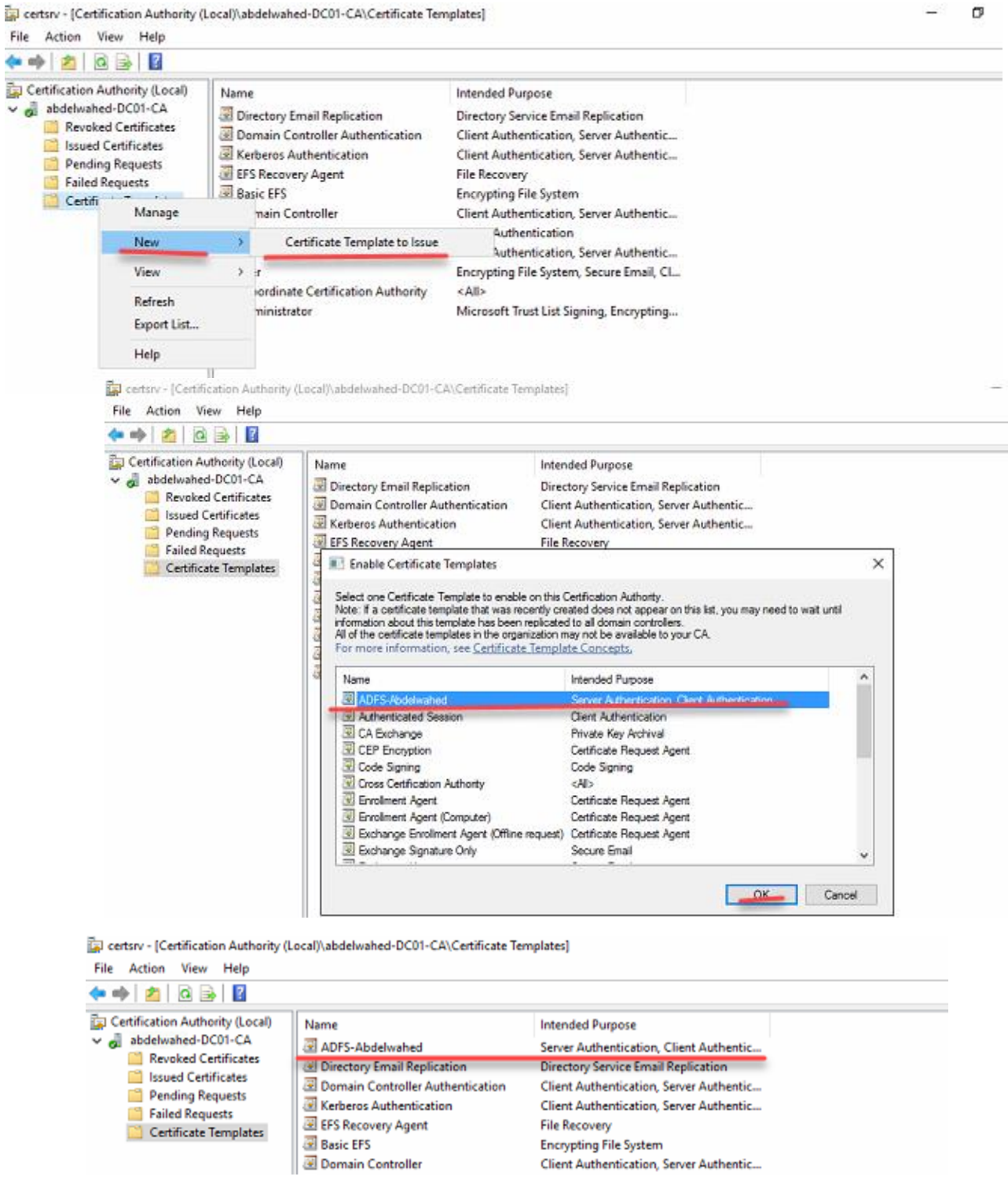



certsrv - [Certification Authority (Local)\abdelwahed-DC01-CA\Certificate Templates]
File Action View Help
Certificate Templates Console
Certification Authority (Local)
abdelwahed-DC01-CA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
Properties of New Template
Subject Name
Server
Issuance Requirements
Superseded Templates
Extensions
Security
Compatibility
General
Request Handling
Cryptography
Key Attestation
Purpose:
Signature and encryption
Include symmetric algorithms allowed by the subject
Archive subject's encryption private key
Allow private key to be exported
Renew with the same key (*)

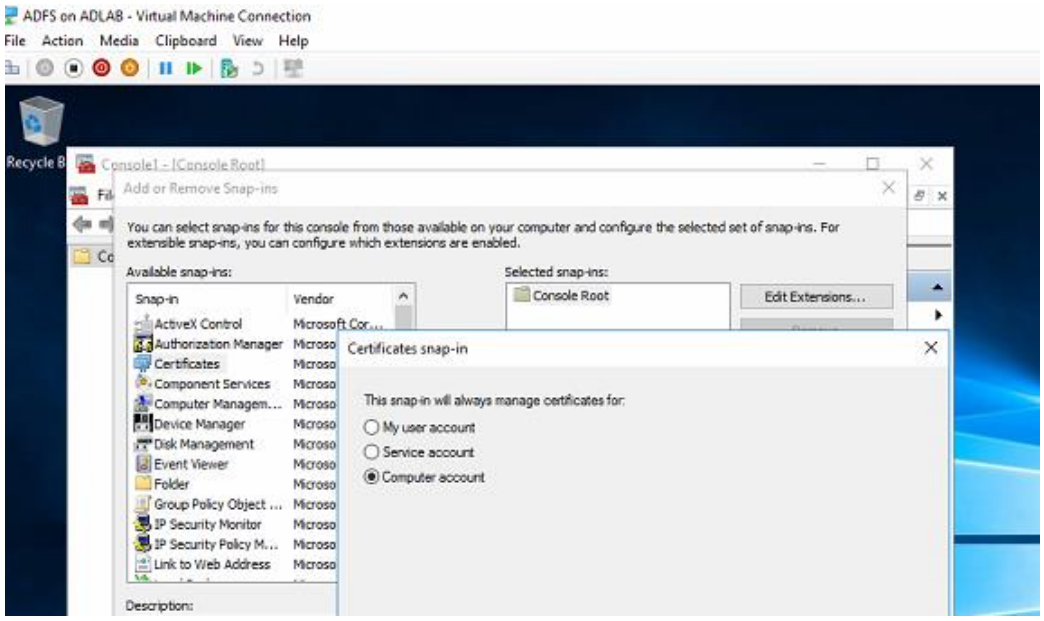

certsrv - [Certification Authority (Local)\abdelwahed-DC01-CA\Certificate Templates]
Certificate Templates Console
Properties of New Template
Security
Group or user names:
ADFS (ABDELWAHED\ADFS$)
Authenticated Users
Administrator
Domain Admins (ABDELWAHED\Domain Admins)
Domain Computers (ABDELWAHED\Domain Computers)
Enterprise Admins (ABDELWAHED\Enterprise Admins)
Add...
Remove
Permissions for ADFS
Allow
Deny
Full Control
Read
Write
Enroll
Autoenroll

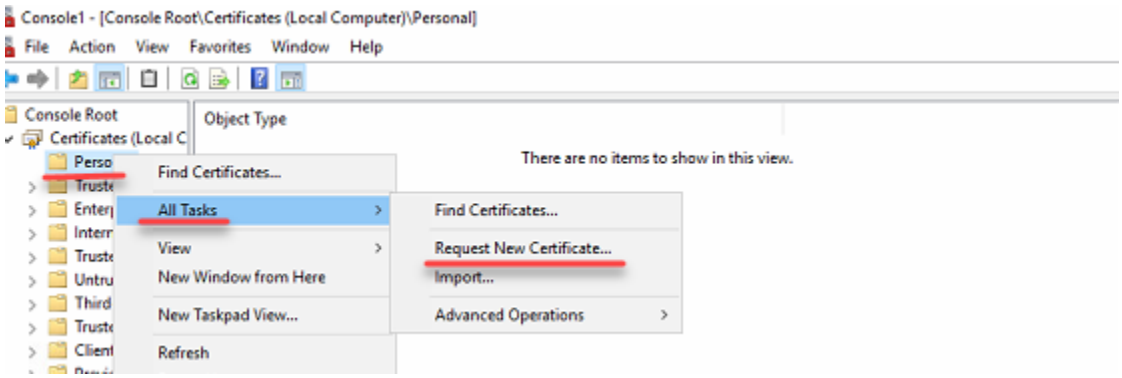

certsrv - [Certification Authority (Local)\abdelwahed-DC01-CA\Certificate Templates]
Certificate Templates Console
Properties of New Template
Subject Name
Supply in the request
Use subject information from existing certificates for autoenrollment renewal requests (*)
Build from this Active Directory information
Select this option to enforce consistency among subject names and to simplify certificate administration.
Subject name format:
Common name
Include e-mail name in subject name
Include this information in alternate subject name:
E-mail name
DNS name
User principal name (UPN)
Service principal name (SPN)

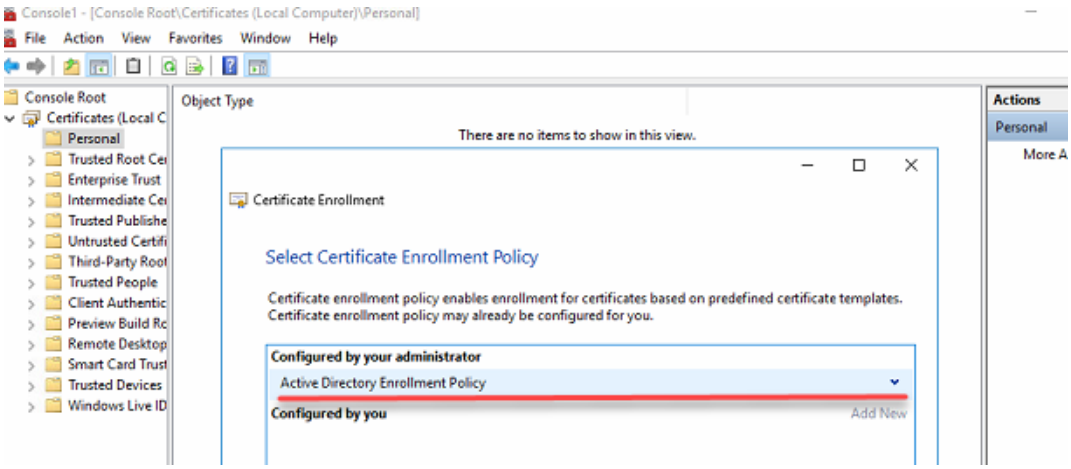
Next, click Apply and OK, and your certificate will be displayed as a Template.

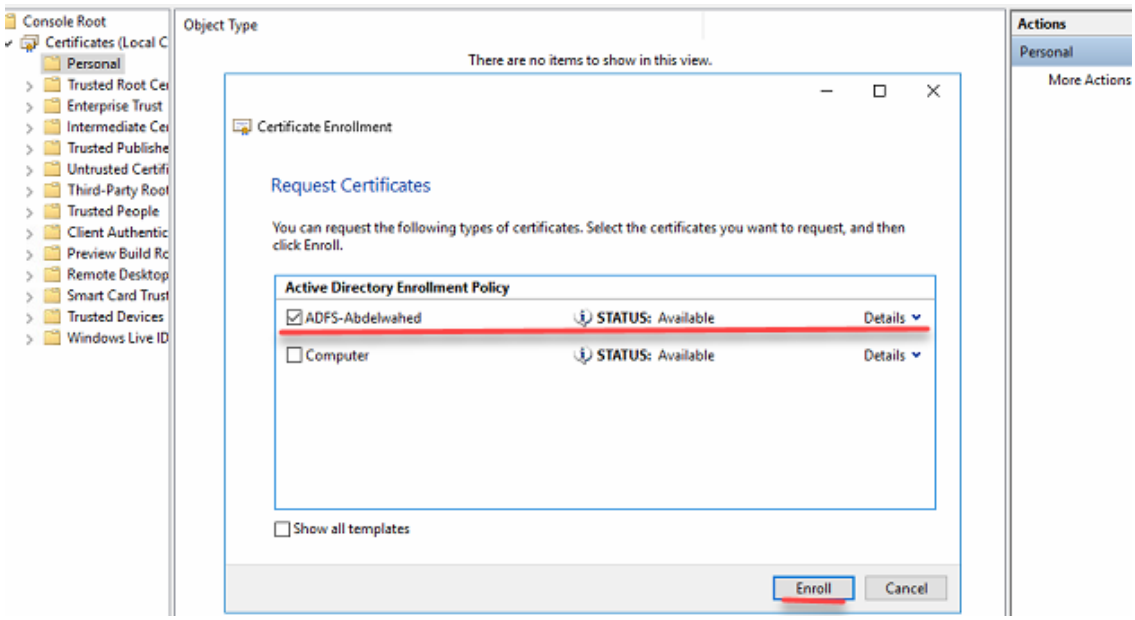


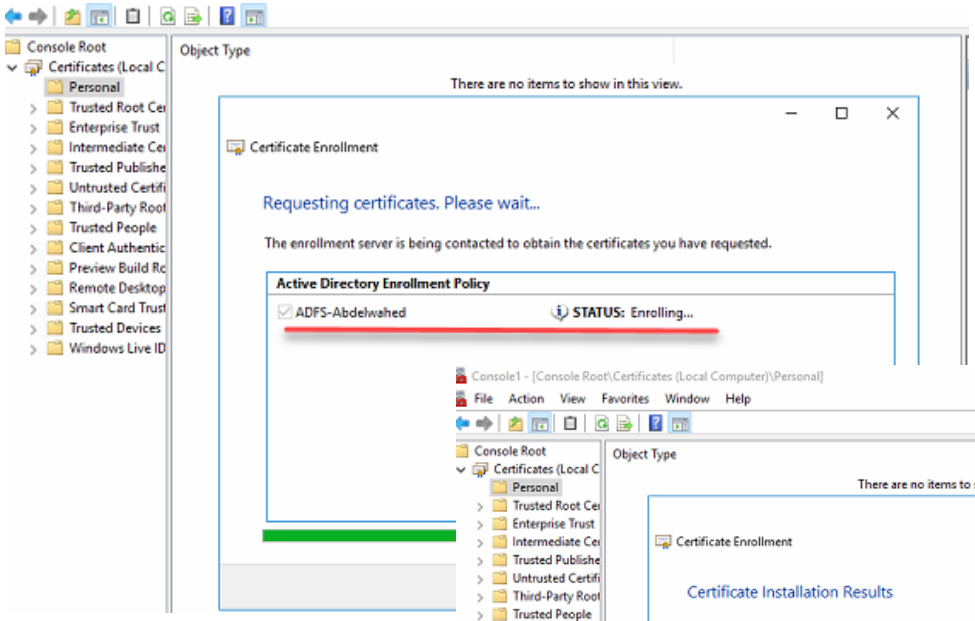
Now, request the certificate from ADFS

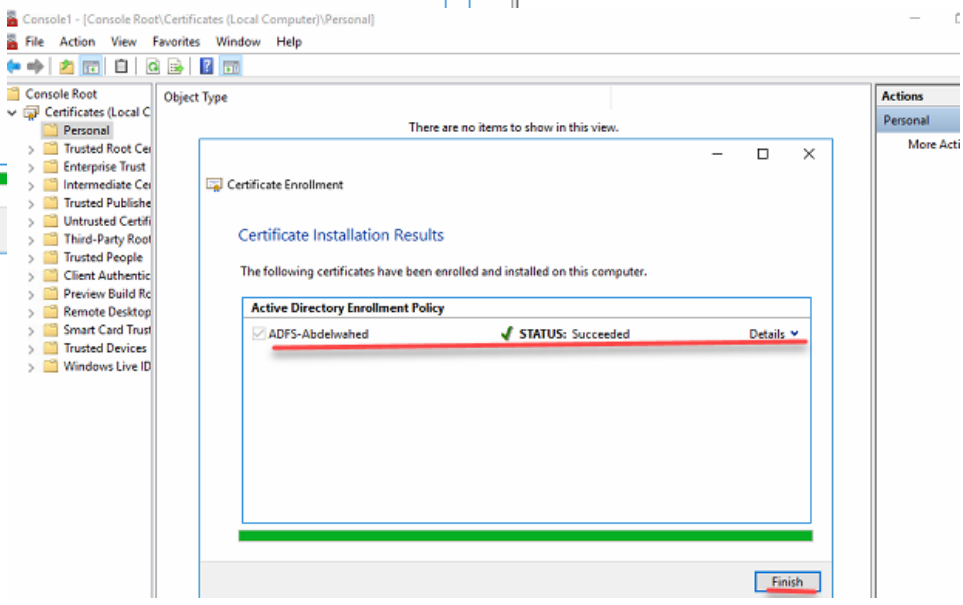


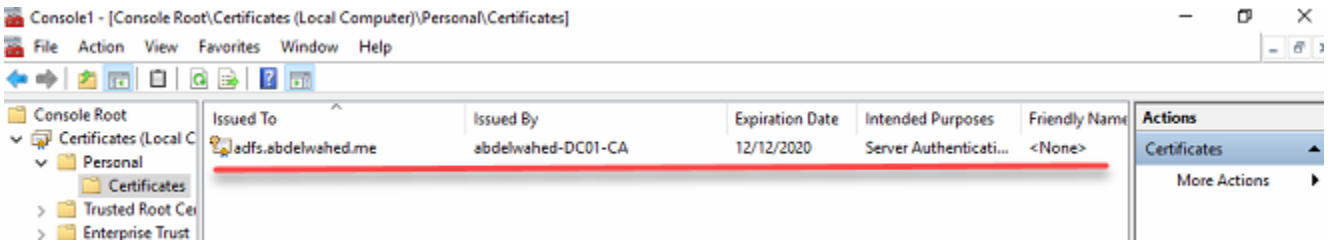




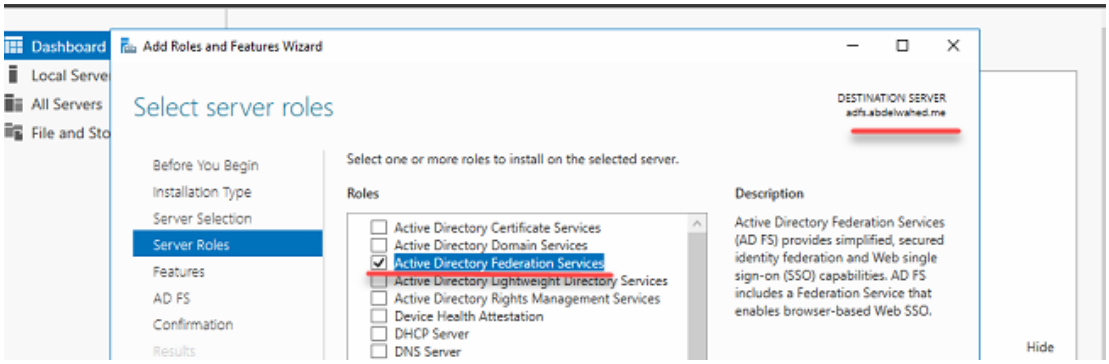

Console Root
Certificates (Local C
Personal
Trusted Root Ce
Enterprise Trust
Intermediate Ce
Trusted Publishe
Untrusted Certifi
Third-Party Root
Trusted People
Client Authentic
Preview Build Rc
Remote Desktop
Smart Card Trust
Trusted Devices
Windows Live ID
Object Type
There are no items to show in this view.
Actions
Personal
More Actions
Certificate Enrollment
Request Certificates
You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.
Active Directory Enrollment Policy
ADFS-Abdelwahed
STATUS: Available
Details
Computer
STATUS: Available
Details
Show all templates
Enroll
Cancel

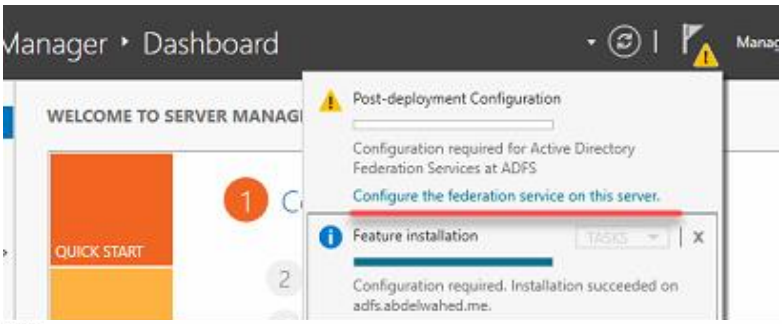

Console Root
Certificates (Local C
Personal
Trusted Root Ce
Enterprise Trust
Intermediate Ce
Trusted Publishe
Untrusted Certifi
Third-Party Root
Trusted People
Client Authentic
Preview Build Rc
Remote Desktop
Smart Card Trust
Trusted Devices
Windows Live ID
Object Type
There are no items to show in this view.
Certificate Enrollment
Requesting certificates. Please wait...
The enrollment server is being contacted to obtain the certificates you have requested.
Active Directory Enrollment Policy
ADFS-Abdelwahed
STATUS: Enrolling...

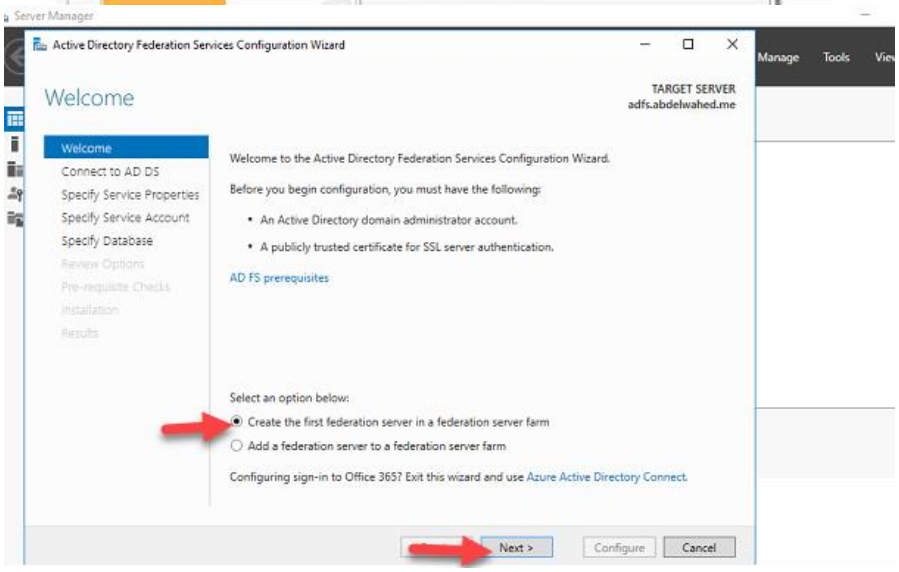

Console1 - [Console Root\Certificates (Local Computer)\Personal]
File Action View Favorites Window Help
Console Root
Certificates (Local C
Personal
Trusted Root Ce
Enterprise Trust
Intermediate Ce
Trusted Publishe
Untrusted Certifi
Third-Party Root
Trusted People
Client Authentic
Preview Build Rc
Remote Desktop
Smart Card Trust
Trusted Devices
Windows Live ID
Object Type
There are no items to show in this view.
Actions
Personal
Certificate Enrollment
Certificate Installation Results
The following certificates have been enrolled and installed on this computer.
Active Directory Enrollment Policy
ADFS-Abdelwahed
STATUS: Succeeded
Details
Finish

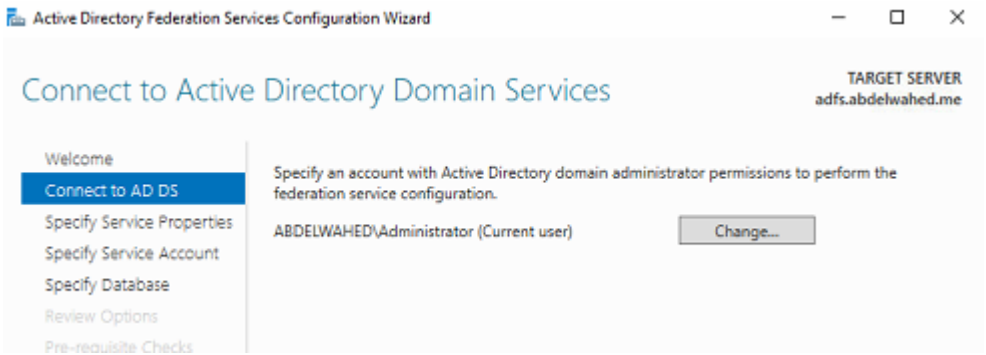


Install ADFS role

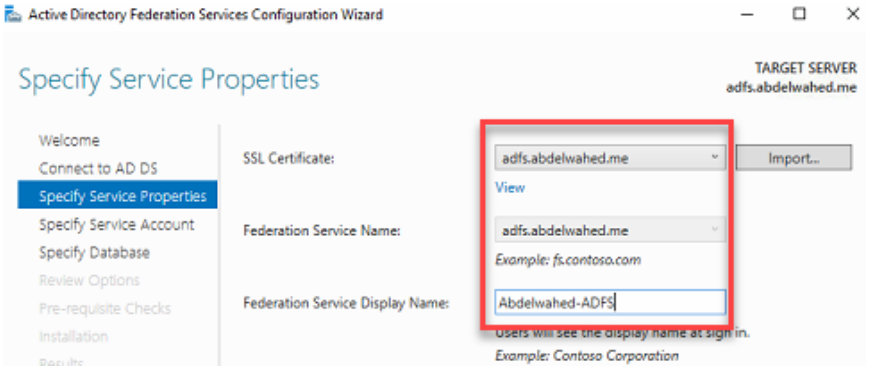




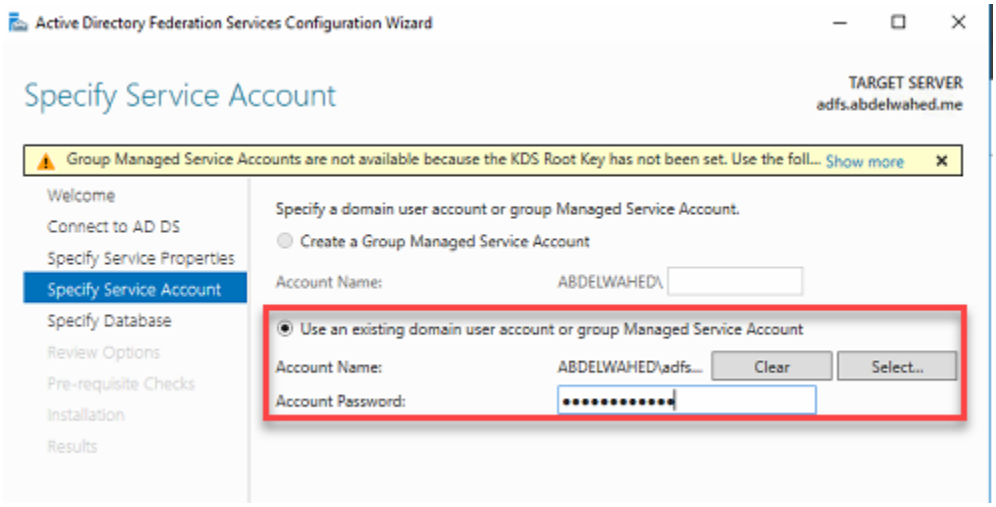




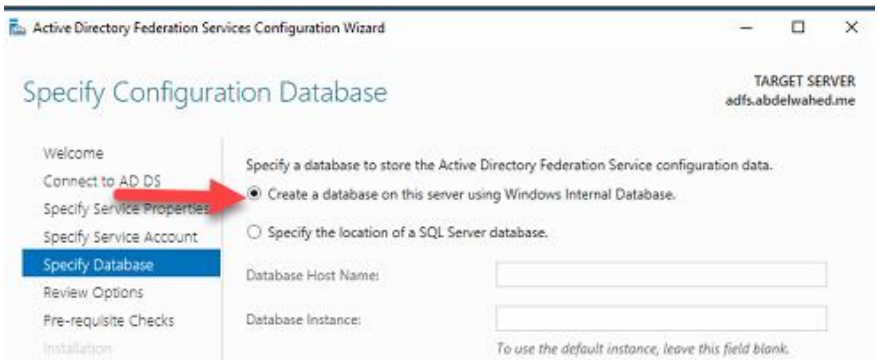
Add display name

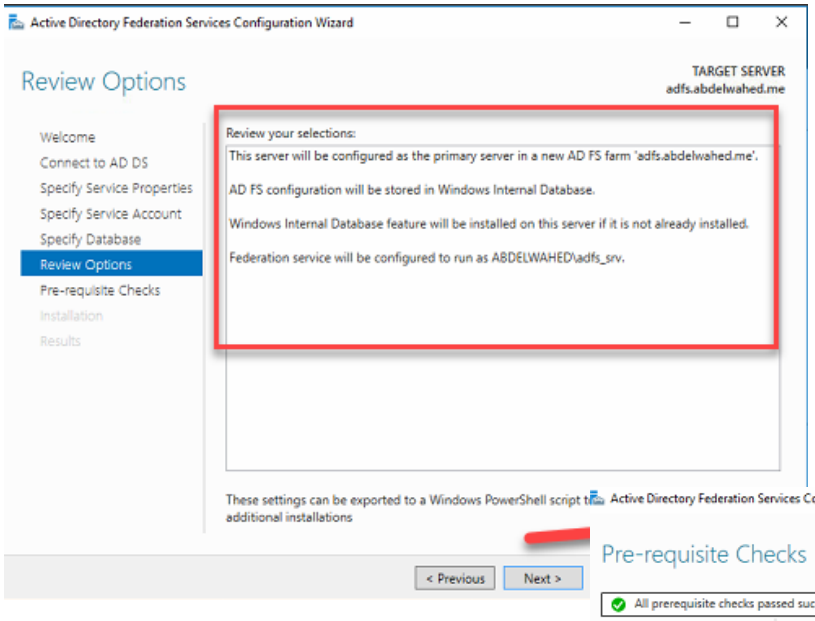


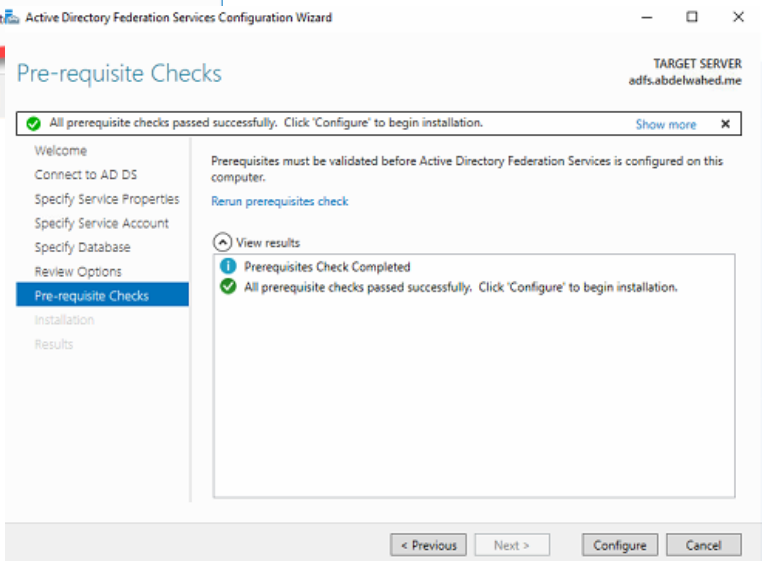
add service account for ADFS

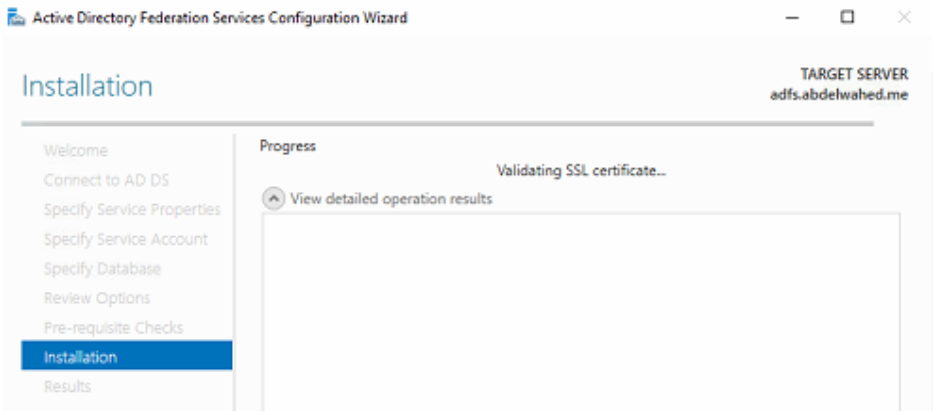


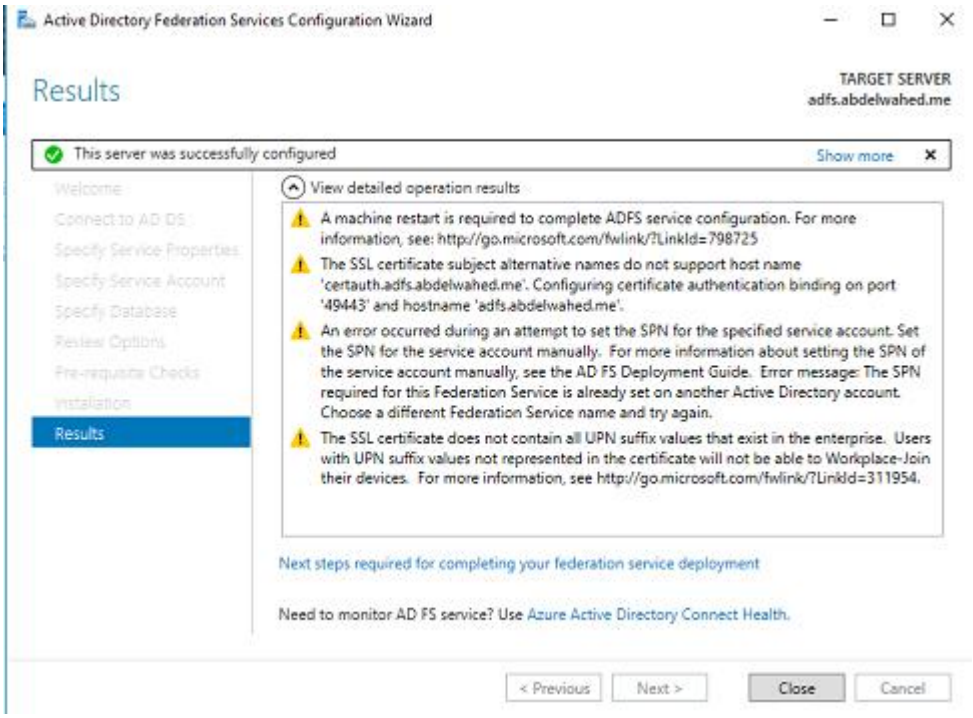
There are instances where articles mention that WID has a limitation of only 5 servers in a farm, but the Windows Server 2012 R2 documentation indicates a farm can contain up to 30 servers, confirming this larger number is possible. Indeed, for large organizations planning to deploy about 30 servers, it would be typical to use SQL in such a setup.





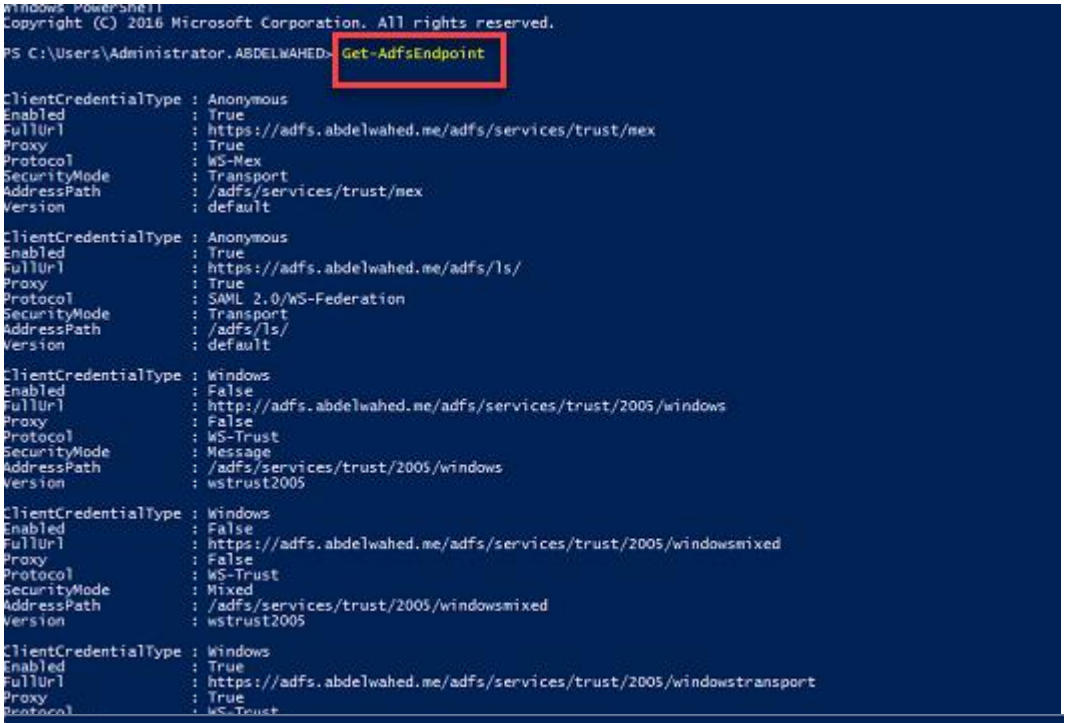






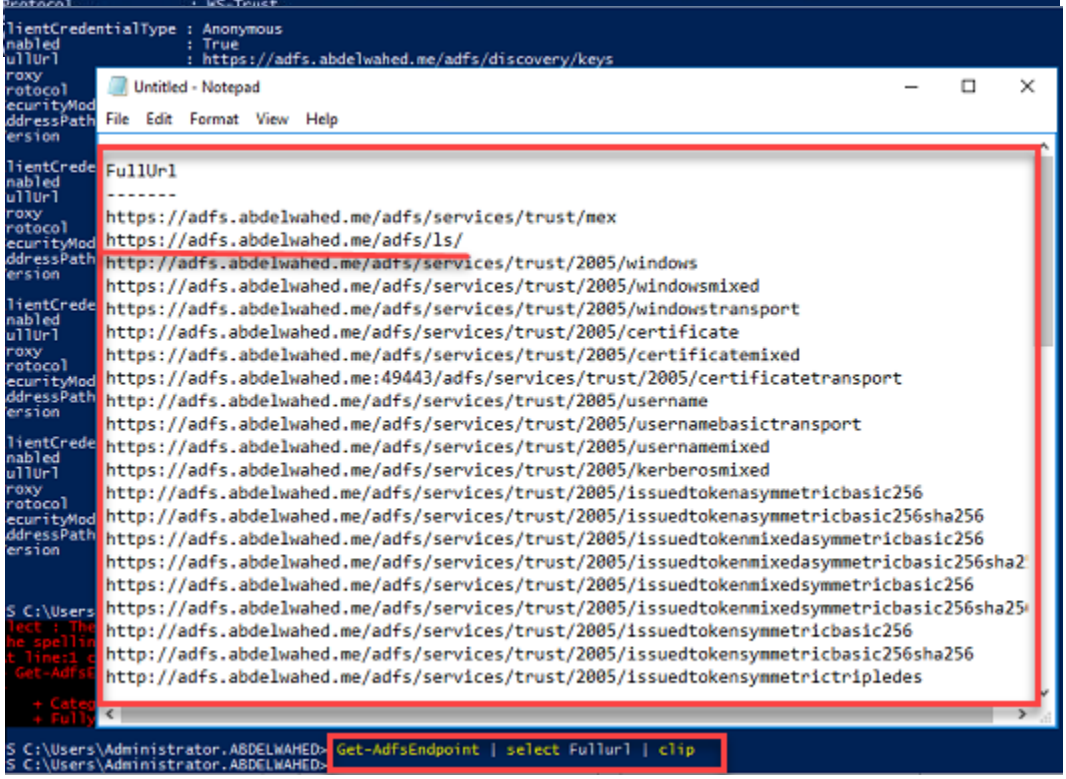
ADFS is installed and configured

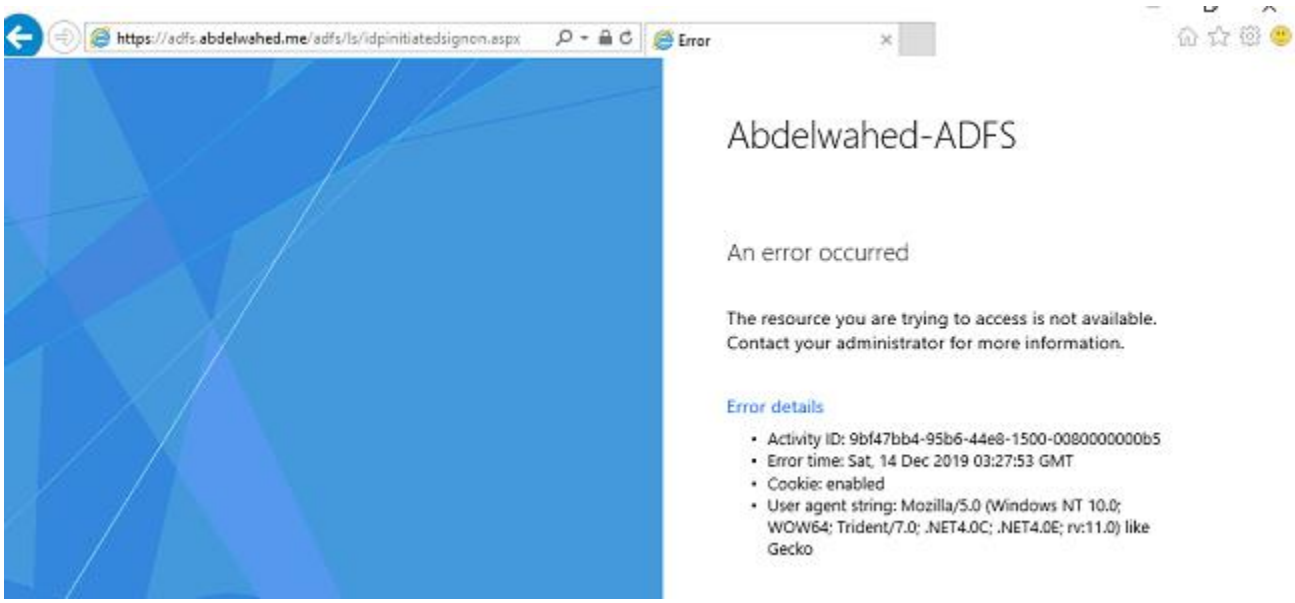
Now open PowerShell to view all ADFS URLs.



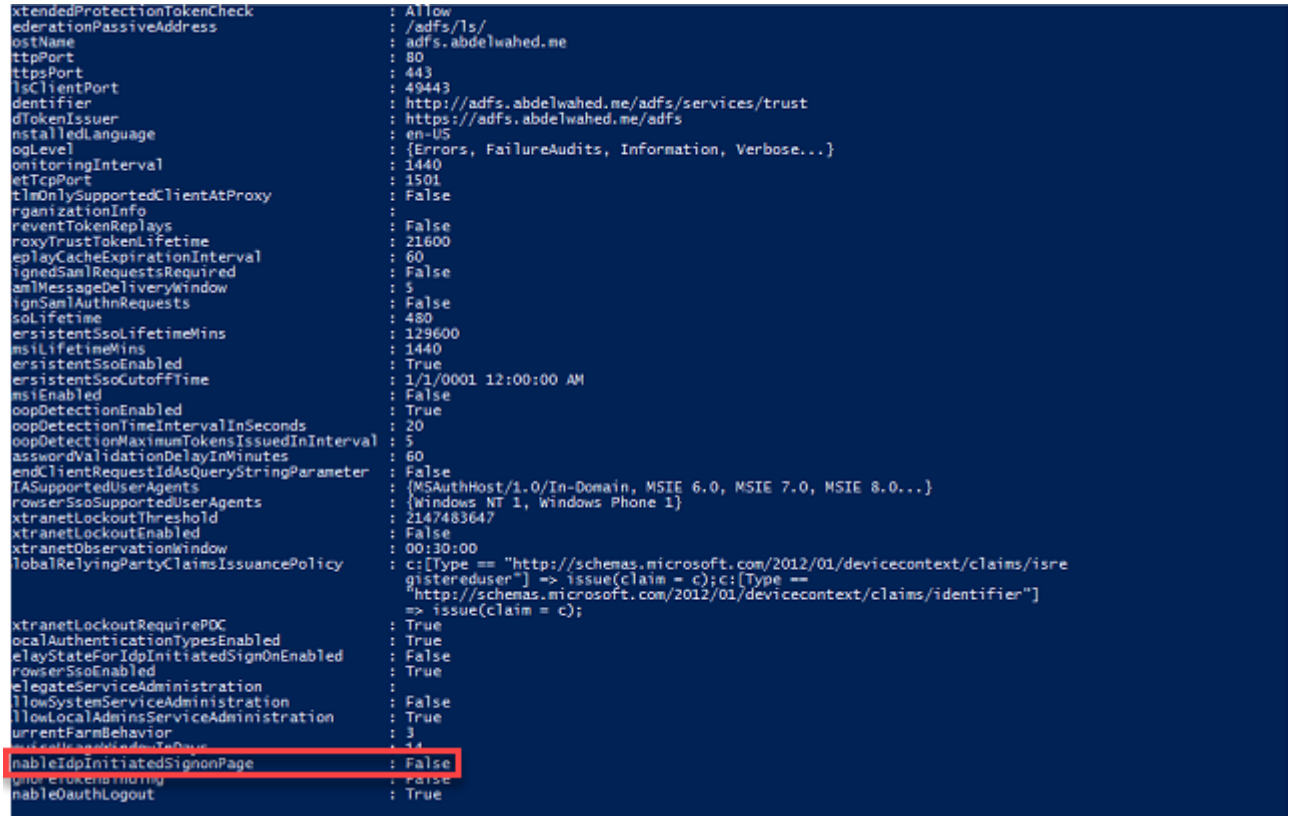
To save a list of URLs into Notepad, execute the command below and then paste the results into Notepad:

Get-adfsEndpoints | Select Fullurl | clip



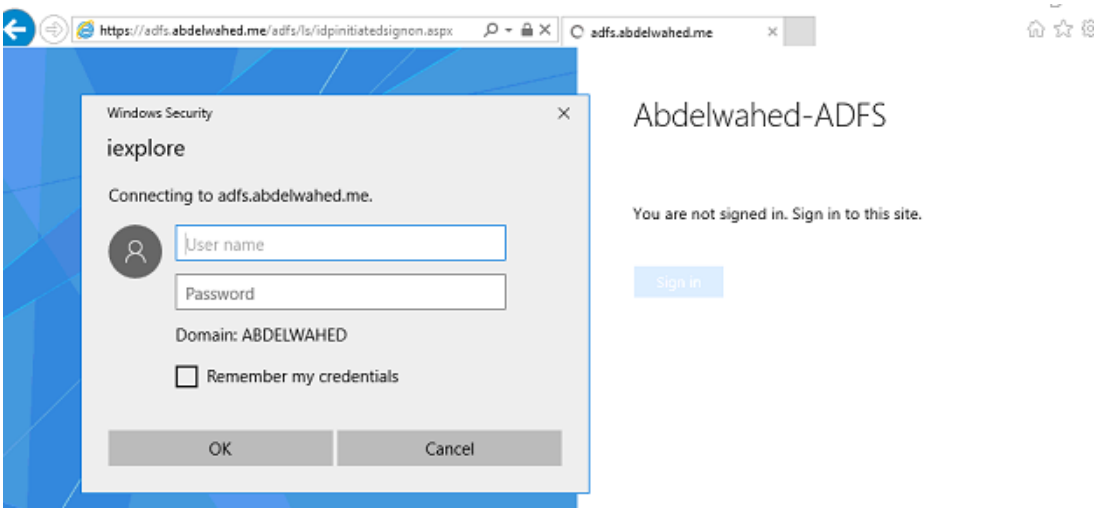


To enable it since it's not the default setting, execute Get-ADFSProperties.

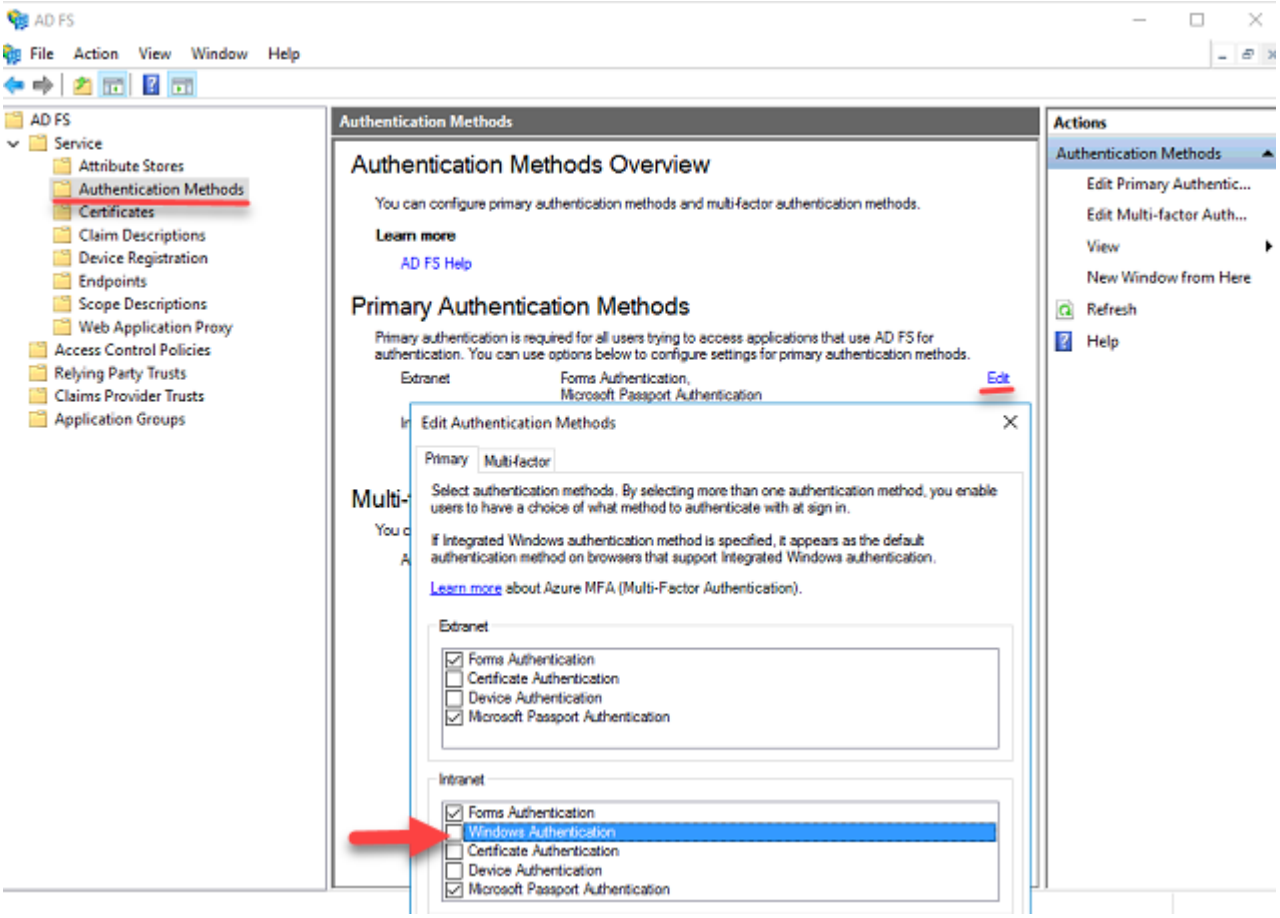


So, run this command to enable it: Set-ADFSProperties -EnableIDPInitiatedsignonpage $true

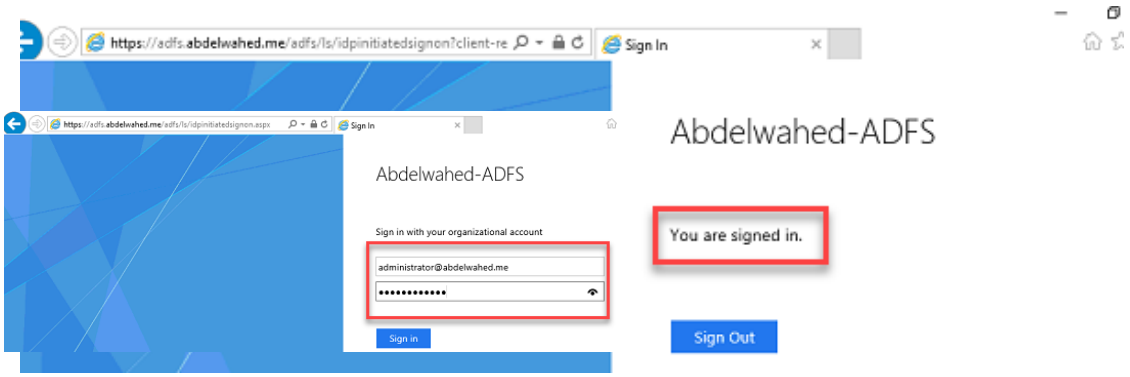
---



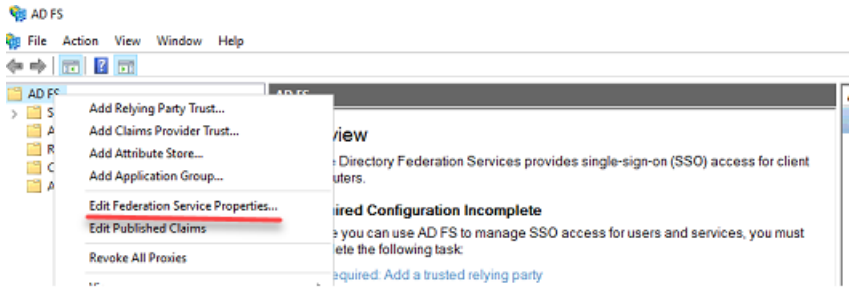
Now its work and you can change authentication type and remove windows authentication

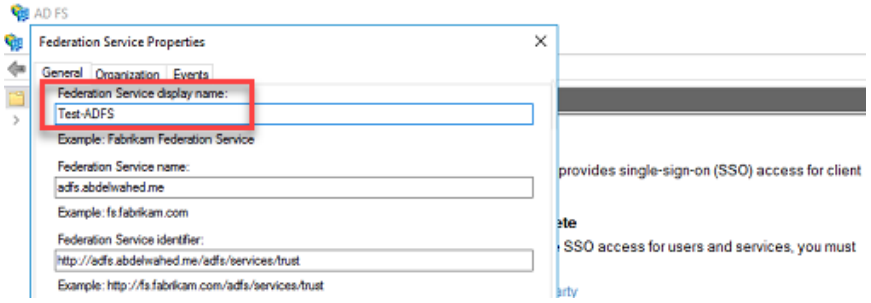


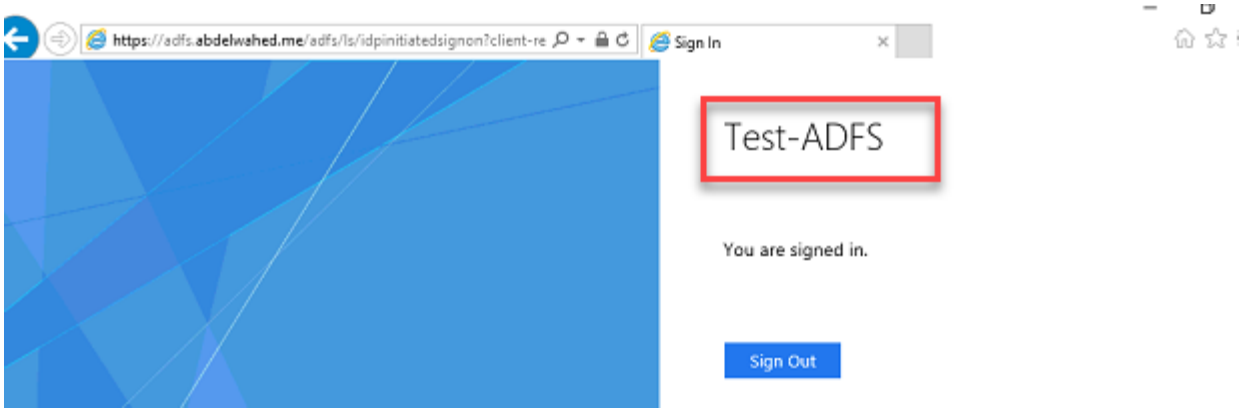
Now authentication changed



We go now to change federation service display name







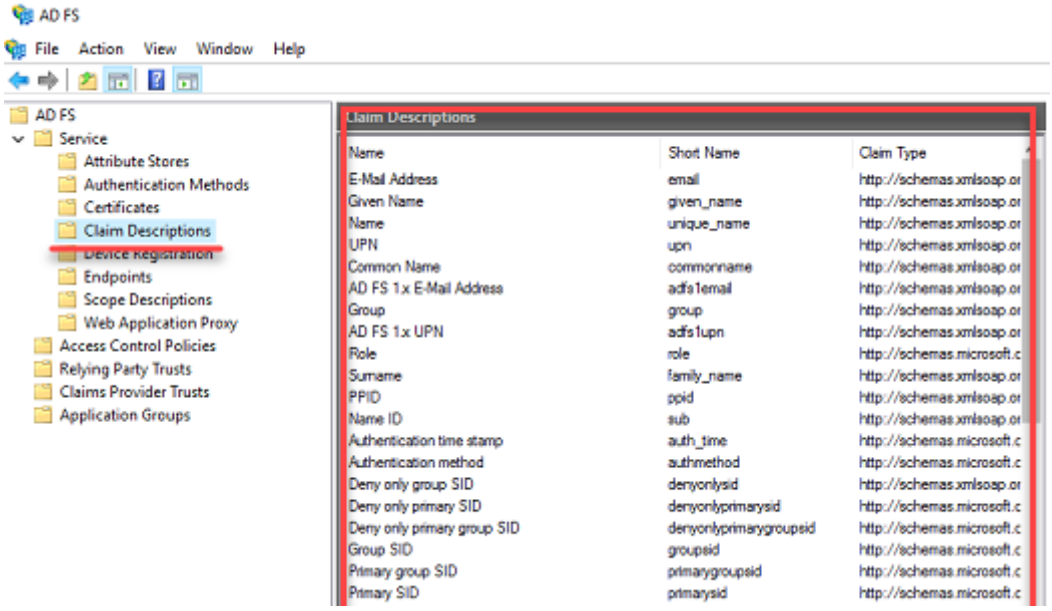
Initially, each URL endpoint is protected by a certificate you designated to the server at the time of setup.

Which type of data that will be offered for claims?

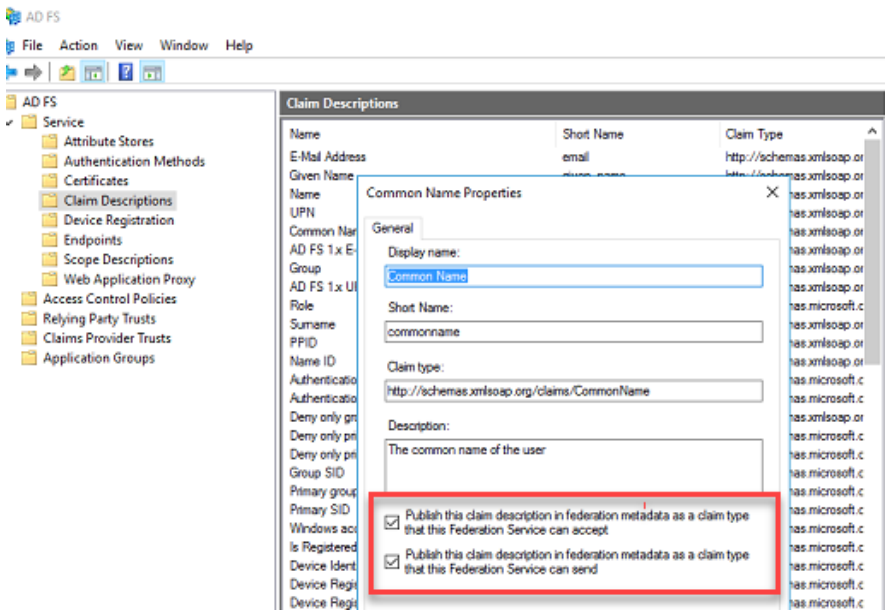
It is referred to as Metadata exchange and is accessible via the given link.

https://adfs.abdelwahed.me/adfs/services/trust/mex

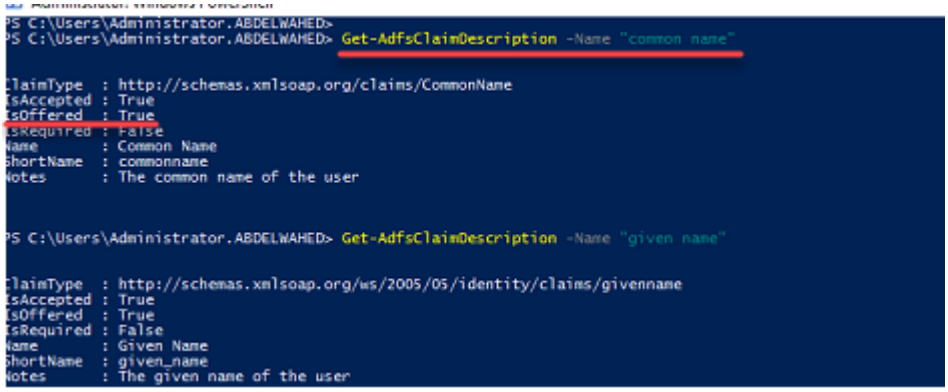
to view all claims the server can issue



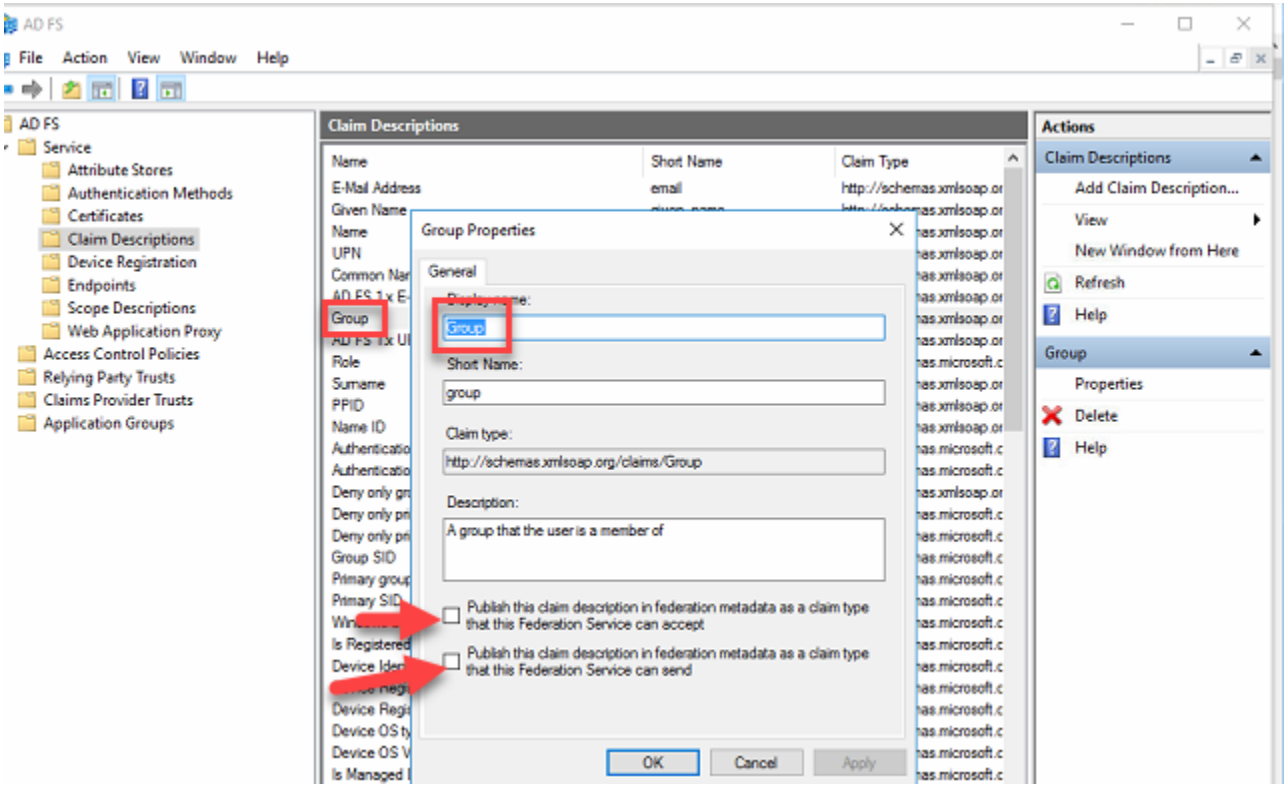
Choose any individual item and examine its characteristics.

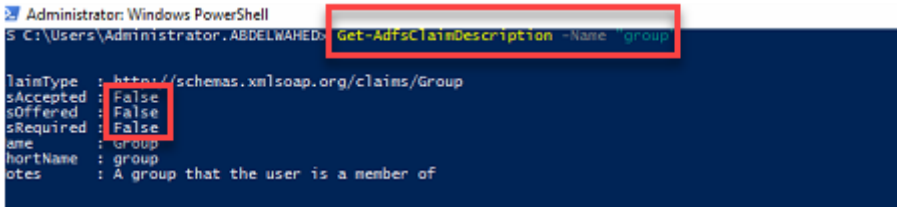


You can obtain additional information about the claim through PowerShell.



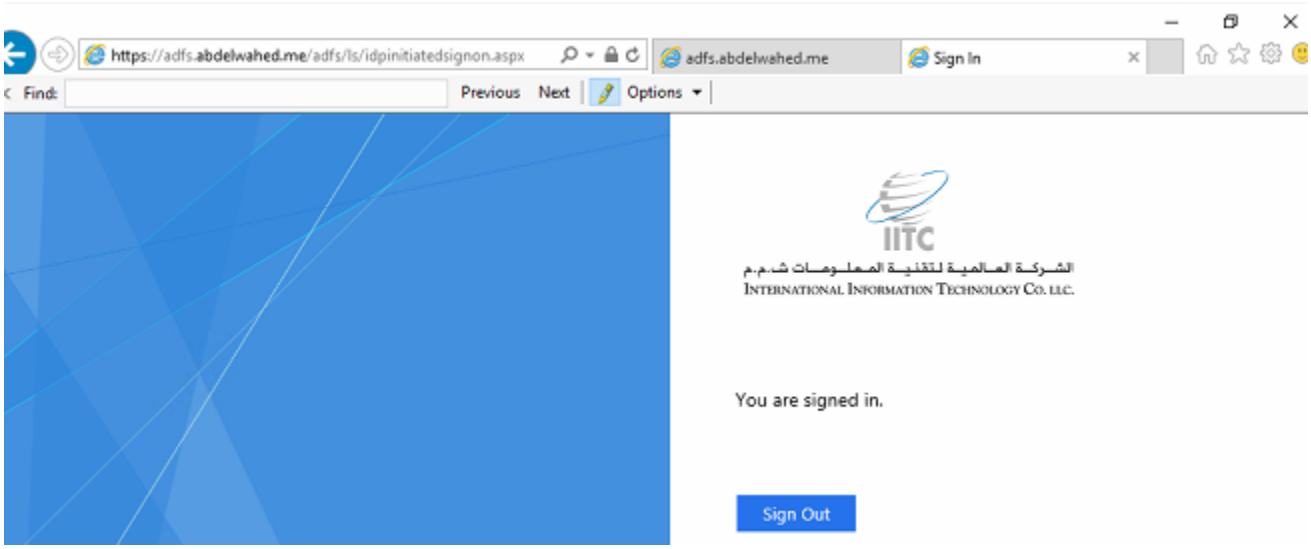
Eliminate descriptors such as "group" from the claim.





Change company logo

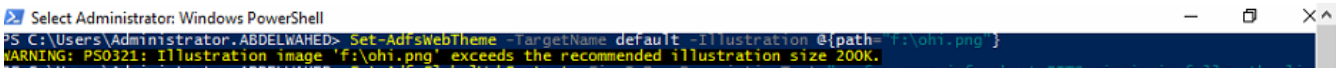
```
PS C:\Users\Administrator.ABDELWAHED> Set-AdfsWebTheme -TargetName default -Logo @{path="f:\iitc.png"}
WARNING: PS0322: Logo image 'f:\iitc.png' exceeds the recommended logo size 10K.
```



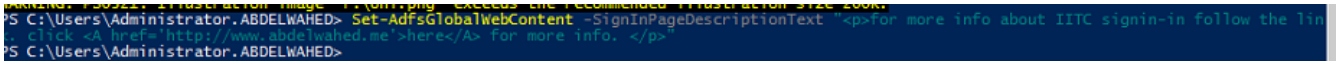
recommended the dimensions for the logo to be 260x35 @ 96 dpi with a file size of no greater than 10 KB.

Change the Illustration

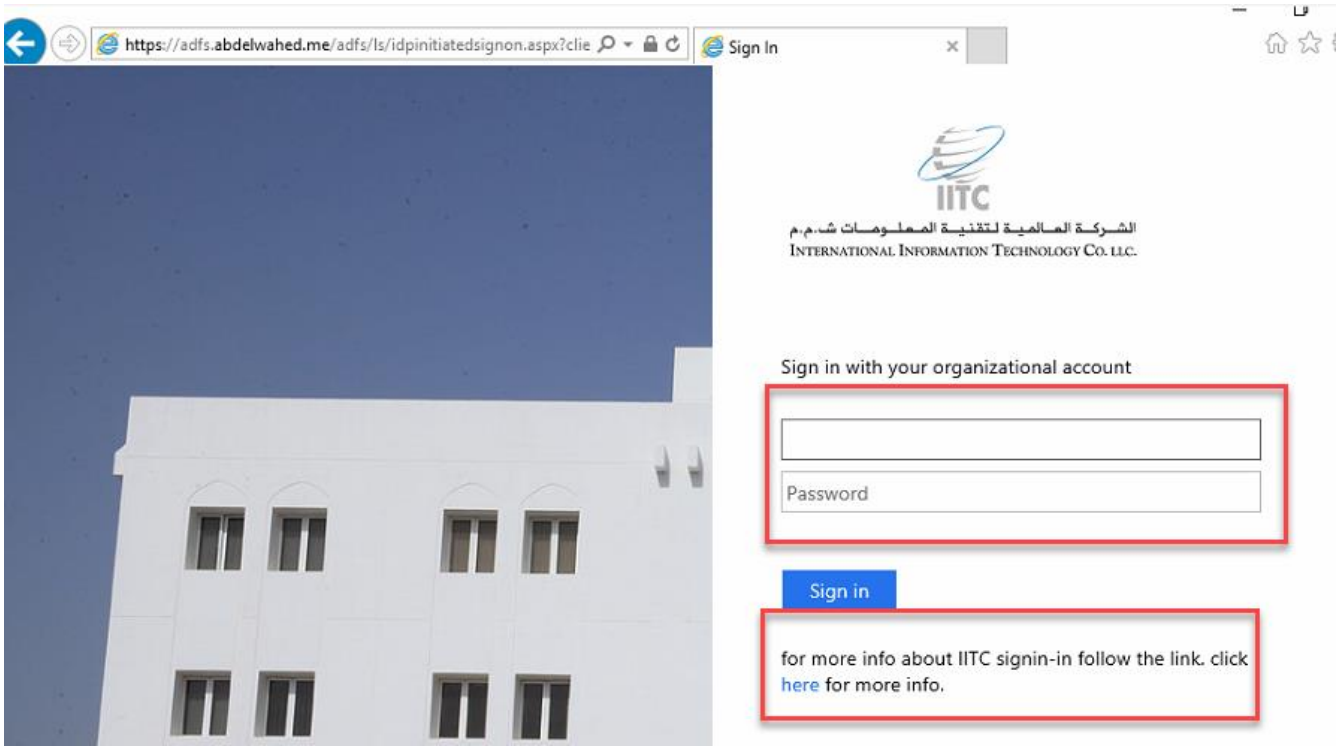
recommended the dimensions for the illustration to be 1420x1080 pixels @ 96 DPI with a file size of no greater than 200 KB.



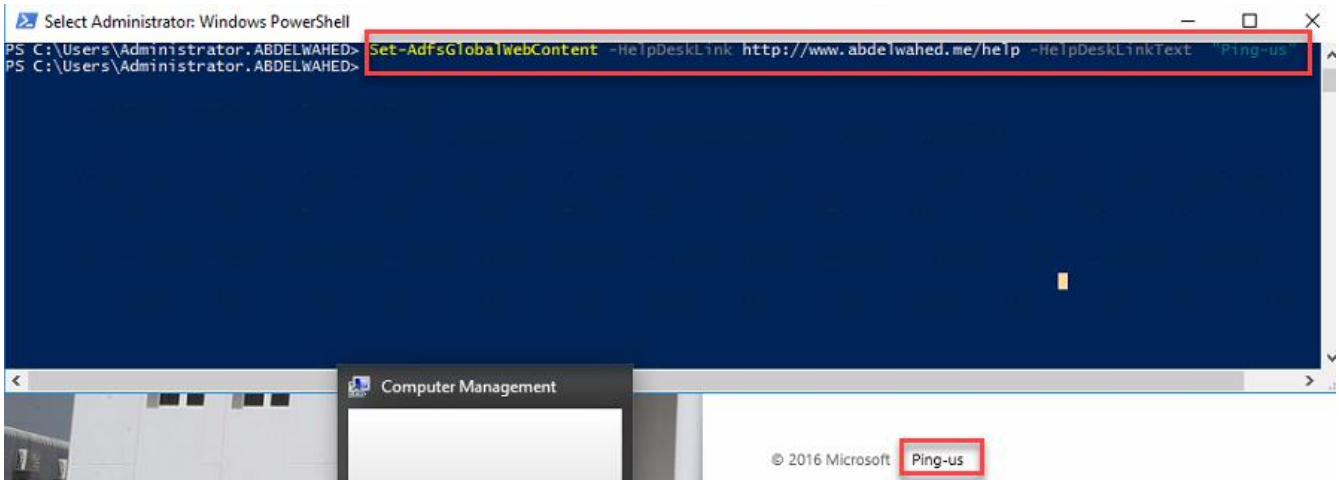
To Add sign-in page description



Set-AdfsGlobalWebContent -SignInPageDescriptionText " Sign-in to Abdelwahed requires device registration. Click <A href='www.abdelwahed.me'>here</A> for more information. "



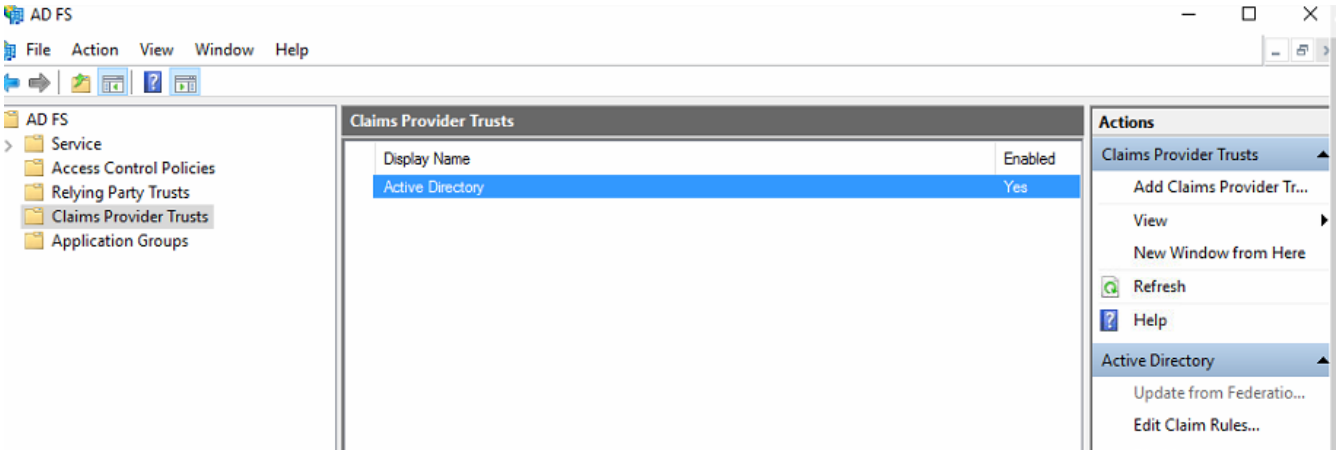
To Add a Help Desk Link



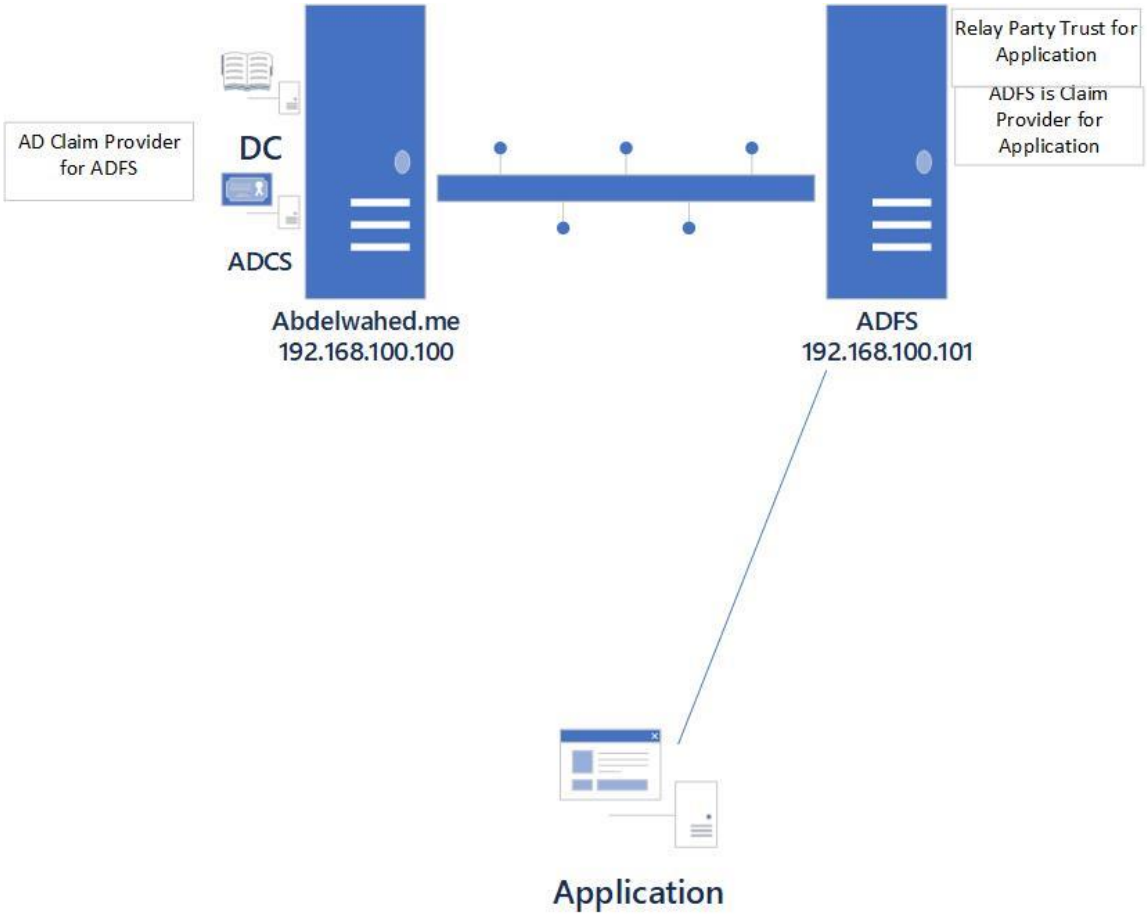
Set-AdfsGlobalWebContent -HelpDeskLink https://www.abdelwahed.me/help/ -HelpDeskLinkText “ping-us”

Claims Provider Trust

Active directory acting as claim provider for ADFS

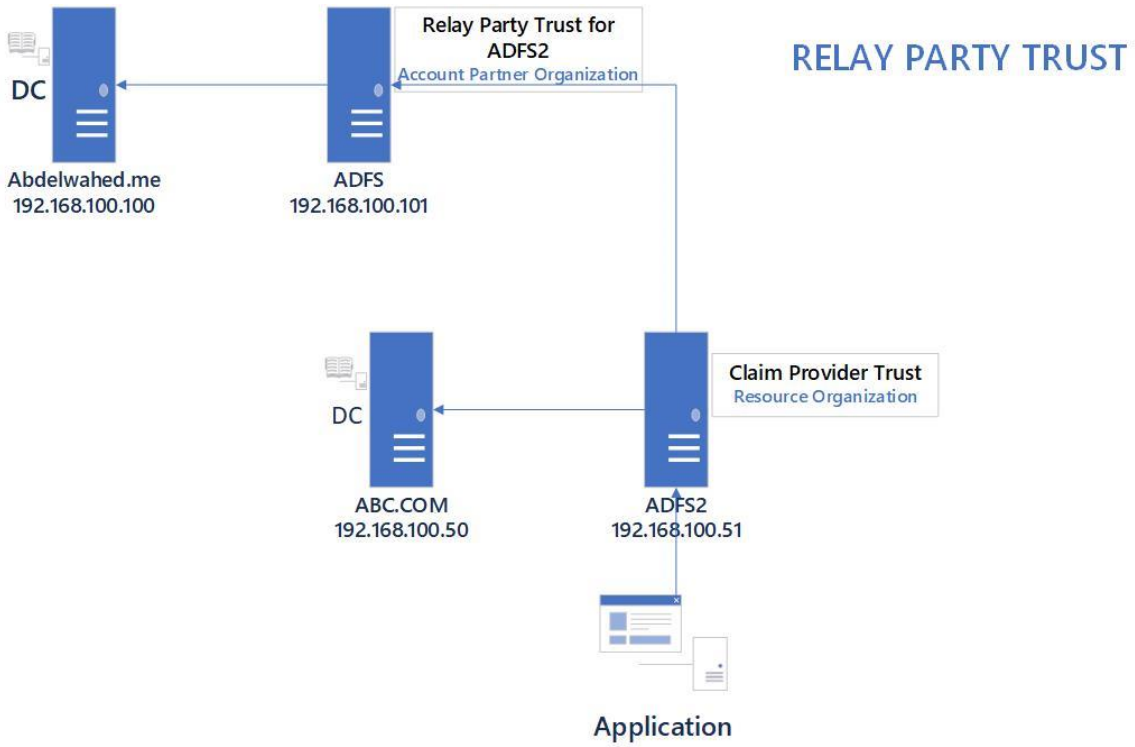


Relay Party Trust



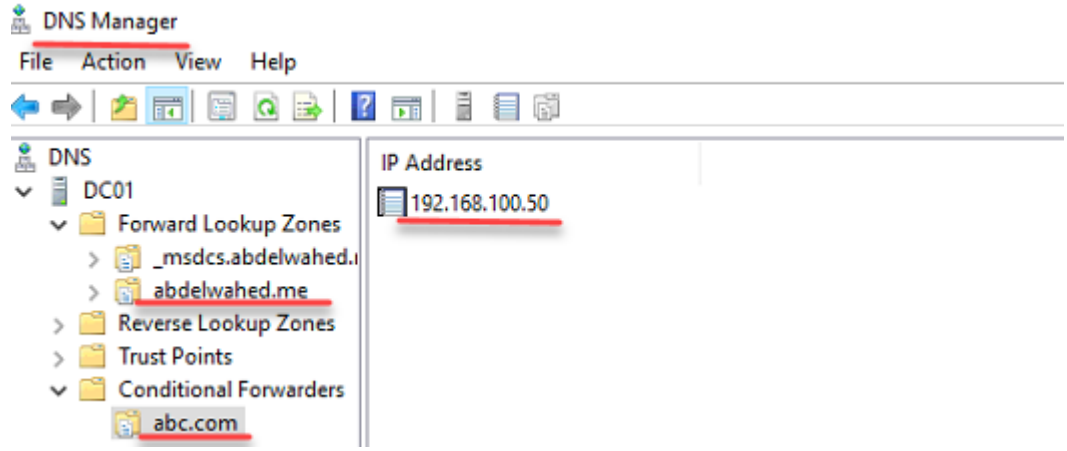
- Its means what data included in the claim
- Created in **accounts partner organization** to support users in **resource organization**
- From other side it must install claim provider trust to trust the relaying party server

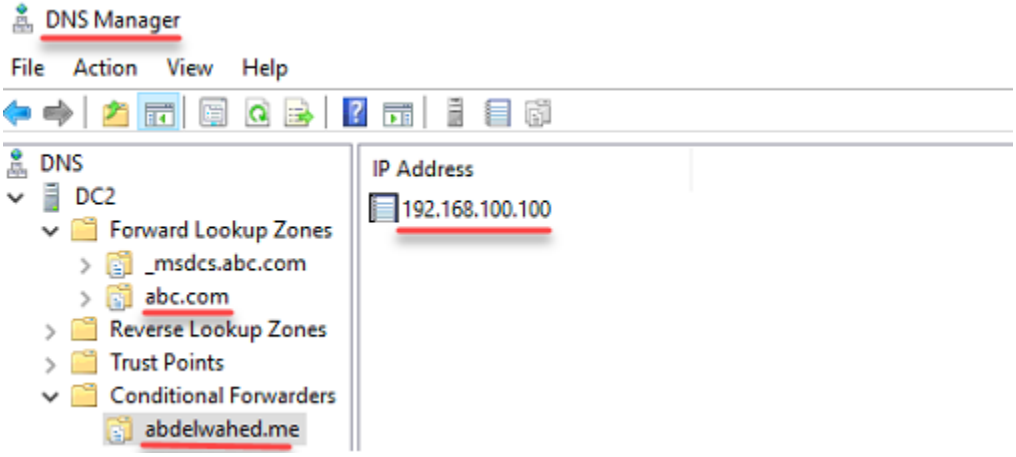
Configuring a Relying Party Trust between 2 ADFS



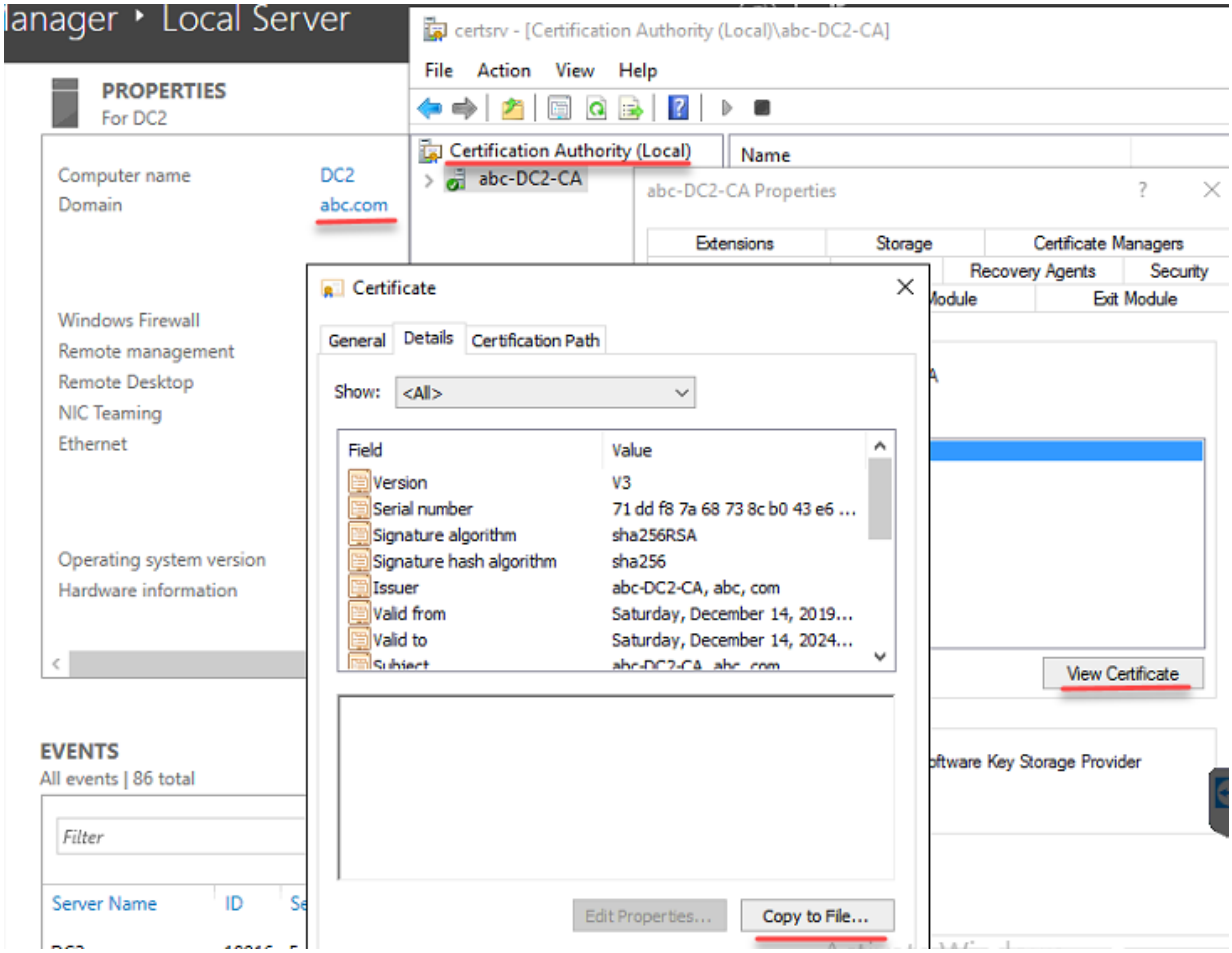
1- Create conditional forwarders between domains – DNS Level
2- Add each domain certificate as a trusted certification authority – DC Level
3- Configure Relay party trust at ADFS.ABDELWAHED.ME to support ADFS2.ABC.COM
4- Add ADFS.ABDELWAHED.ME as a Claim trust provider at ADFS2.ABC.COM

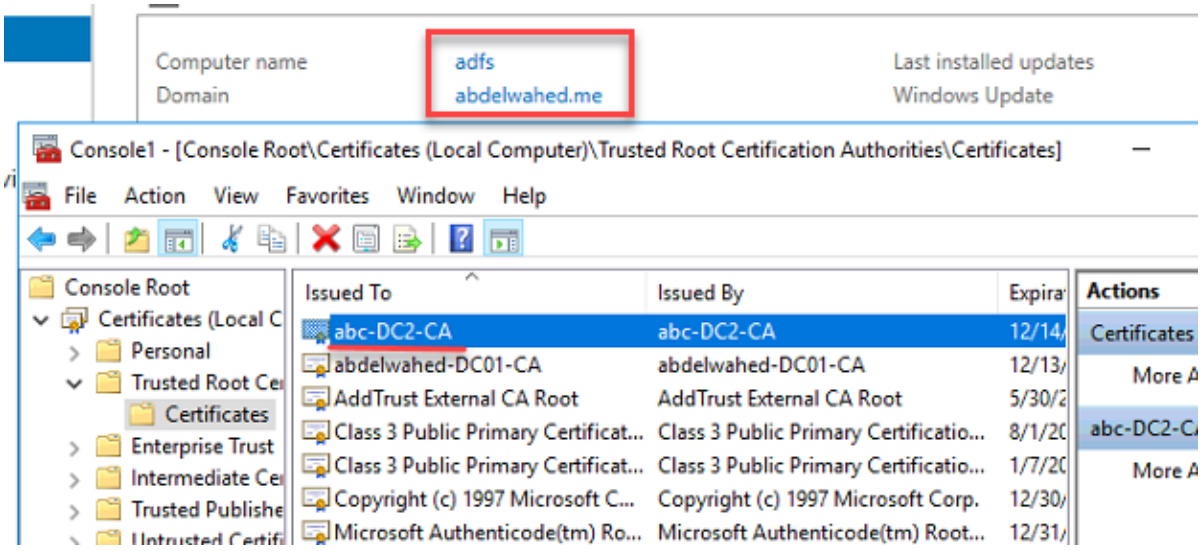
Create conditional forwarders between domains

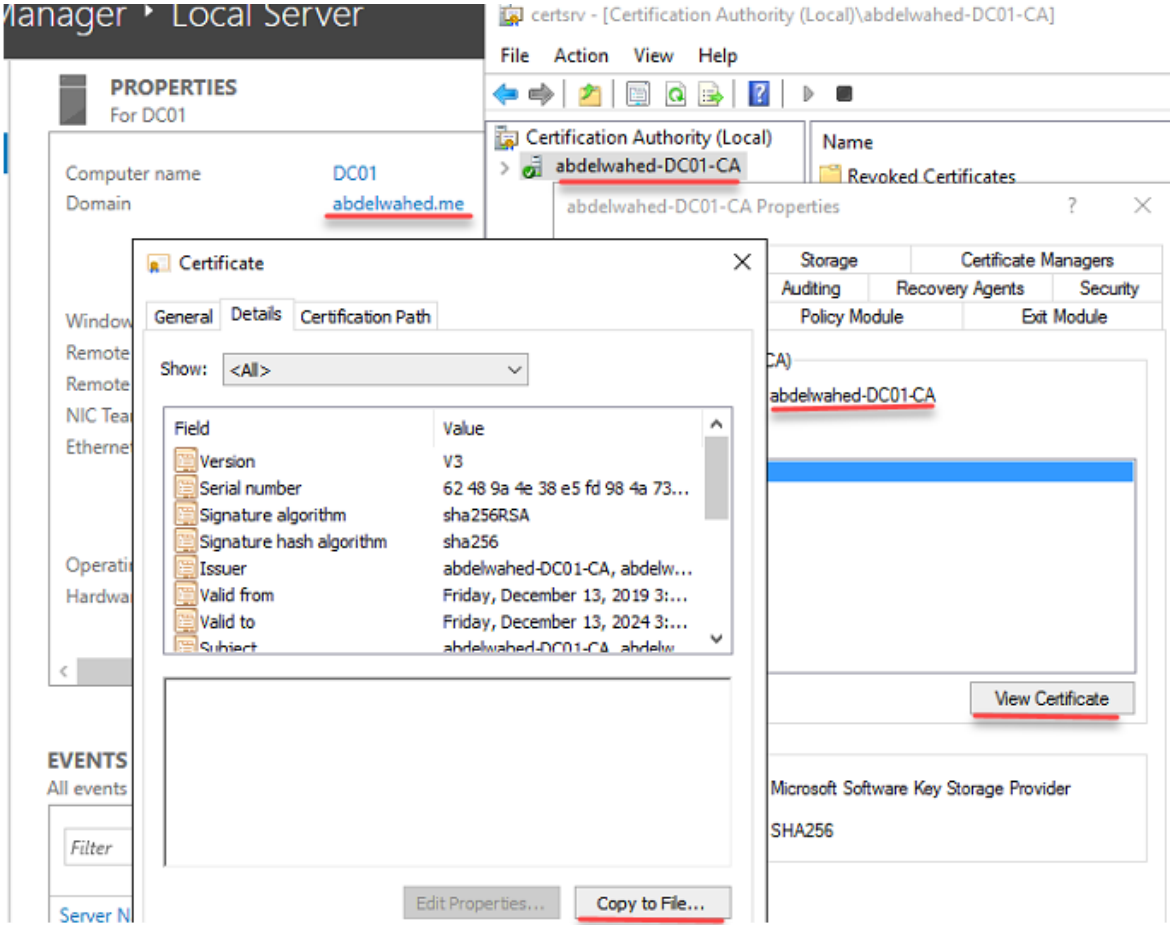


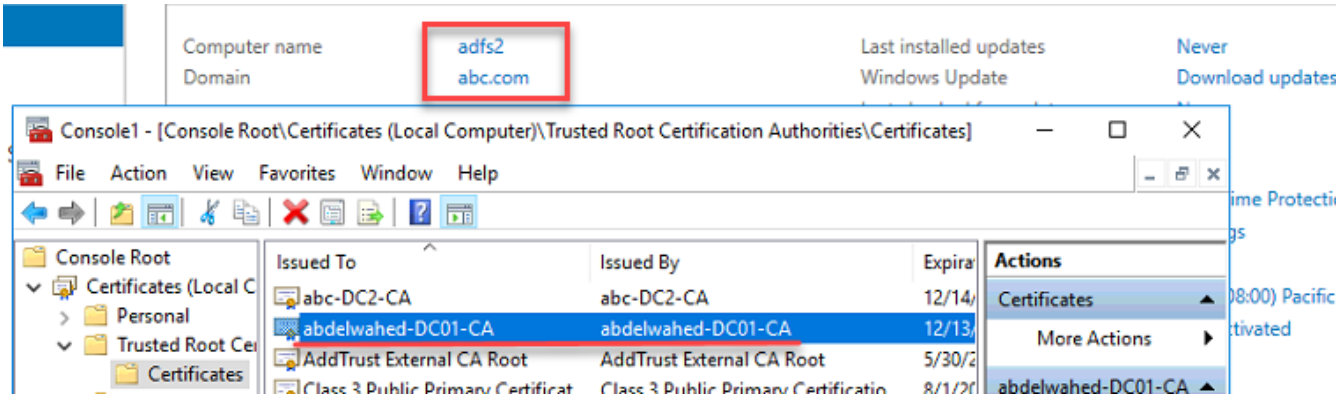


Add each domain certificate as a trusted certification authority

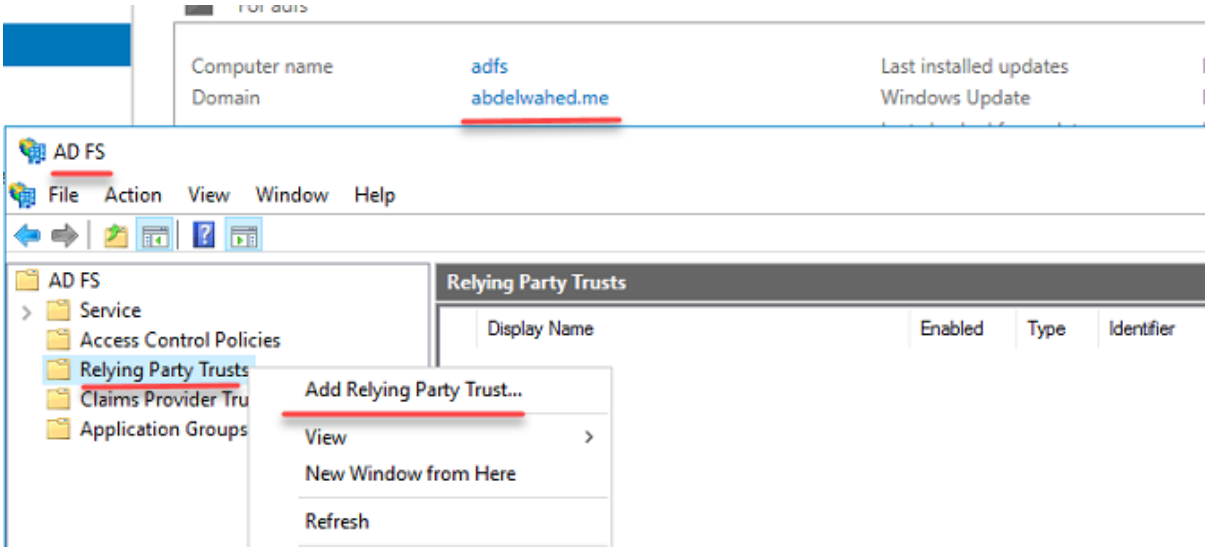


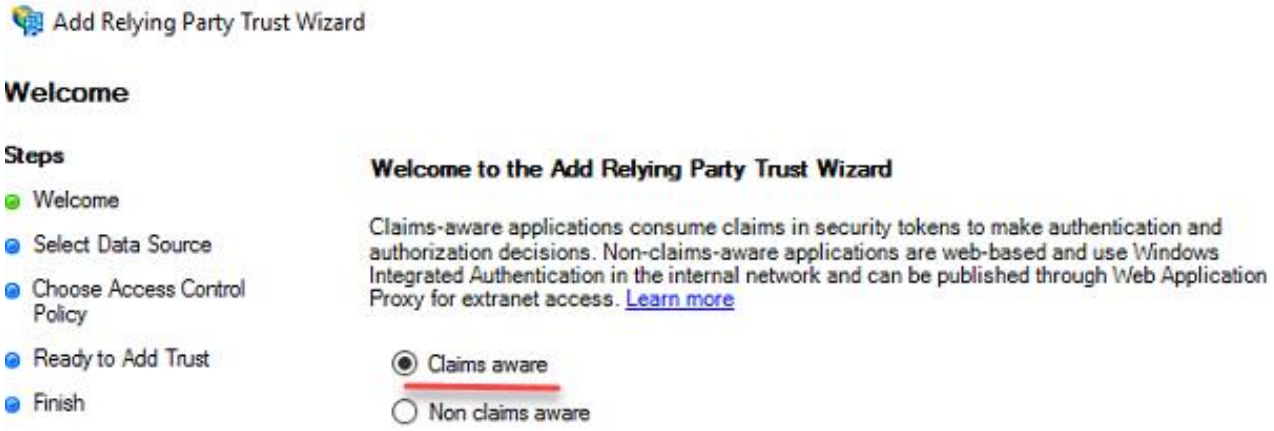


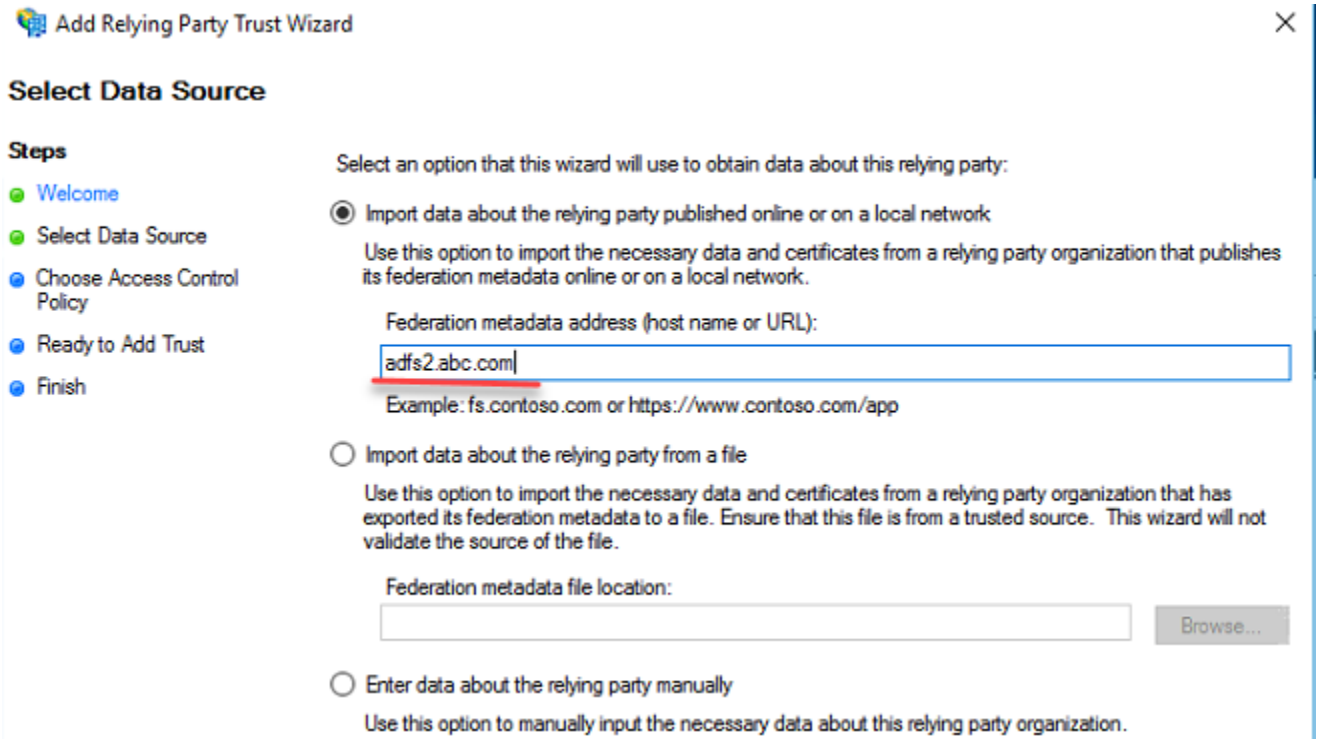

Manager • Local Server
PROPERTIES
For DC01
Computer name DC01
Domain abdelwahed.me
EVENTS
All events
Filter
certsrv - [Certification Authority (Local)\abdelwahed-DC01-CA]
File Action View Help
Certification Authority (Local)
abdelwahed-DC01-CA
Name
Revoked Certificates
abdelwahed-DC01-CA Properties
Certificate
General Details Certification Path
Show: <All>
Field Value
Version V3
Serial number 62 48 9a 4e 38 e5 fd 98 4a 73...
Signature algorithm sha256RSA
Signature hash algorithm sha256
Issuer abdelwahed-DC01-CA, abdelw...
Valid from Friday, December 13, 2019 3:...
Valid to Friday, December 13, 2024 3:...
Edit Properties... Copy to File...
Storage Certificate Managers
Auditing Recovery Agents Security
Policy Module Exit Module
abdelwahed-DC01-CA
View Certificate
Microsoft Software Key Storage Provider
SHA256

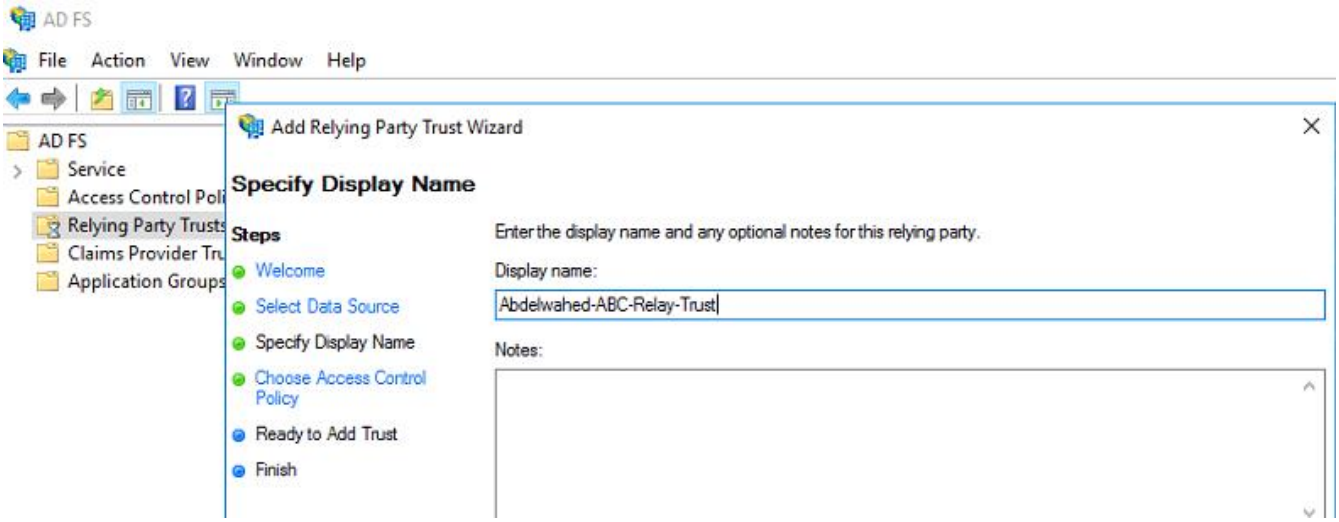

Computer name adfs2
Domain abc.com
Last installed updates Never
Windows Update Download updates
Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]
File Action View Favorites Window Help
Console Root
Certificates (Local C
Personal
Trusted Root Ce
Certificates
Issued To Issued By Expira
abc-DC2-CA abc-DC2-CA 12/14/
abdelwahed-DC01-CA abdelwahed-DC01-CA 12/13/
AddTrust External CA Root AddTrust External CA Root 5/30/2
Actions
Certificates
More Actions
abdelwahed-DC01-CA

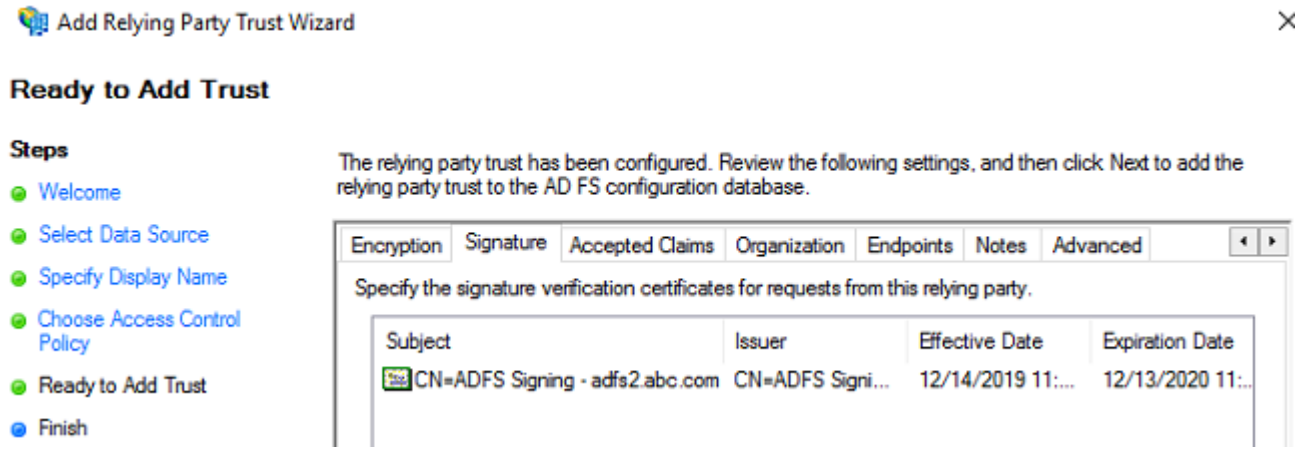
Configure Relay party trust at ADFS.ABDELWAHED.ME to support ADFS2.ABC

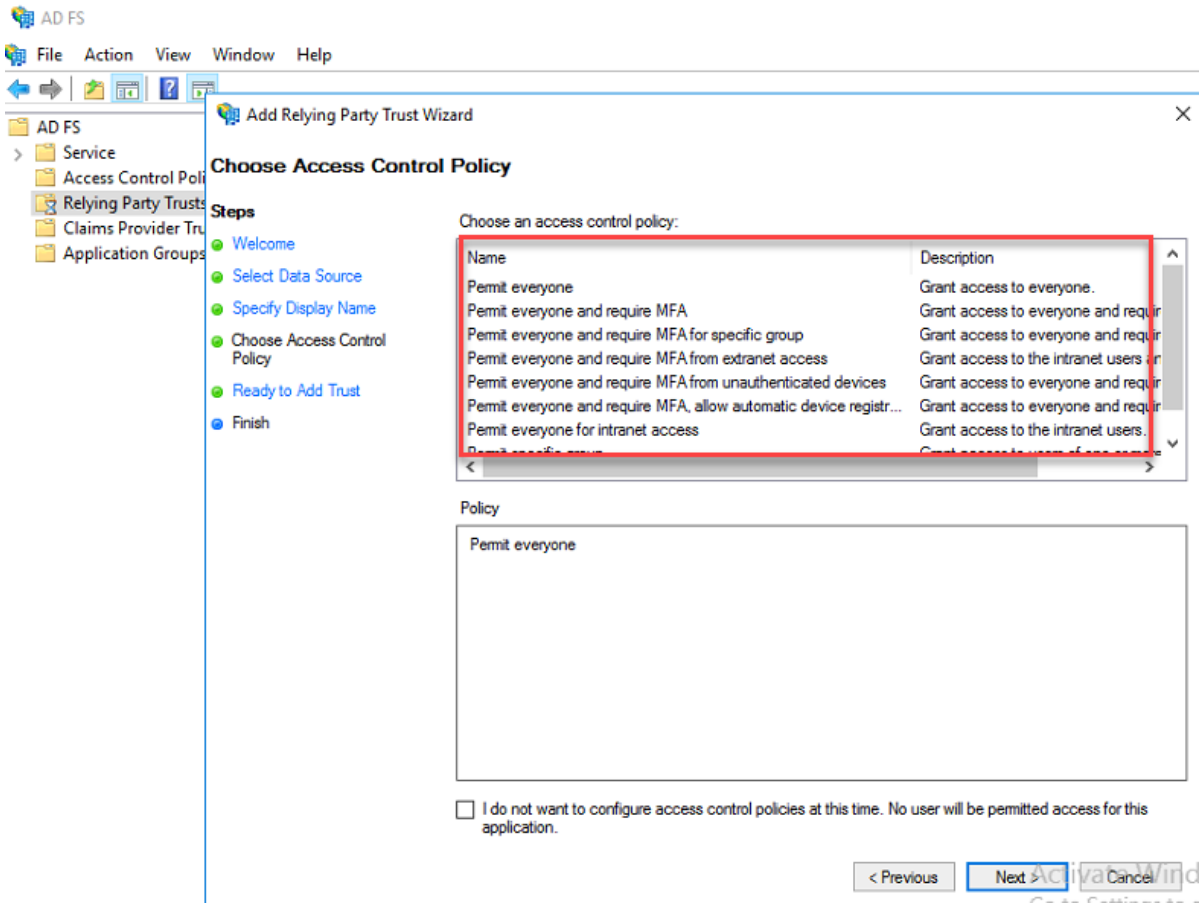


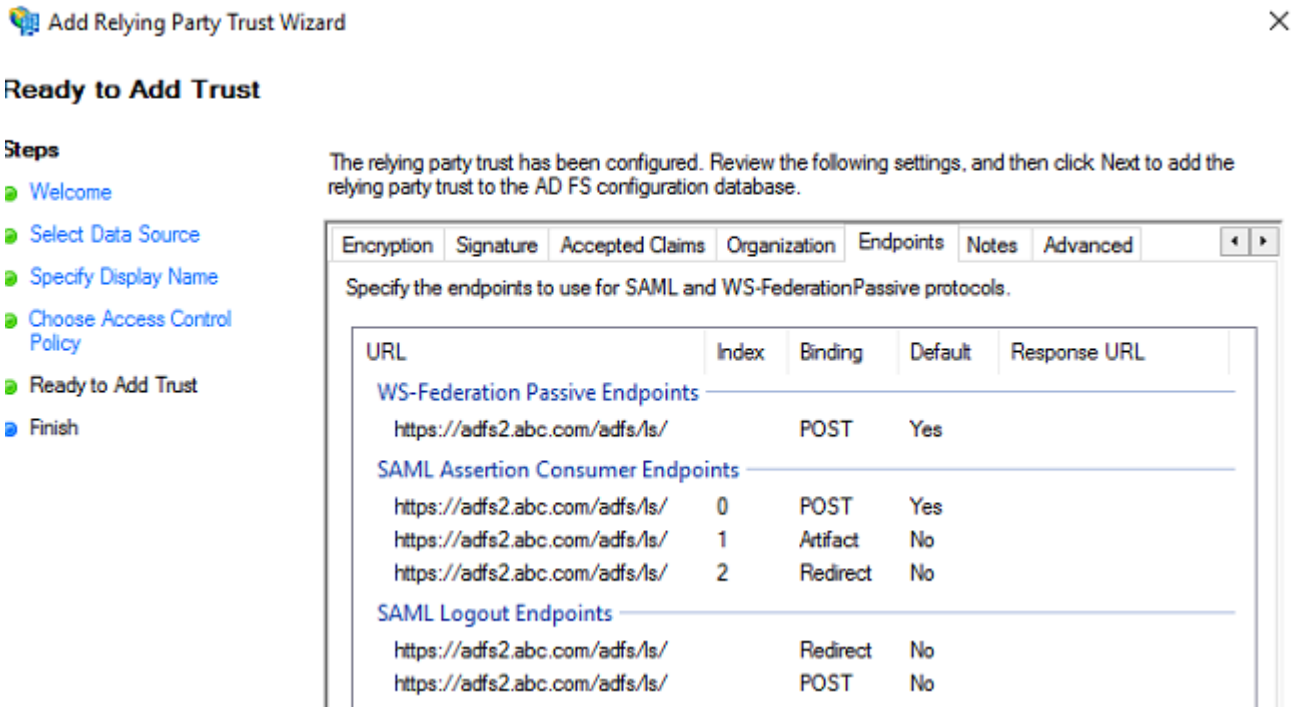


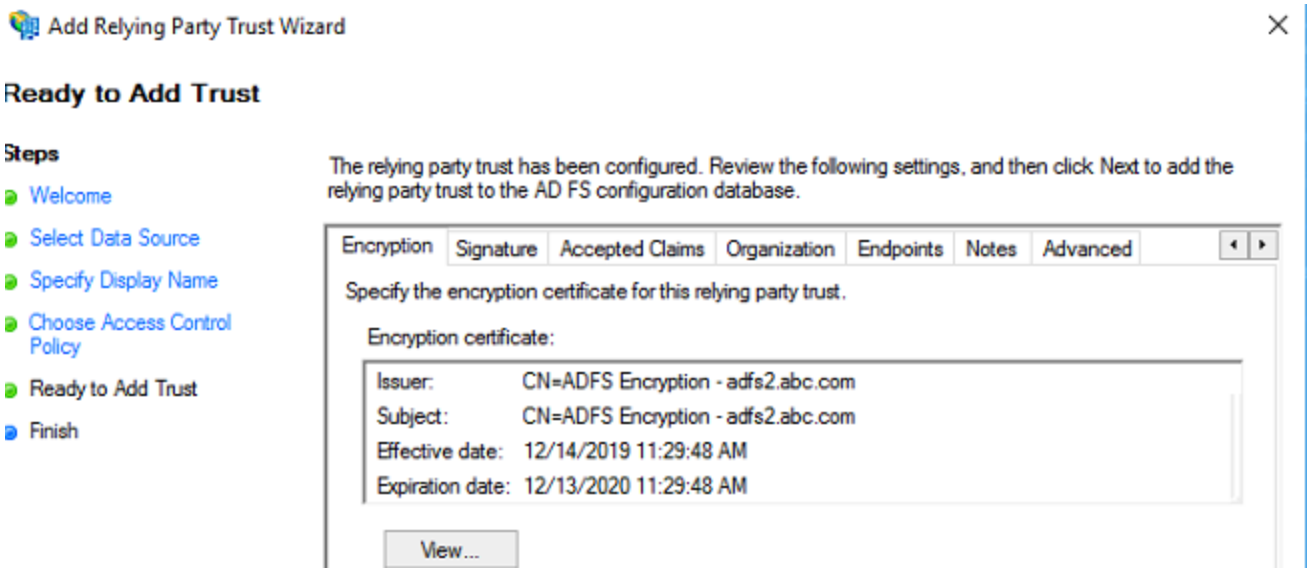

Add Relying Party Trust Wizard
Select Data Source
Steps
Welcome
Select Data Source
Choose Access Control Policy
Ready to Add Trust
Finish
Select an option that this wizard will use to obtain data about this relying party:
Import data about the relying party published online or on a local network
Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.
Federation metadata address (host name or URL):
adfs2.abc.com
Example: fs.contoso.com or https://www.contoso.com/app
Import data about the relying party from a file
Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.
Federation metadata file location:
Browse...
Enter data about the relying party manually
Use this option to manually input the necessary data about this relying party organization.

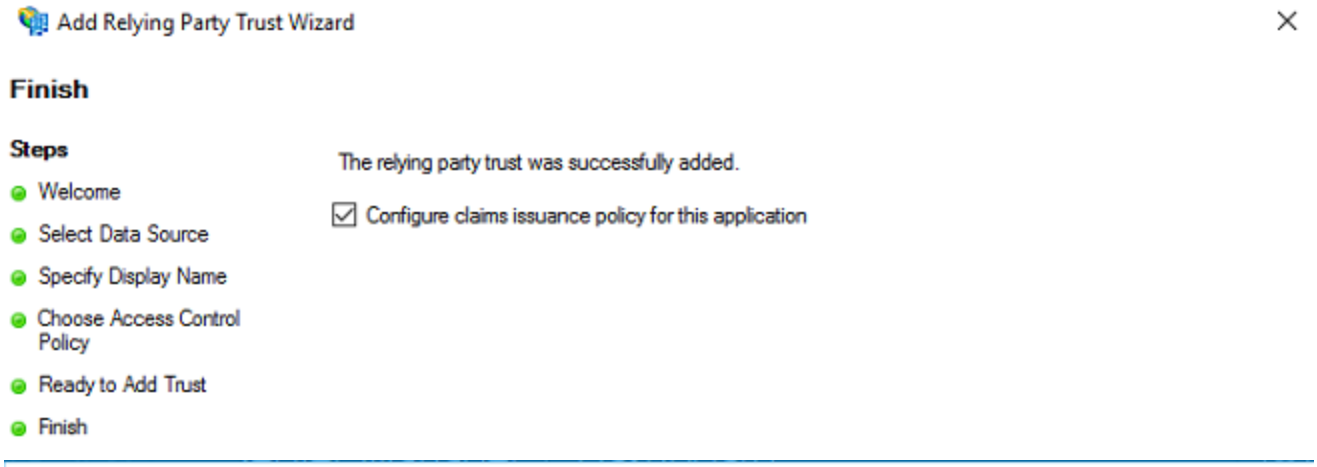

AD FS
File Action View Window Help
AD FS
Service
Access Control Poli
Relying Party Trusts
Claims Provider Tru
Application Groups
Add Relying Party Trust Wizard
Specify Display Name
Steps
Welcome
Select Data Source
Specify Display Name
Choose Access Control Policy
Ready to Add Trust
Finish
Enter the display name and any optional notes for this relying party.
Display name:
Abdelwahed-ABC-Relay-Trust
Notes:

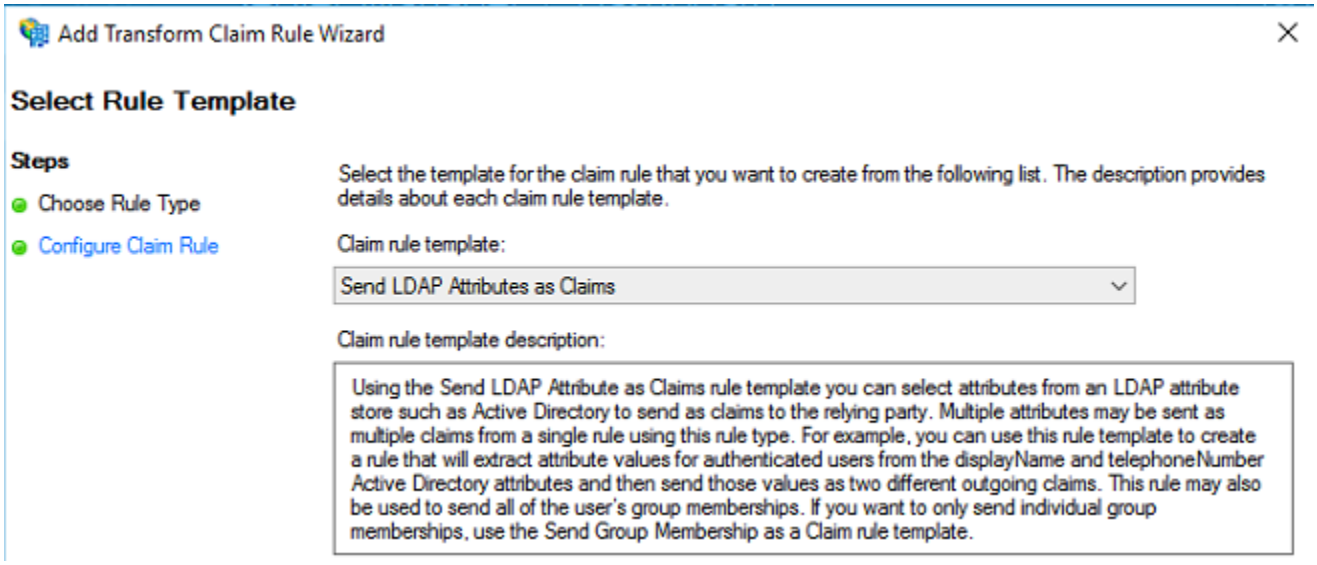

Add Relying Party Trust Wizard
Ready to Add Trust
Steps
Welcome
Select Data Source
Specify Display Name
Choose Access Control Policy
Ready to Add Trust
Finish
The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.
Encryption
Signature
Accepted Claims
Organization
Endpoints
Notes
Advanced
Specify the signature verification certificates for requests from this relying party.
Subject
Issuer
Effective Date
Expiration Date
CN=ADFS Signing - adfs2.abc.com
CN=ADFS Signi...
12/14/2019 11:...
12/13/2020 11:...

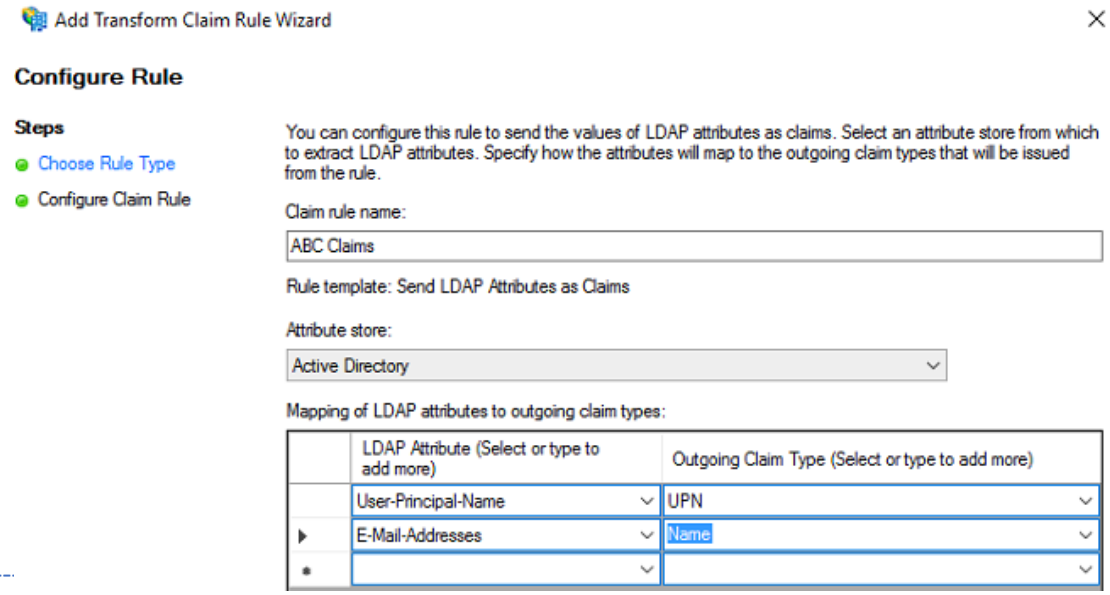

AD FS
File
Action
View
Window
Help
AD FS
Service
Access Control Poli
Relying Party Trusts
Claims Provider Tru
Application Groups
Add Relying Party Trust Wizard
Choose Access Control Policy
Steps
Welcome
Select Data Source
Specify Display Name
Choose Access Control Policy
Ready to Add Trust
Finish
Choose an access control policy:
Name
Description
Permit everyone
Grant access to everyone.
Permit everyone and require MFA
Grant access to everyone and requir
Permit everyone and require MFA for specific group
Grant access to everyone and requir
Permit everyone and require MFA from extranet access
Grant access to the intranet users
Permit everyone and require MFA from unauthenticated devices
Grant access to everyone and requir
Permit everyone and require MFA, allow automatic device registr...
Grant access to everyone and requir
Permit everyone for intranet access
Grant access to the intranet users.
Policy
Permit everyone
I do not want to configure access control policies at this time. No user will be permitted access for this application.
< Previous
Next >
Cancel


Add Relying Party Trust Wizard
Ready to Add Trust
Steps
Welcome
Select Data Source
Specify Display Name
Choose Access Control Policy
Ready to Add Trust
Finish
The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.
Encryption
Signature
Accepted Claims
Organization
Endpoints
Notes
Advanced
Specify the endpoints to use for SAML and WS-FederationPassive protocols.
URL
Index
Binding
Default
Response URL
WS-Federation Passive Endpoints
https://adfs2.abc.com/adfs/ls/
POST
Yes
SAML Assertion Consumer Endpoints
https://adfs2.abc.com/adfs/ls/ 0 POST Yes
https://adfs2.abc.com/adfs/ls/ 1 Artifact No
https://adfs2.abc.com/adfs/ls/ 2 Redirect No
SAML Logout Endpoints
https://adfs2.abc.com/adfs/ls/
Redirect
No
https://adfs2.abc.com/adfs/ls/
POST
No

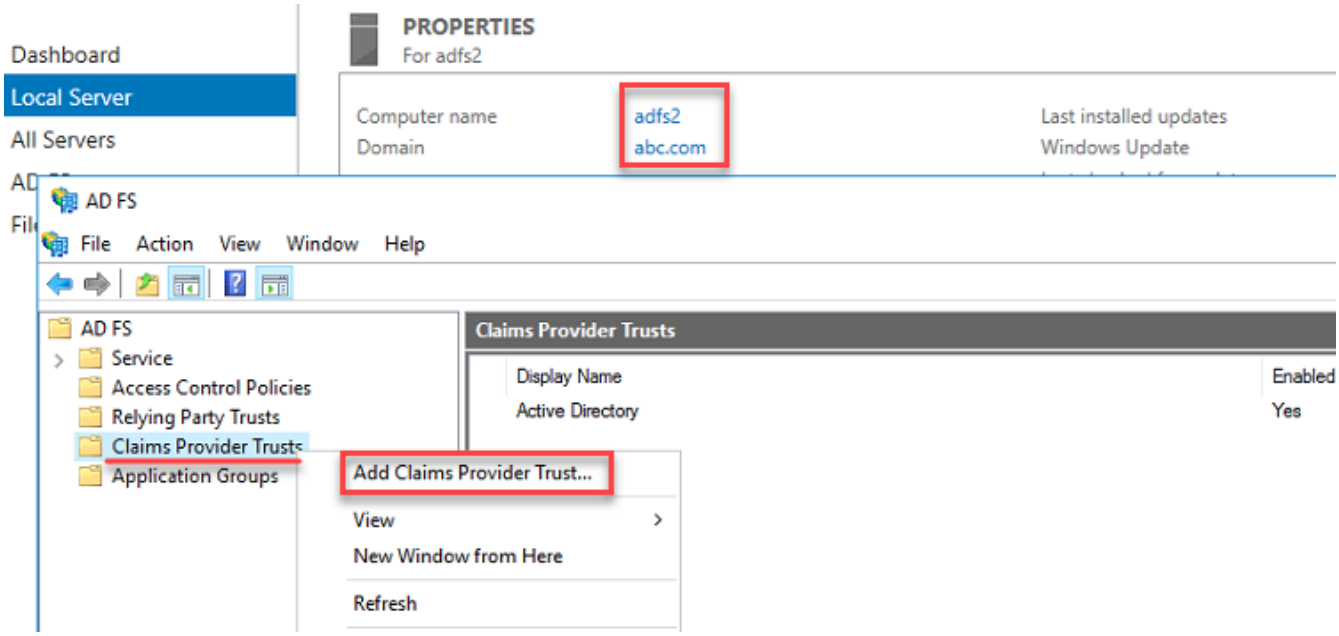

Add Relying Party Trust Wizard
Ready to Add Trust
Steps
Welcome
Select Data Source
Specify Display Name
Choose Access Control Policy
Ready to Add Trust
Finish
The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.
Encryption
Signature
Accepted Claims
Organization
Endpoints
Notes
Advanced
Specify the encryption certificate for this relying party trust.
Encryption certificate:
Issuer: CN=ADFS Encryption - adfs2.abc.com
Subject: CN=ADFS Encryption - adfs2.abc.com
Effective date: 12/14/2019 11:29:48 AM
Expiration date: 12/13/2020 11:29:48 AM
View...

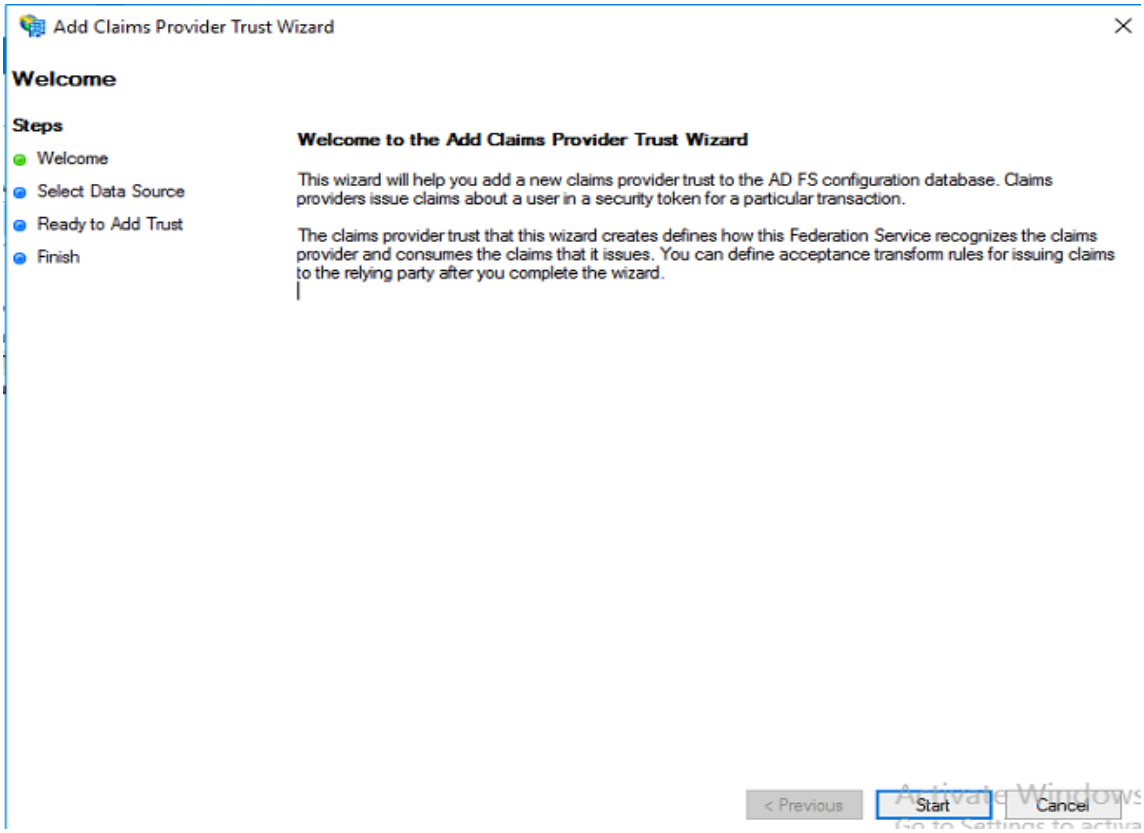

Add Relying Party Trust Wizard
Finish
Steps
Welcome
Select Data Source
Specify Display Name
Choose Access Control Policy
Ready to Add Trust
Finish
The relying party trust was successfully added.
Configure claims issuance policy for this application

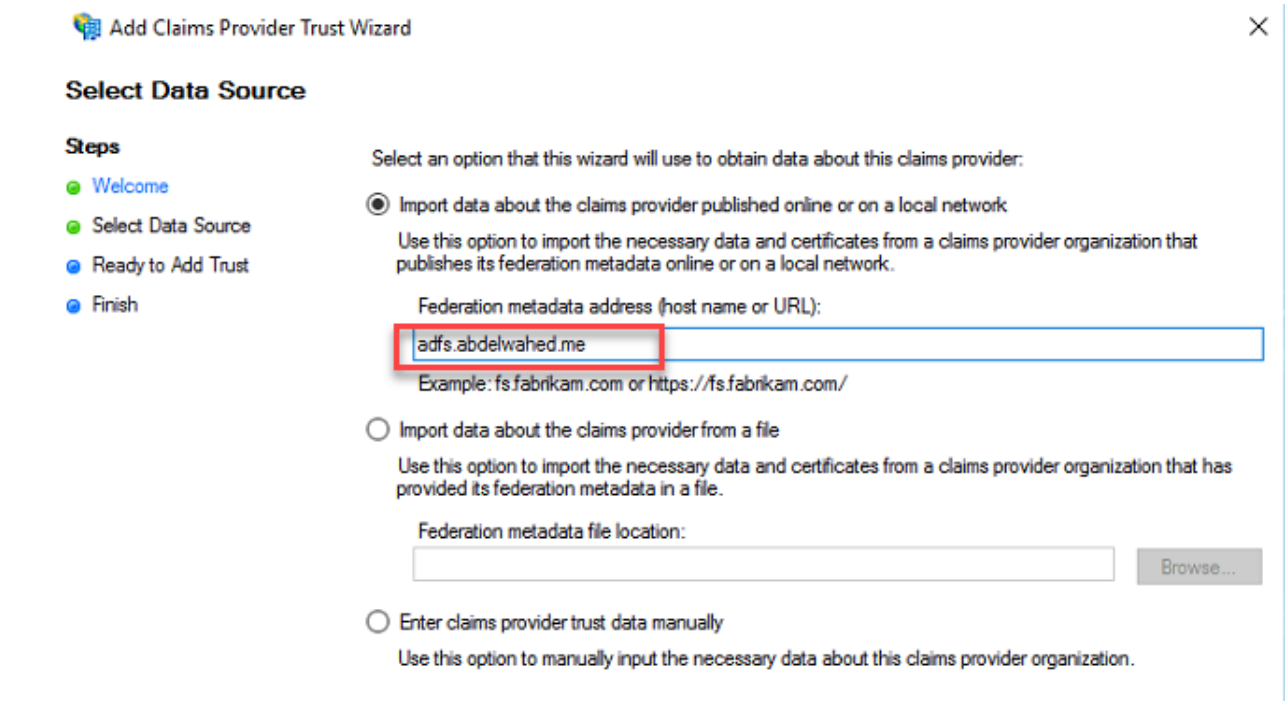

Add Transform Claim Rule Wizard
Select Rule Template
Steps
Choose Rule Type
Configure Claim Rule
Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.
Claim rule template:
Send LDAP Attributes as Claims
Claim rule template description:
Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

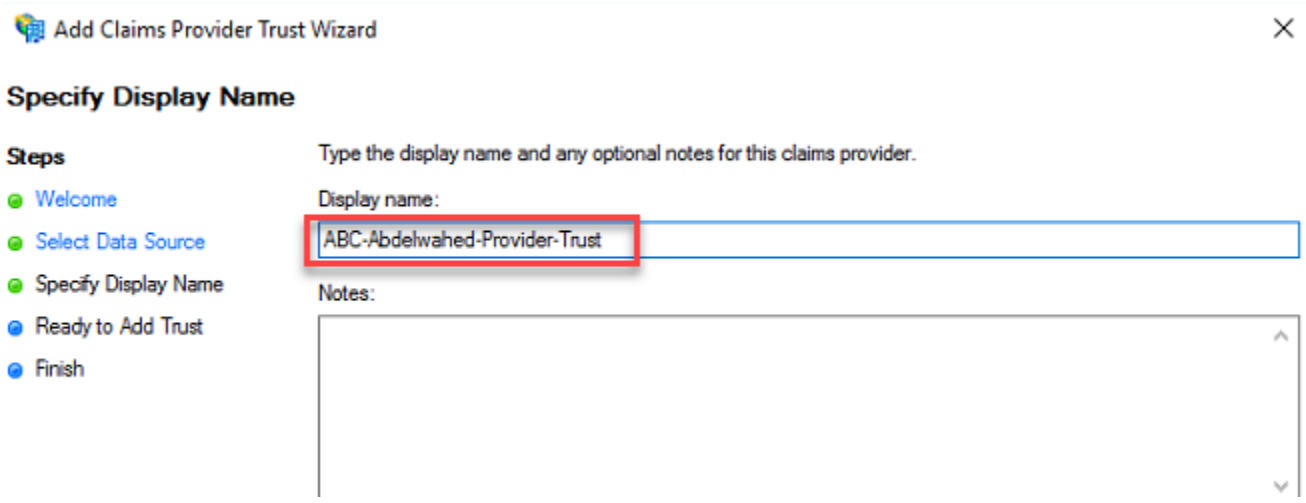

Add Transform Claim Rule Wizard
Configure Rule
Steps
Choose Rule Type
Configure Claim Rule
You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.
Claim rule name:
ABC Claims
Rule template: Send LDAP Attributes as Claims
Attribute store:
Active Directory
Mapping of LDAP attributes to outgoing claim types:
LDAP Attribute (Select or type to add more)
Outgoing Claim Type (Select or type to add more)
User-Principal-Name
UPN
E-Mail-Addresses
Name

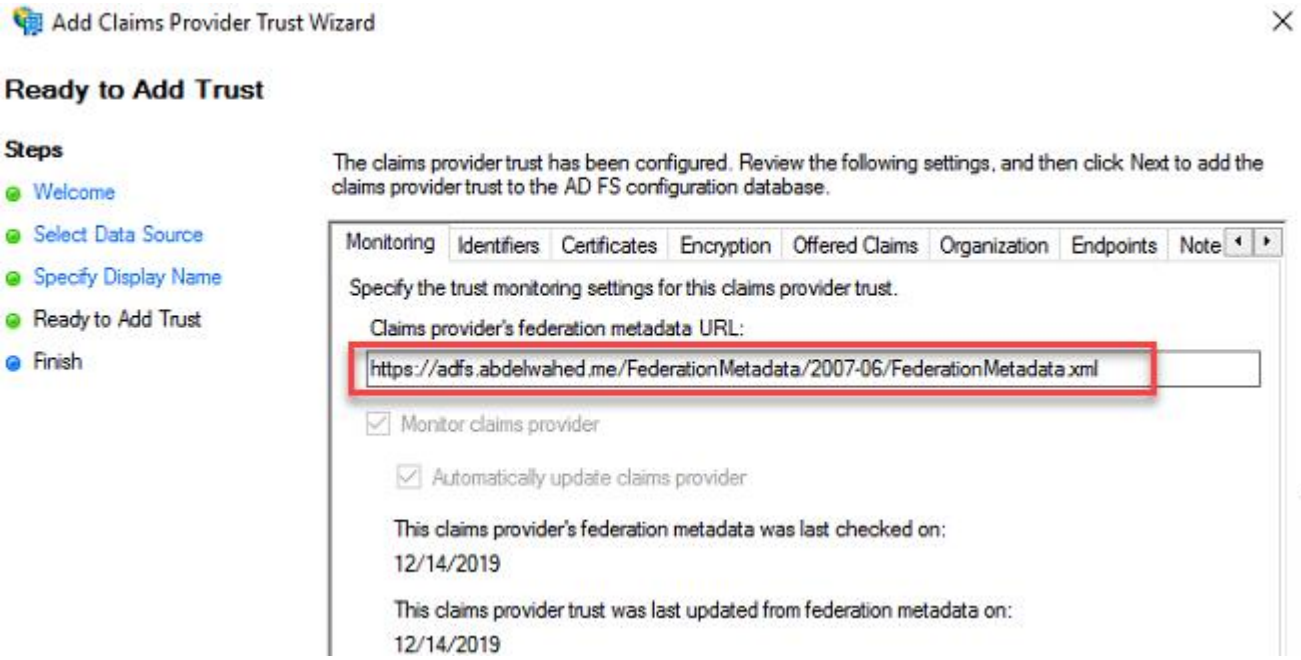
Add ADFS.ABDELWAHED.ME as a Claim trust provider at ADFS2.ABC.COM

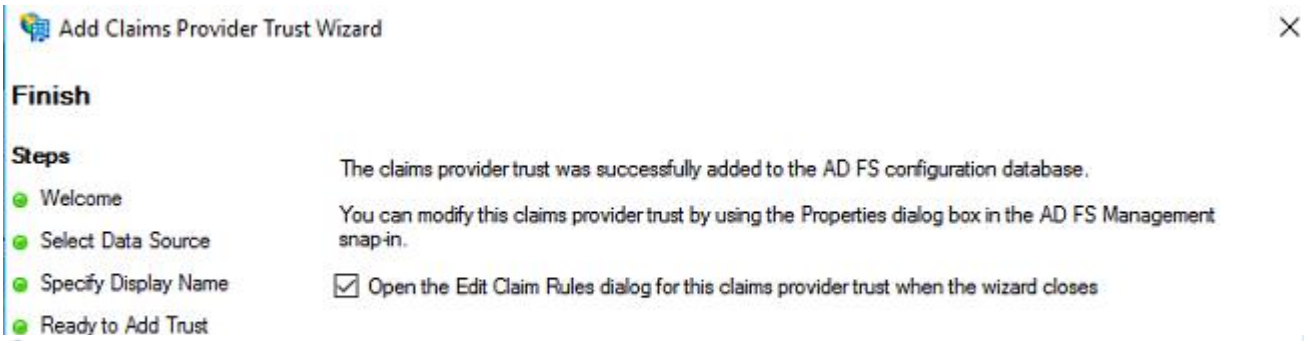


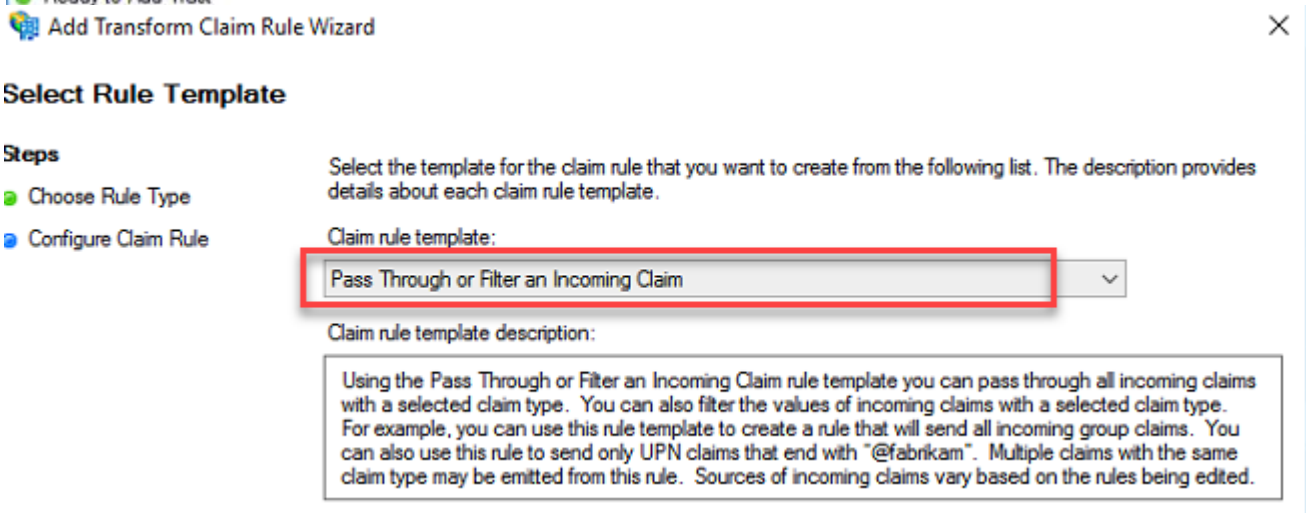


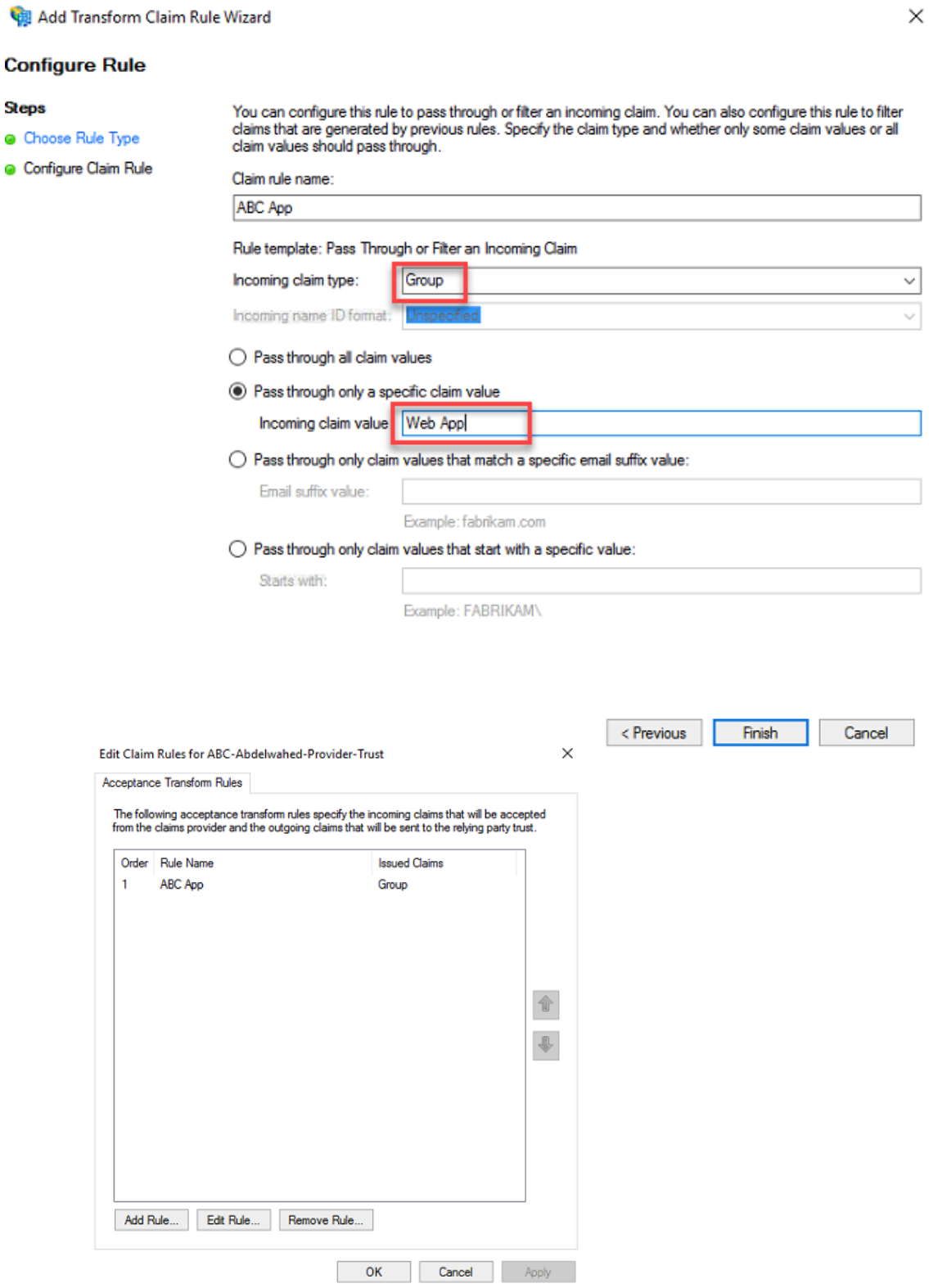

Add Claims Provider Trust Wizard
Select Data Source
Steps
Welcome
Select Data Source
Ready to Add Trust
Finish
Select an option that this wizard will use to obtain data about this claims provider:
Import data about the claims provider published online or on a local network
Use this option to import the necessary data and certificates from a claims provider organization that publishes its federation metadata online or on a local network.
Federation metadata address (host name or URL):
adfs.abdelwahed.me
Example: fs.fabrikam.com or https://fs.fabrikam.com/
Import data about the claims provider from a file
Use this option to import the necessary data and certificates from a claims provider organization that has provided its federation metadata in a file.
Federation metadata file location:
Browse...
Enter claims provider trust data manually
Use this option to manually input the necessary data about this claims provider organization.

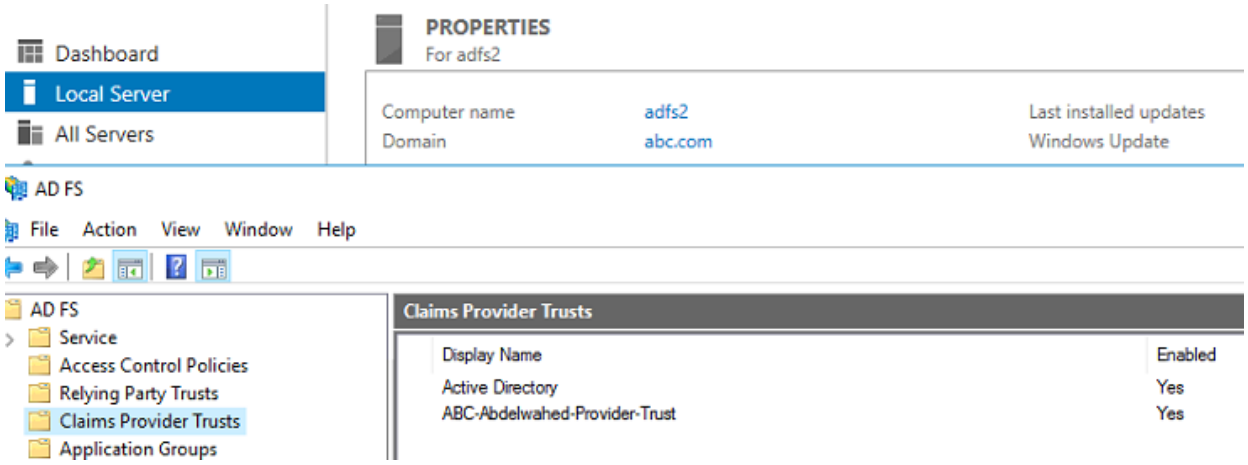

Add Claims Provider Trust Wizard
Specify Display Name
Steps
Welcome
Select Data Source
Specify Display Name
Ready to Add Trust
Finish
Type the display name and any optional notes for this claims provider.
Display name:
ABC-Abdelwahed-Provider-Trust
Notes:


Add Claims Provider Trust Wizard
Ready to Add Trust
Steps
Welcome
Select Data Source
Specify Display Name
Ready to Add Trust
Finish
The claims provider trust has been configured. Review the following settings, and then click Next to add the claims provider trust to the AD FS configuration database.
Monitoring
Identifiers
Certificates
Encryption
Offered Claims
Organization
Endpoints
Note
Specify the trust monitoring settings for this claims provider trust.
Claims provider's federation metadata URL:
https://adfs.abdelwahed.me/FederationMetadata/2007-06/FederationMetadata.xml
Monitor claims provider
Automatically update claims provider
This claims provider's federation metadata was last checked on:
12/14/2019
This claims provider trust was last updated from federation metadata on:
12/14/2019

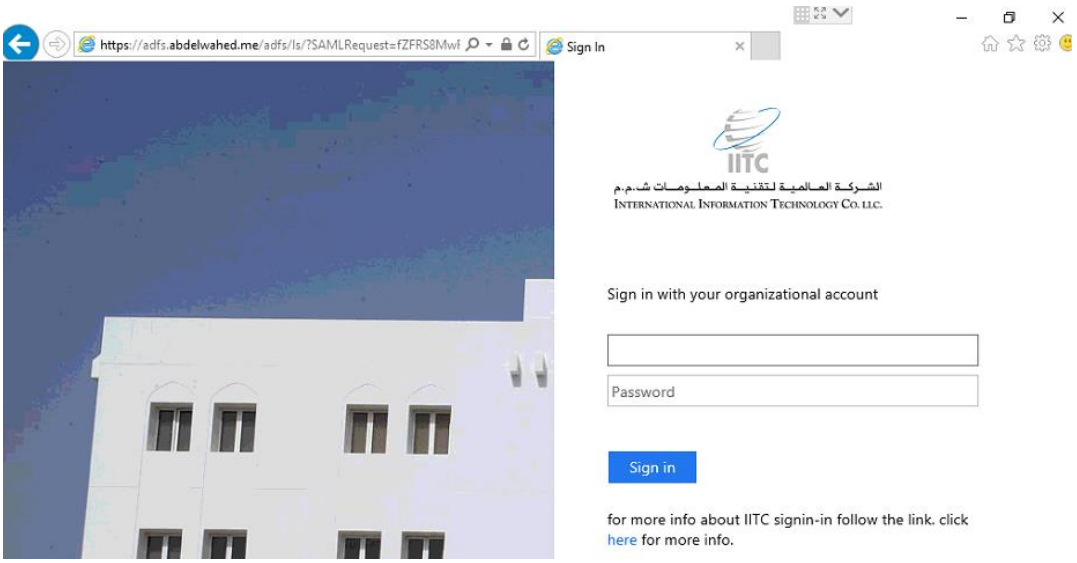

Add Claims Provider Trust Wizard
Finish
Steps
Welcome
Select Data Source
Specify Display Name
Ready to Add Trust
The claims provider trust was successfully added to the AD FS configuration database.
You can modify this claims provider trust by using the Properties dialog box in the AD FS Management snap-in.
Open the Edit Claim Rules dialog for this claims provider trust when the wizard closes


Add Transform Claim Rule Wizard
Select Rule Template
Steps
Choose Rule Type
Configure Claim Rule
Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.
Claim rule template:
Pass Through or Filter an Incoming Claim
Claim rule template description:
Using the Pass Through or Filter an Incoming Claim rule template you can pass through all incoming claims with a selected claim type. You can also filter the values of incoming claims with a selected claim type. For example, you can use this rule template to create a rule that will send all incoming group claims. You can also use this rule to send only UPN claims that end with "@fabrikam". Multiple claims with the same claim type may be emitted from this rule. Sources of incoming claims vary based on the rules being edited.


Add Transform Claim Rule Wizard
Configure Rule
Steps
Choose Rule Type
Configure Claim Rule
You can configure this rule to pass through or filter an incoming claim. You can also configure this rule to filter claims that are generated by previous rules. Specify the claim type and whether only some claim values or all claim values should pass through.
Claim rule name:
ABC App
Rule template: Pass Through or Filter an Incoming Claim
Incoming claim type:
Group
Incoming name ID format:
Unspecified
Pass through all claim values
Pass through only a specific claim value
Incoming claim value:
Web App
Pass through only claim values that match a specific email suffix value:
Email suffix value:
Example: fabrikam.com
Pass through only claim values that start with a specific value:
Starts with:
Example: FABRIKAM\
< Previous
Finish
Cancel
Edit Claim Rules for ABC-Abdelwahed-Provider-Trust
Acceptance Transform Rules
The following acceptance transform rules specify the incoming claims that will be accepted from the claims provider and the outgoing claims that will be sent to the relying party trust.
Order
Rule Name
Issued Claims
1
ABC App
Group
Add Rule...
Edit Rule...
Remove Rule...
OK
Cancel
Apply



Now that both providers are visible, choose the first one associated with the relying party trust.



Hyper-v

Install and Configure Windows Server 2016 Core on Hyper-V 2016

Lab Scenario

This lab provides basic information about:

1- Install and configure Hyper-V 2016 Server role.
2- Install Windows Server 2016 Core on Hyper-V and configure it locally and remotely.

During this lab session, we are utilizing Active Directory and DNS on a Windows Server 2016 identified as ITPROLABS.XYZ. We will integrate an additional Windows Server 2016 named Hyper-V01 into our domain. This server will fulfill the role of a Hyper-V server, hosting a Windows Server Core 2016 instance.

Domain: **ITPROLABS.XYZ**

DC IP: **192.168.153.10**

DNS: **192.168.153.10**

Hyper-V01: **192.168.153.50**

Working with Hyper-V

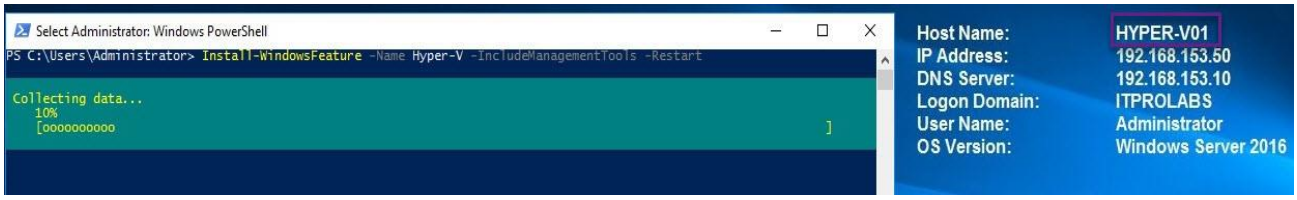
Sign in to the server designated for the Hyper-V role.

Server name: **Hyper-V01**

IP address: **192.168.153.50**

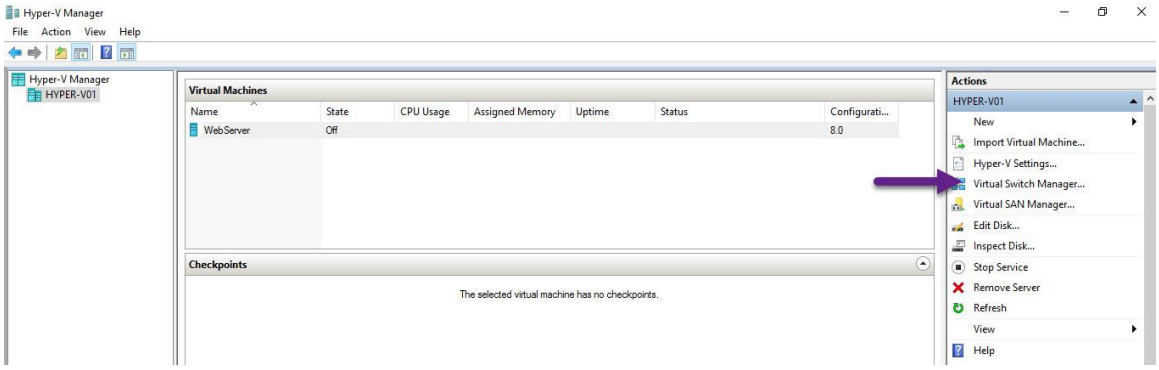
Domain: **ITProLab.xyz**

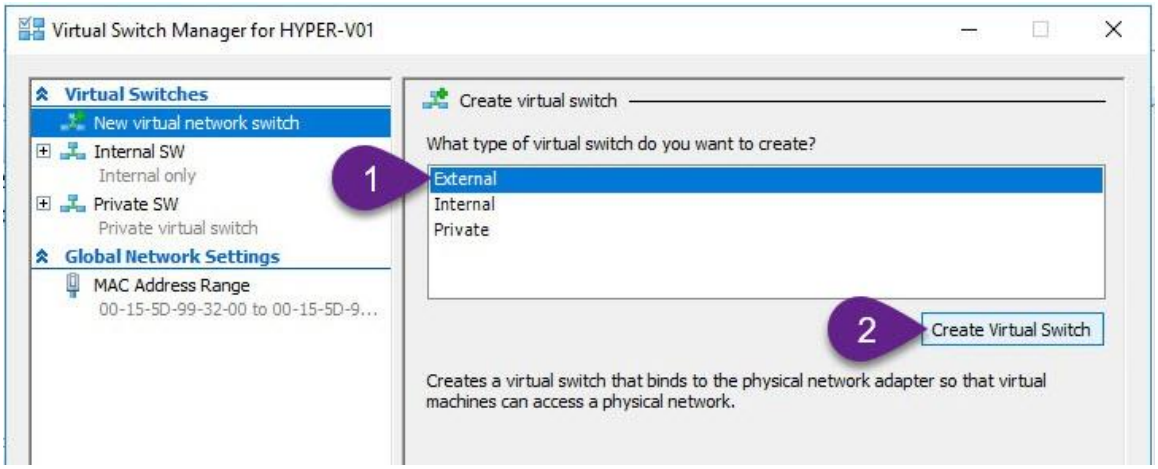
```
Install-WindowsFeature -Name Hyper-V -IncludeManagementTools -Restart
```

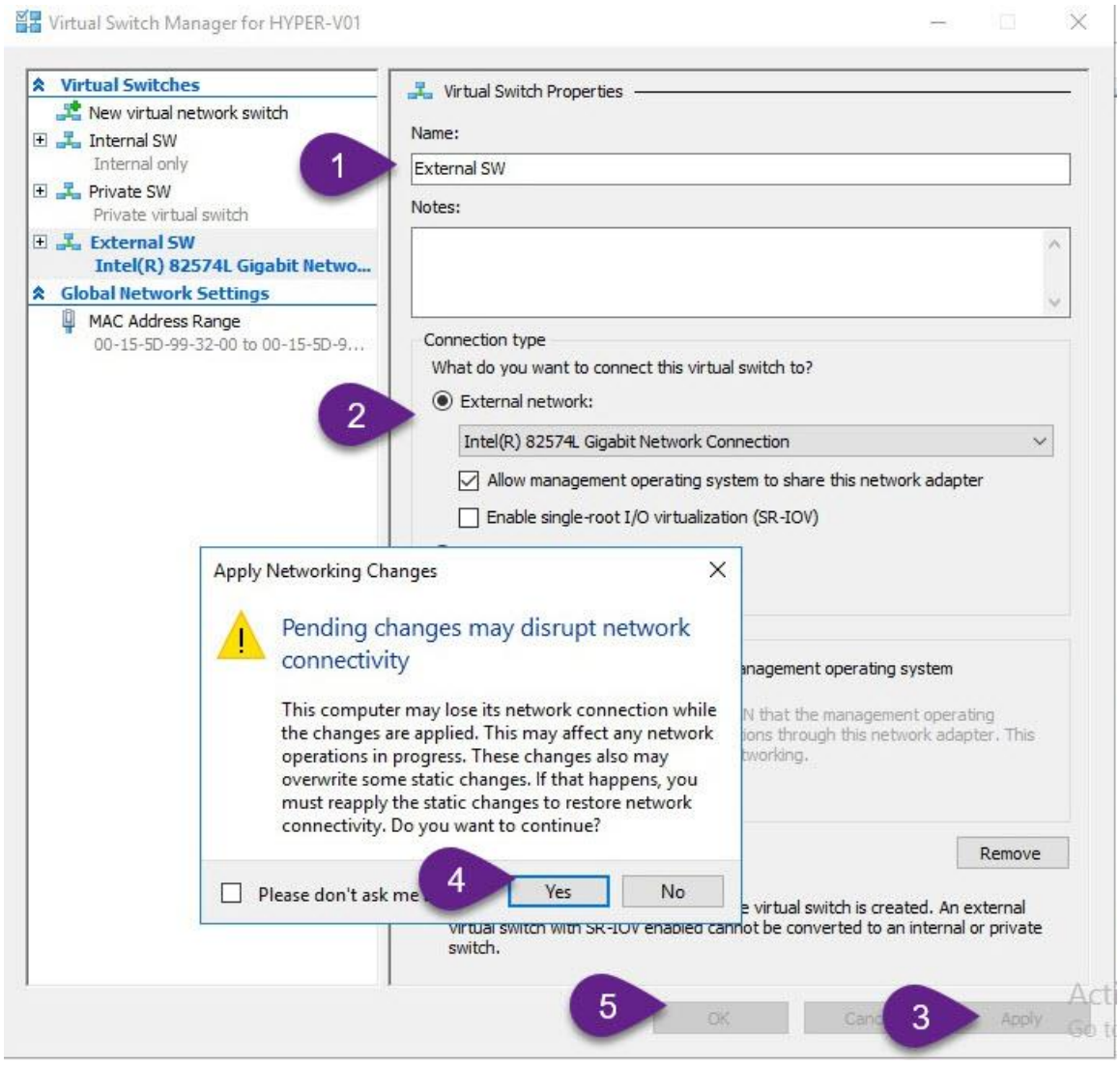


Add a Virtual Switch in Hyper-V.

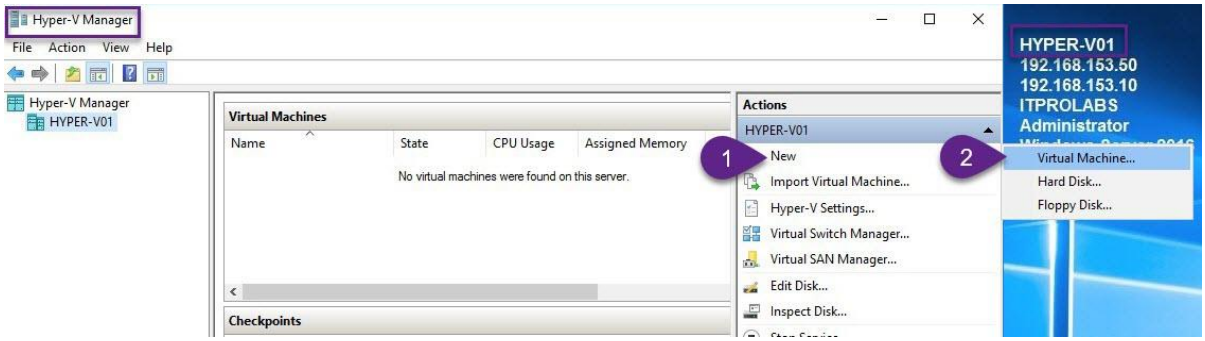
Create an external virtual switch to enable Hyper-V hosted VMs to connect with other VMs.



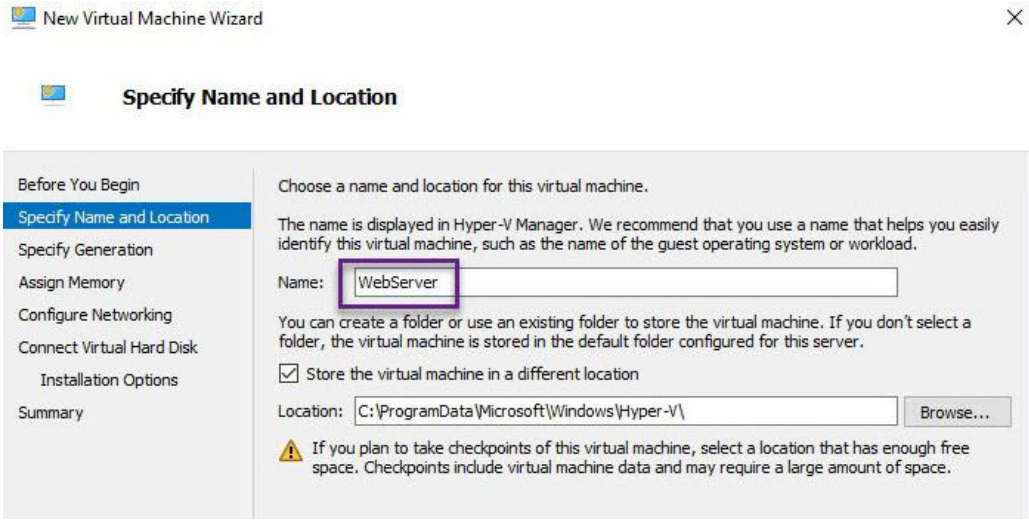

Virtual Switch Manager for HYPER-V01
Virtual Switches
New virtual network switch
Internal SW
Internal only
Private SW
Private virtual switch
Global Network Settings
MAC Address Range
00-15-5D-99-32-00 to 00-15-5D-9...
Create virtual switch
What type of virtual switch do you want to create?
External
Internal
Private
1
2
Create Virtual Switch
Creates a virtual switch that binds to the physical network adapter so that virtual machines can access a physical network.

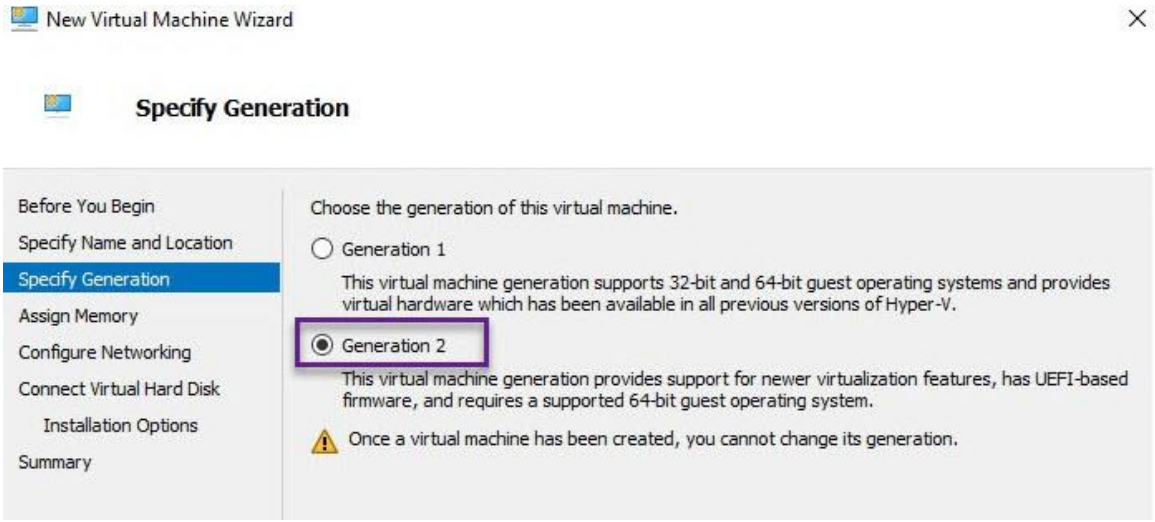

Virtual Switch Manager for HYPER-V01
Virtual Switches
New virtual network switch
Internal SW
Internal only
Private SW
Private virtual switch
External SW
Intel(R) 82574L Gigabit Netwo...
Global Network Settings
MAC Address Range
00-15-5D-99-32-00 to 00-15-5D-9...
Virtual Switch Properties
Name:
External SW
Notes:
Connection type
What do you want to connect this virtual switch to?
External network:
Intel(R) 82574L Gigabit Network Connection
Allow management operating system to share this network adapter
Enable single-root I/O virtualization (SR-IOV)
1
2
Apply Networking Changes
Pending changes may disrupt network connectivity
This computer may lose its network connection while the changes are applied. This may affect any network operations in progress. These changes also may overwrite some static changes. If that happens, you must reapply the static changes to restore network connectivity. Do you want to continue?
Please don't ask me
4
Yes
No
Remove
virtual switch is created. An external
virtual switch with SR-IOV enabled cannot be converted to an internal or private switch.
5
OK
3
Apply

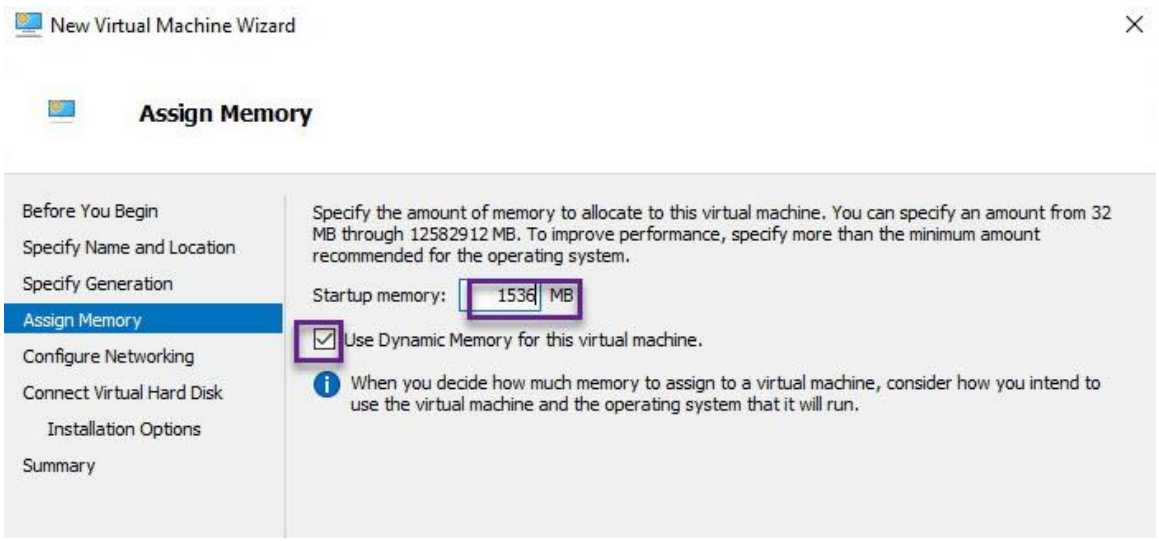
Set up Server Core 2016 in Hyper-V.

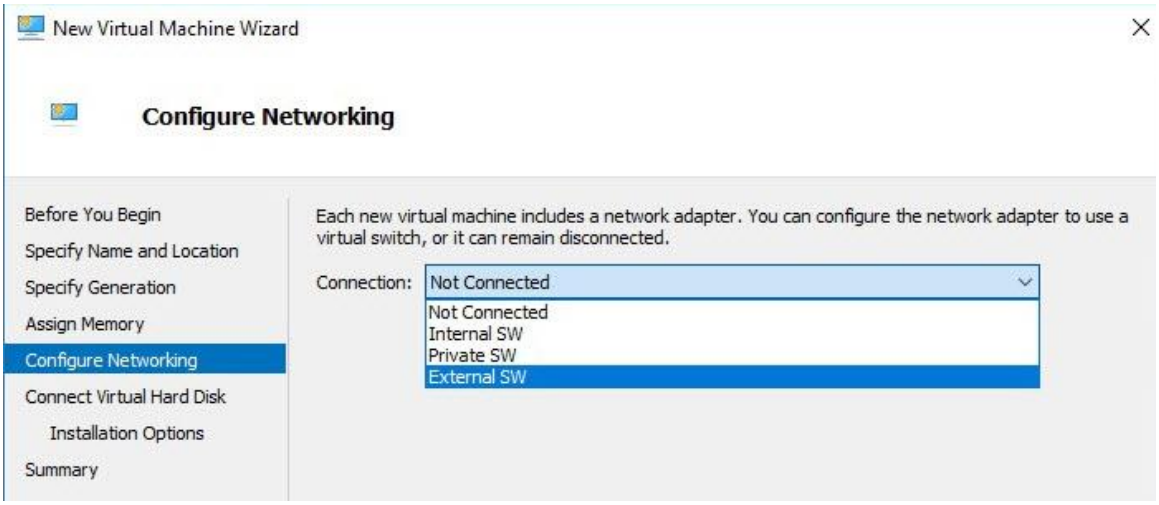


Use the Hyper-V01 server manager to open the Hyper-V management console and comply with the subsequent illustrations to set up a Server Core 2016 VM.

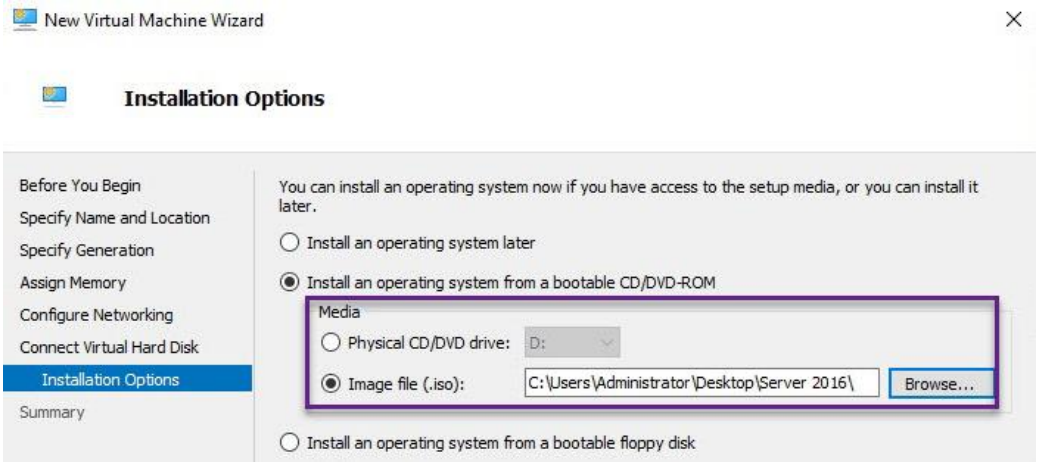


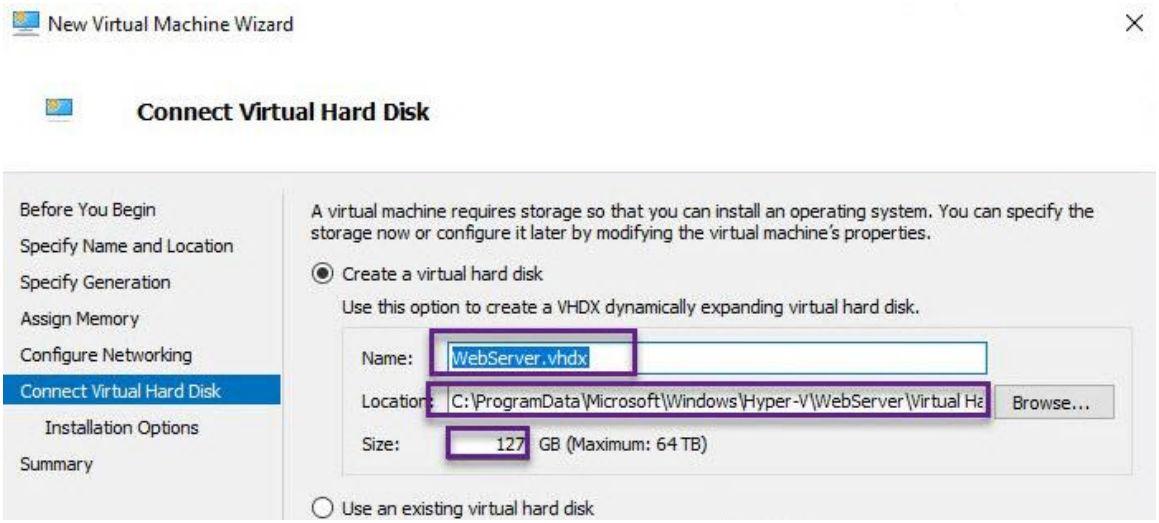




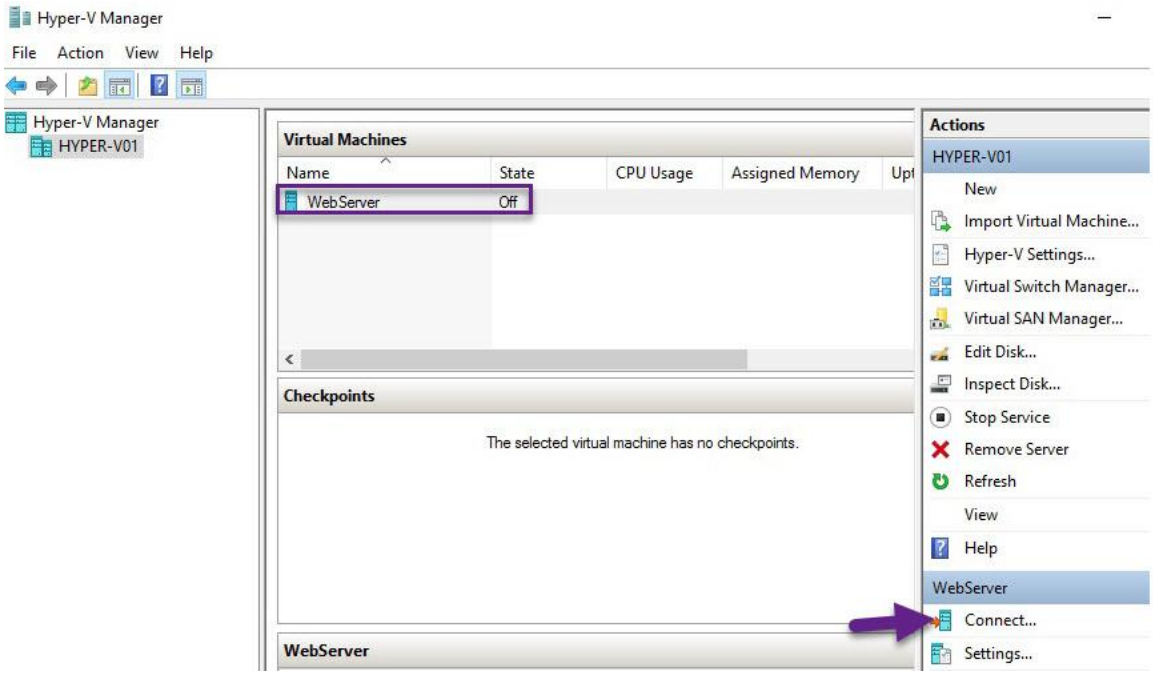


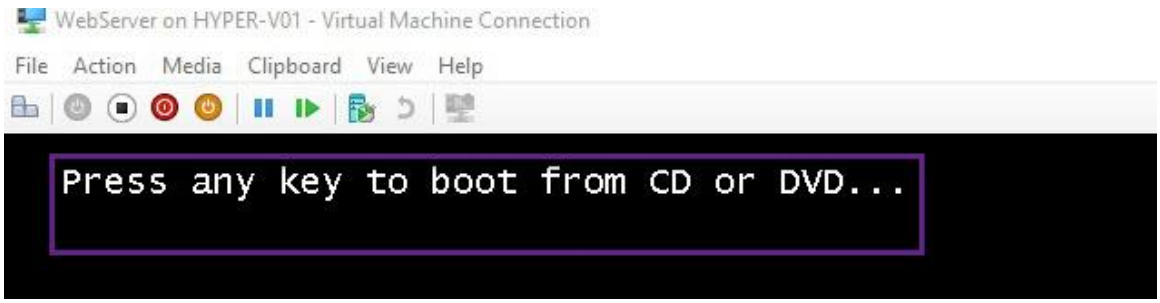
Choose and use the Windows Server 2016 ISO image as the source for installation.

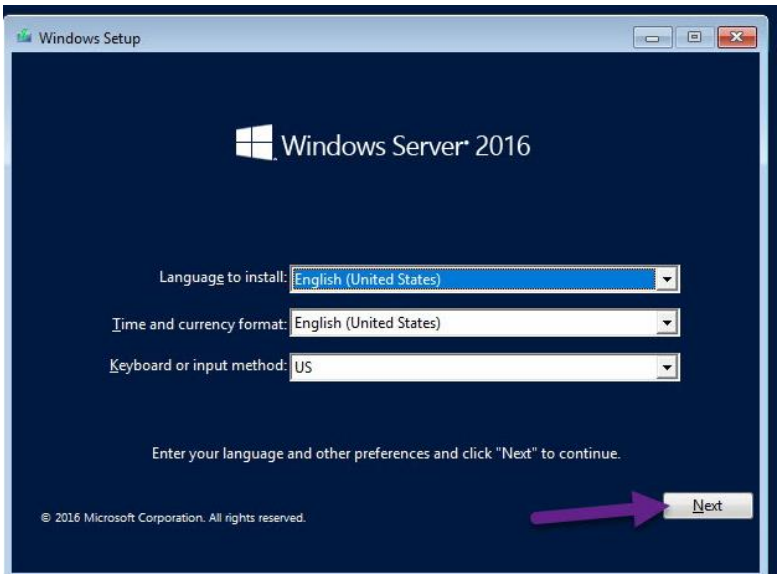


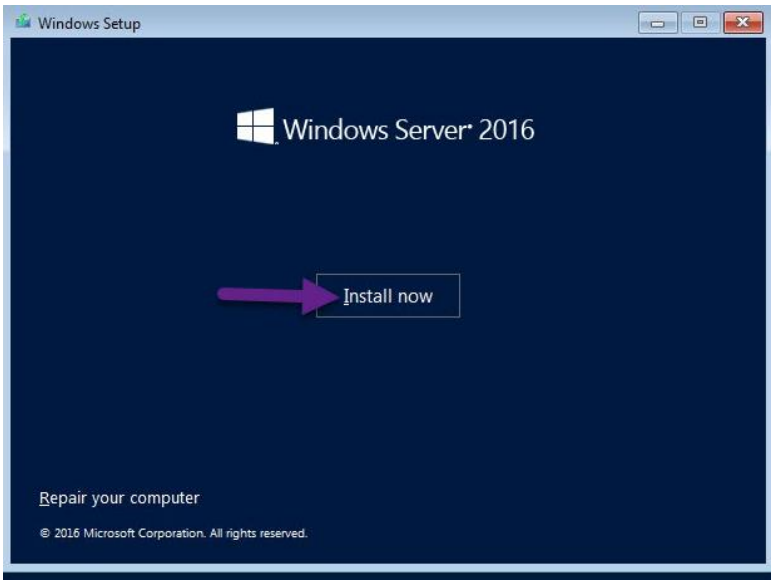


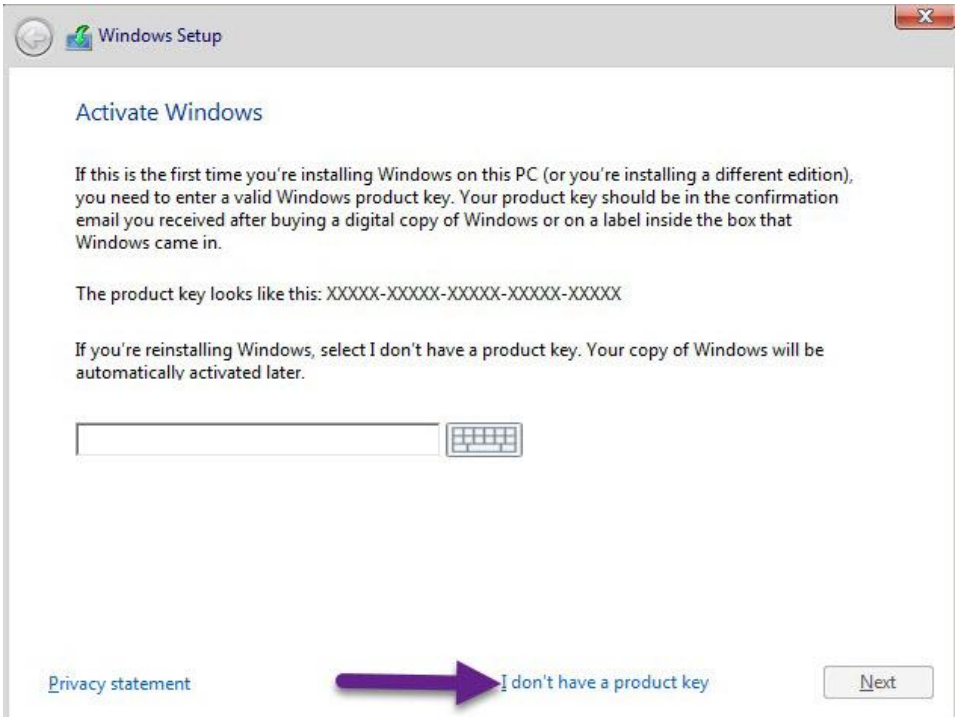
Access the Server Core VM and initiate the installation procedure.



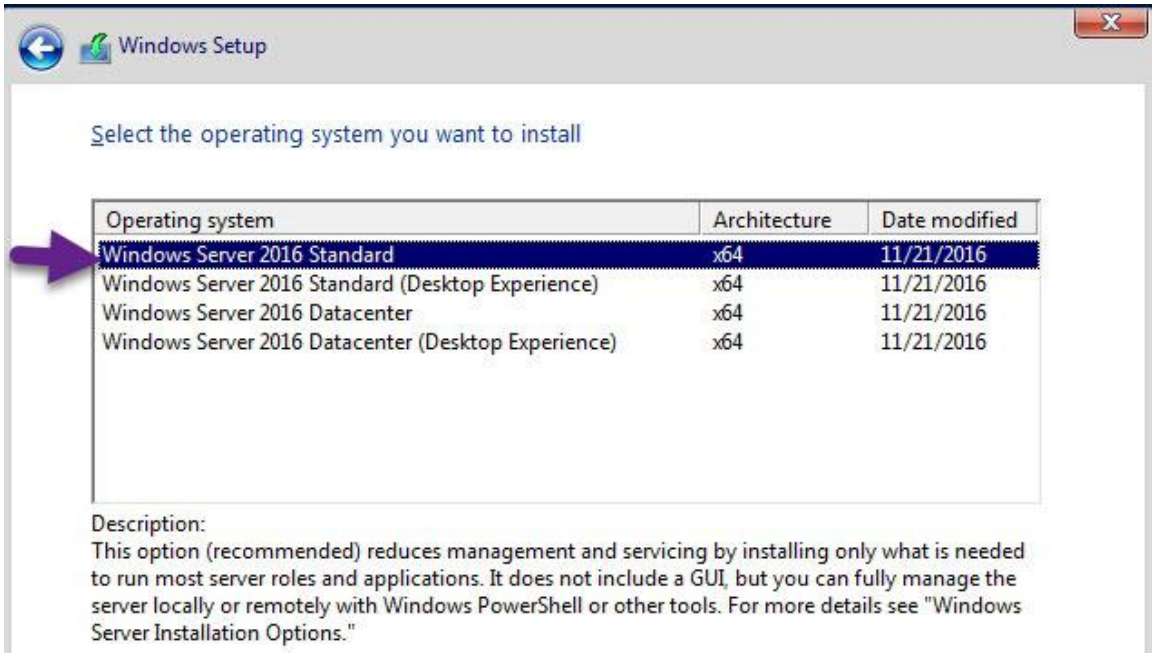

WebServer on HYPER-V01 - Virtual Machine Connection
File Action Media Clipboard View Help
Press any key to boot from CD or DVD...

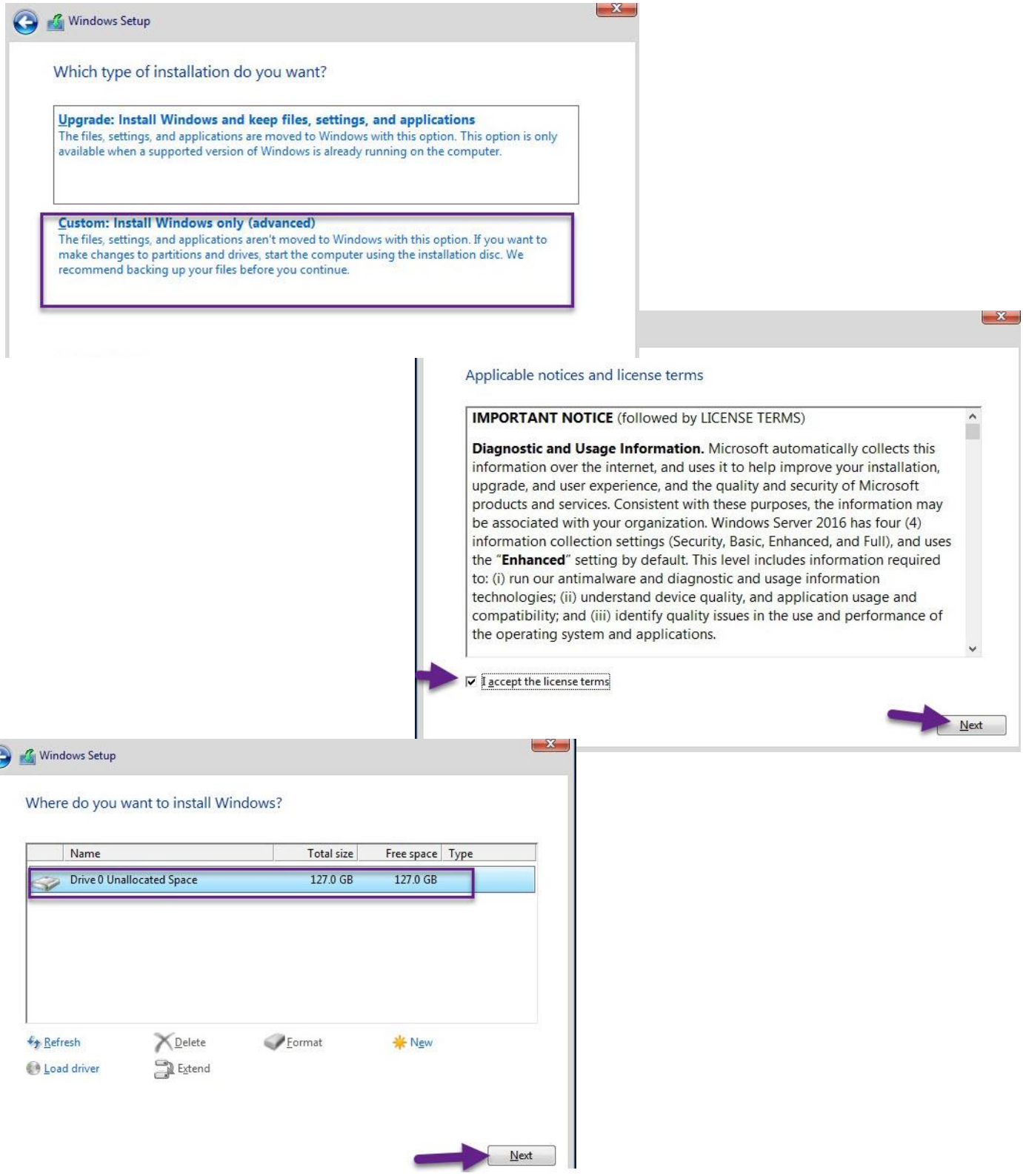

Windows Setup
Windows Server 2016
Language to install: English (United States)
Time and currency format: English (United States)
Keyboard or input method: US
Enter your language and other preferences and click "Next" to continue.
© 2016 Microsoft Corporation. All rights reserved.
Next

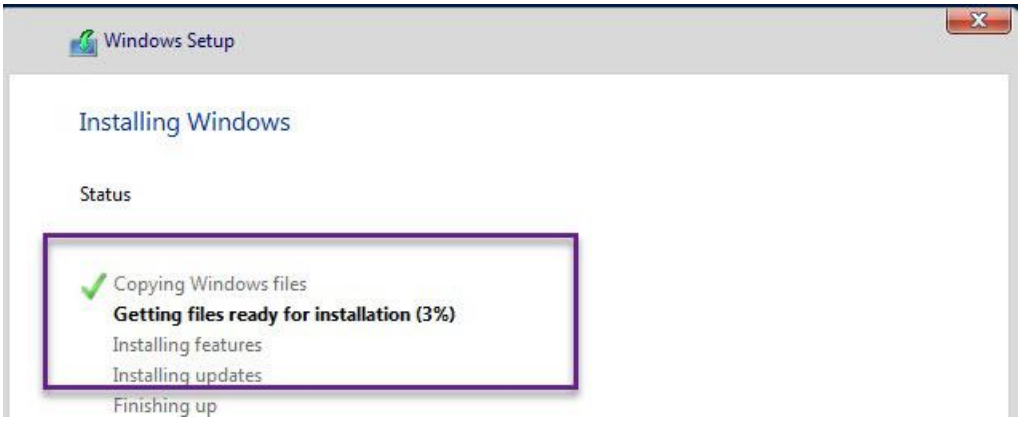

Windows Setup
Windows Server 2016
Install now
Repair your computer
© 2016 Microsoft Corporation. All rights reserved.



Choose Windows Server 2016 Standard Core.




Windows Setup
Which type of installation do you want?
Upgrade: Install Windows and keep files, settings, and applications
The files, settings, and applications are moved to Windows with this option. This option is only available when a supported version of Windows is already running on the computer.
Custom: Install Windows only (advanced)
The files, settings, and applications aren't moved to Windows with this option. If you want to make changes to partitions and drives, start the computer using the installation disc. We recommend backing up your files before you continue.
Applicable notices and license terms
IMPORTANT NOTICE (followed by LICENSE TERMS)
Diagnostic and Usage Information. Microsoft automatically collects this information over the internet, and uses it to help improve your installation, upgrade, and user experience, and the quality and security of Microsoft products and services. Consistent with these purposes, the information may be associated with your organization. Windows Server 2016 has four (4) information collection settings (Security, Basic, Enhanced, and Full), and uses the "Enhanced" setting by default. This level includes information required to: (i) run our antimalware and diagnostic and usage information technologies; (ii) understand device quality, and application usage and compatibility; and (iii) identify quality issues in the use and performance of the operating system and applications.
I accept the license terms
Next
Windows Setup
Where do you want to install Windows?
Name
Total size
Free space
Type
Drive 0 Unallocated Space
127.0 GB
127.0 GB
Refresh
Delete
Format
New
Load driver
Extend
Next



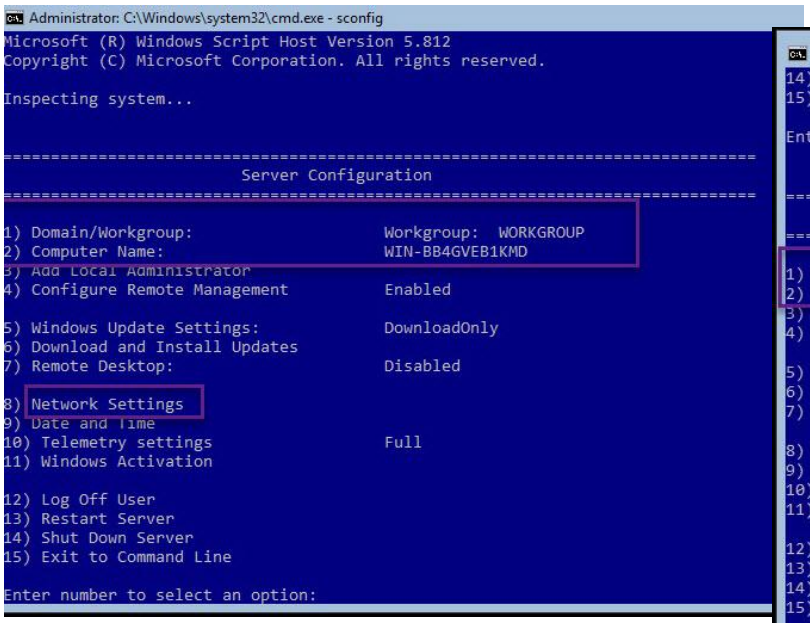
Once the installation is complete, please modify the local administrator's password as it is required to access our server initially.

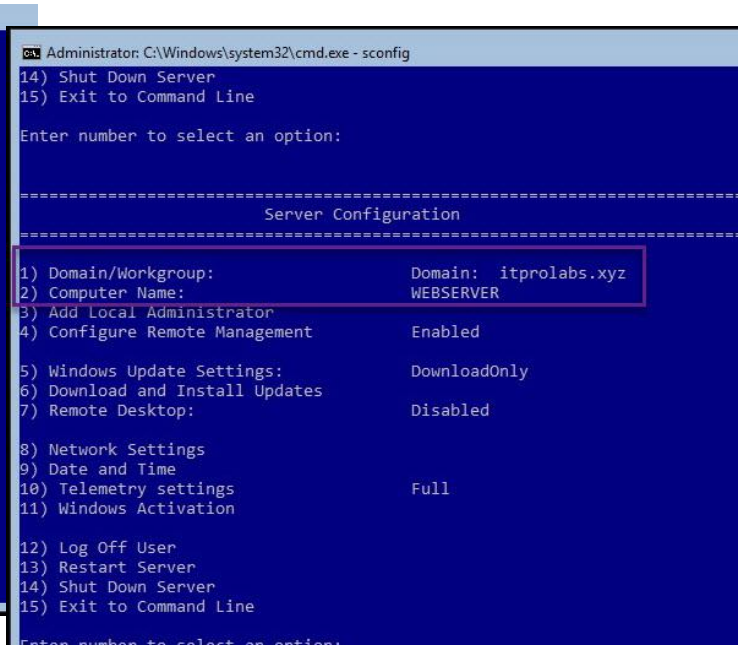
Manage server 2016 Core locally

Windows Server 2016 Initial Configuration

Access the server core with the local admin account and utilize Sconfig to adjust initial settings such as the Server name and network setup for joining the server to the ITPROLABS.XYZ domain.

Server Name: **WebServer**
IP address: **192.168.153.52**
SM:**255.255.255.0**
DNS: **192.168.153.10**
DG: 192.168.153.2

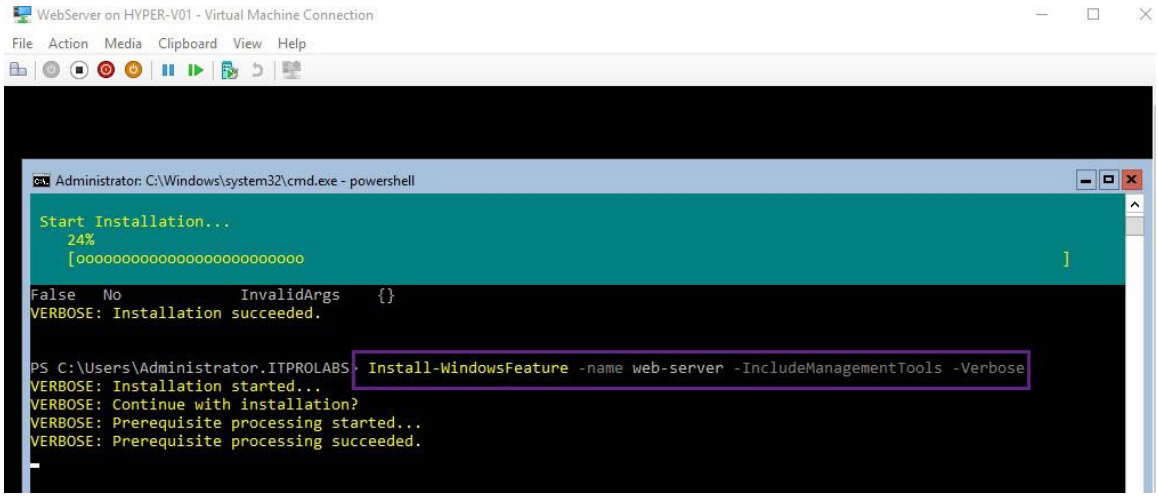




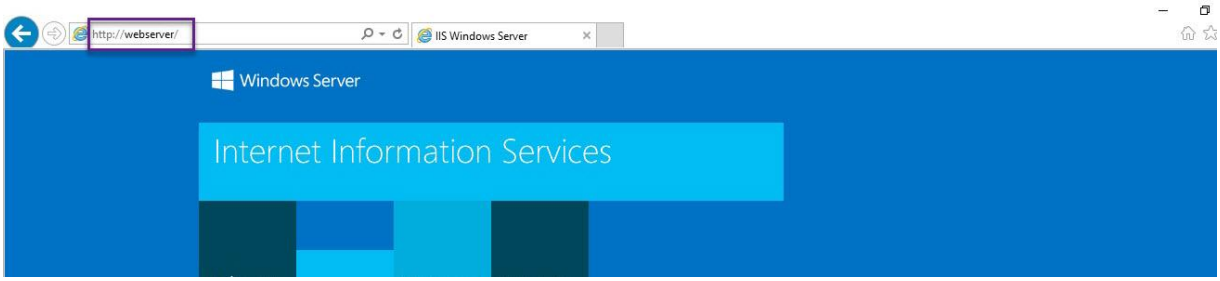
add IIS Role

Type 15 to exit **sconfig** to command line mode then type PowerShell to access PowerShell mode. Through PowerShell use the following command to install IIS server role

```
Install-WindowsFeature -name Web-Server -IncludeManagementTools -verbose
```



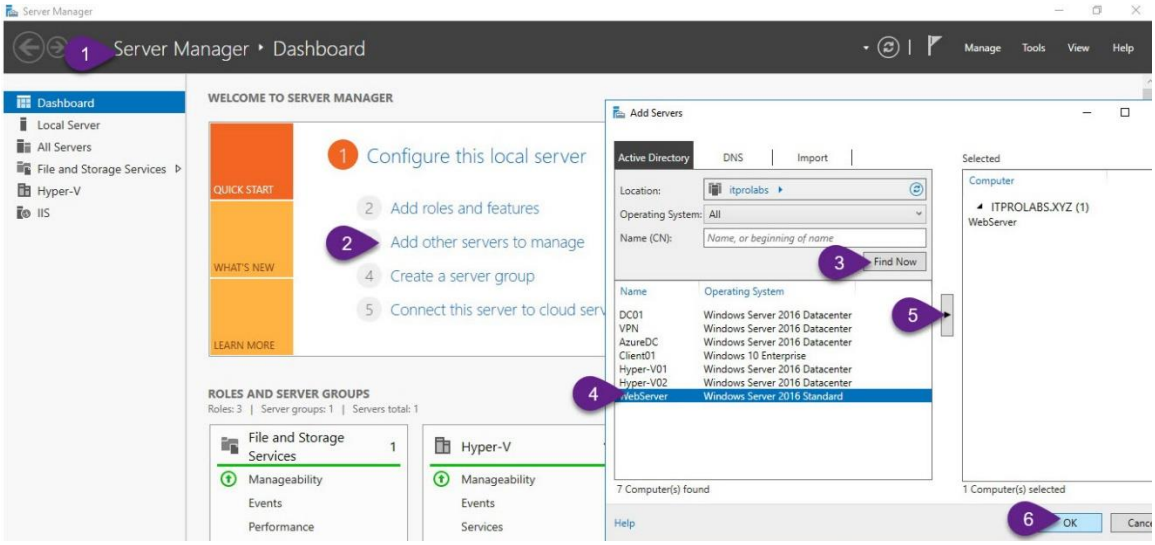
Once the IIS installation is complete, you can access the WebServer via the web as demonstrated below.



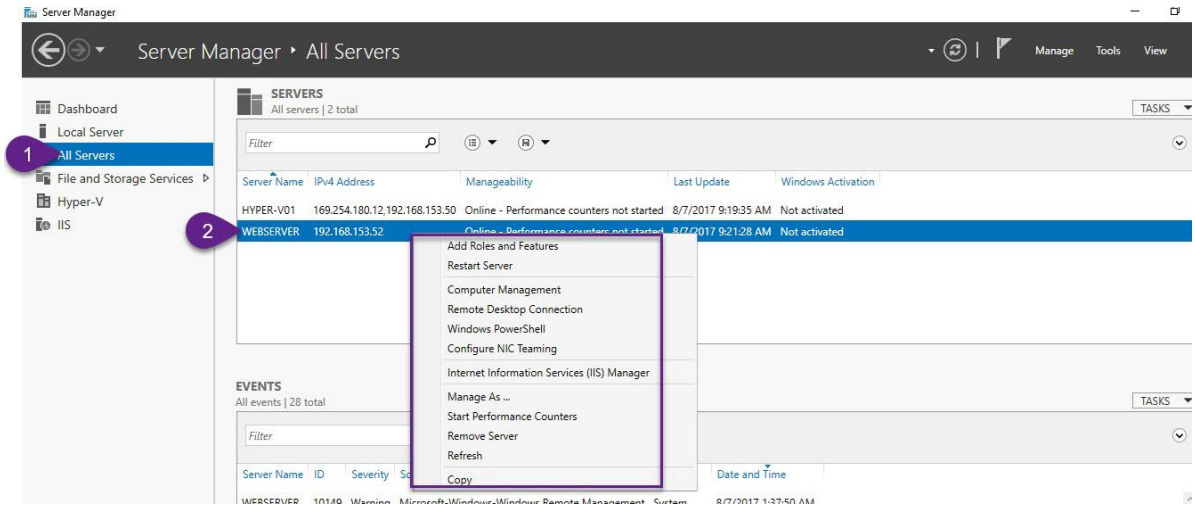
Manage Server Core 2016 Remotely

Using GUI

We have included the server core into an existing GUI server manager as illustrated below, by integrating it with another server that is already a part of our ITPROLABS.XYZ domain network.

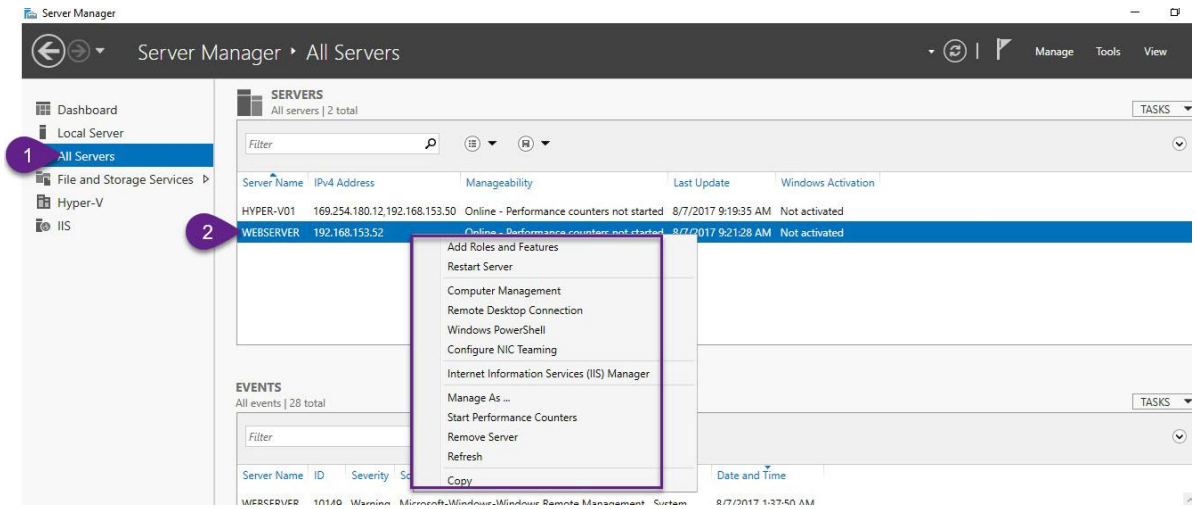


Server Core can now be managed through another server's GUI, enabling remote addition and removal of roles and features, as well as configuration of certain management tasks, as depicted below.



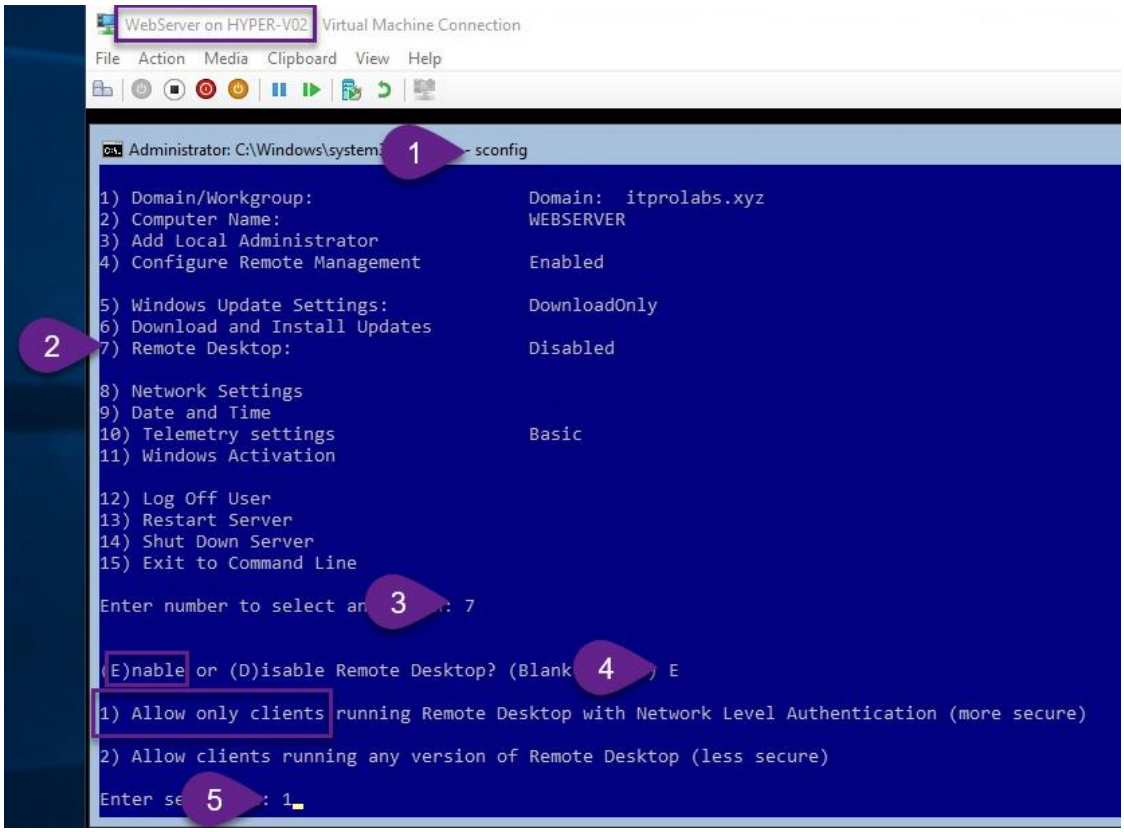
Using PowerShell

By selecting PowerShell from the following down list.



Using Remote Desktop

Additionally, you can access and control the server core remotely using remote desktop, but first, it's necessary to activate remote desktop via the Sconfig console as demonstrated below:



Hyper-V Replication

Lab Scenario

This lab provides basic information about:

1- Install and configure Hyper-V 2016 Server role.
2- Install Windows Server 2016 Core VM on Hyper-V.
3- Enable and configure Hyper-V 2016 Replica Server.
4- Replicate Server Core 2016 VM from Hyper-V server to another through Hyper-V.

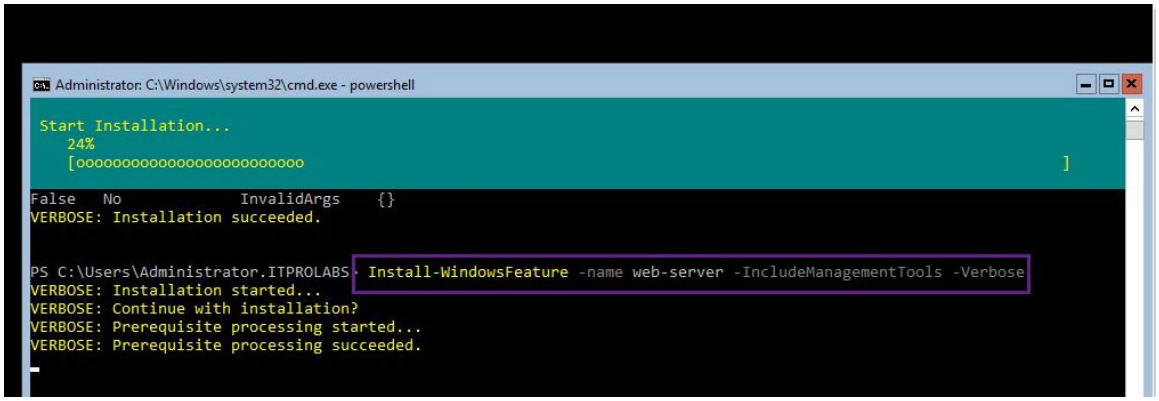
Existing Environment

We will proceed with the previous lab configuration.

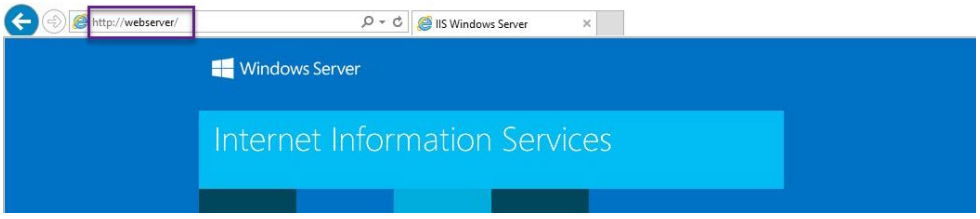
add IIS Role

Type 15 to exit sconfig and access the command line interface, then input PowerShell to enter PowerShell mode. Through PowerShell use the following command to install IIS server role

```
Install-WindowsFeature -name Web-Server -IncludeManagementTools -verbose
```

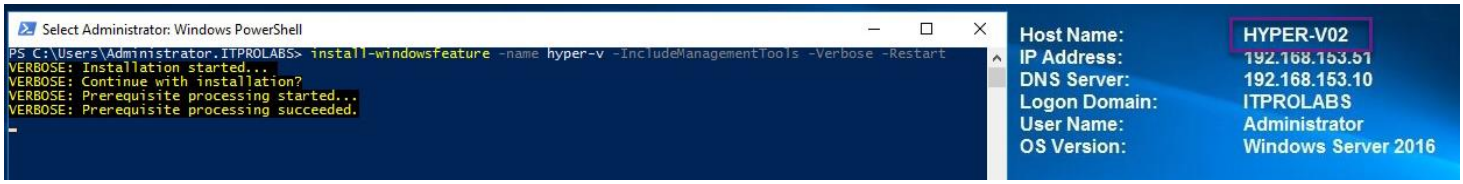


Once the installation of IIS is complete, you will be able to reach the Web Server via the web as demonstrated below.

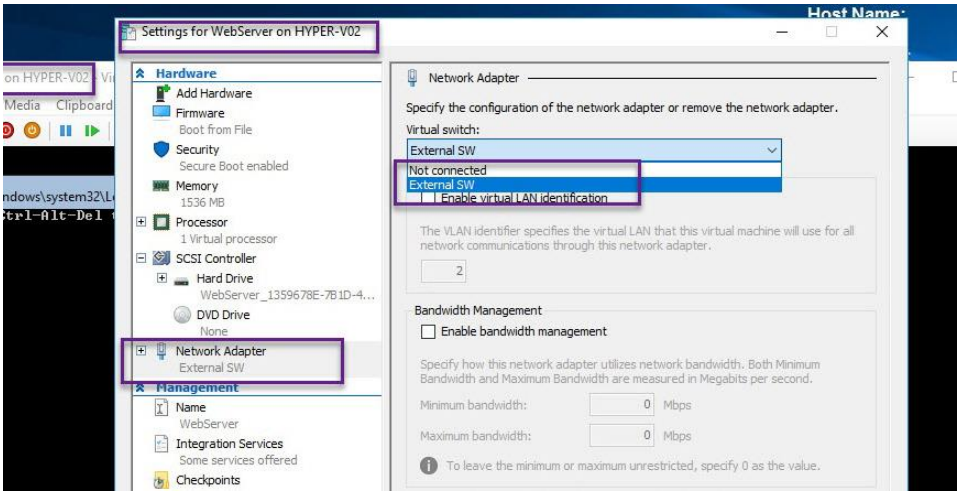


Configure Hyper-V Replica Server to server HYPER-V02

add Hyper-V role through PowerShell



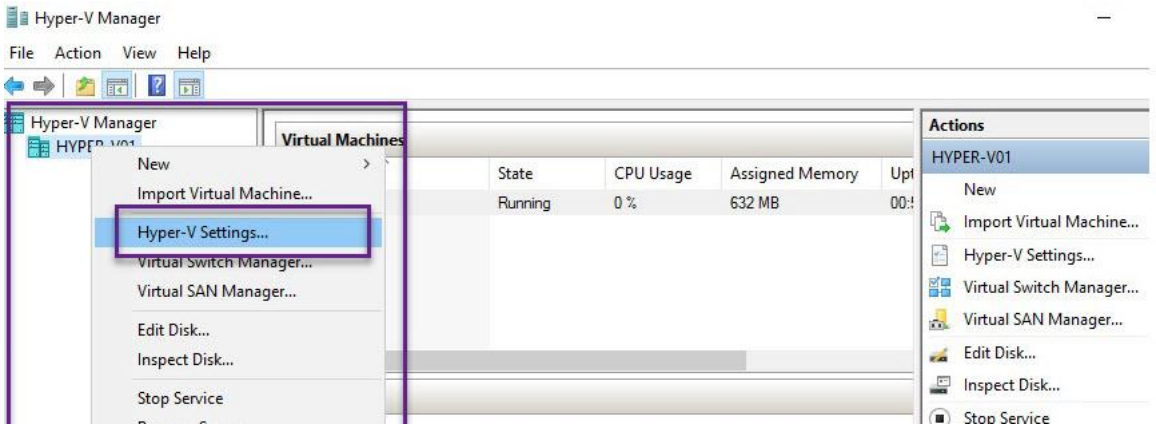
add Virtual Switch to Hyper-V



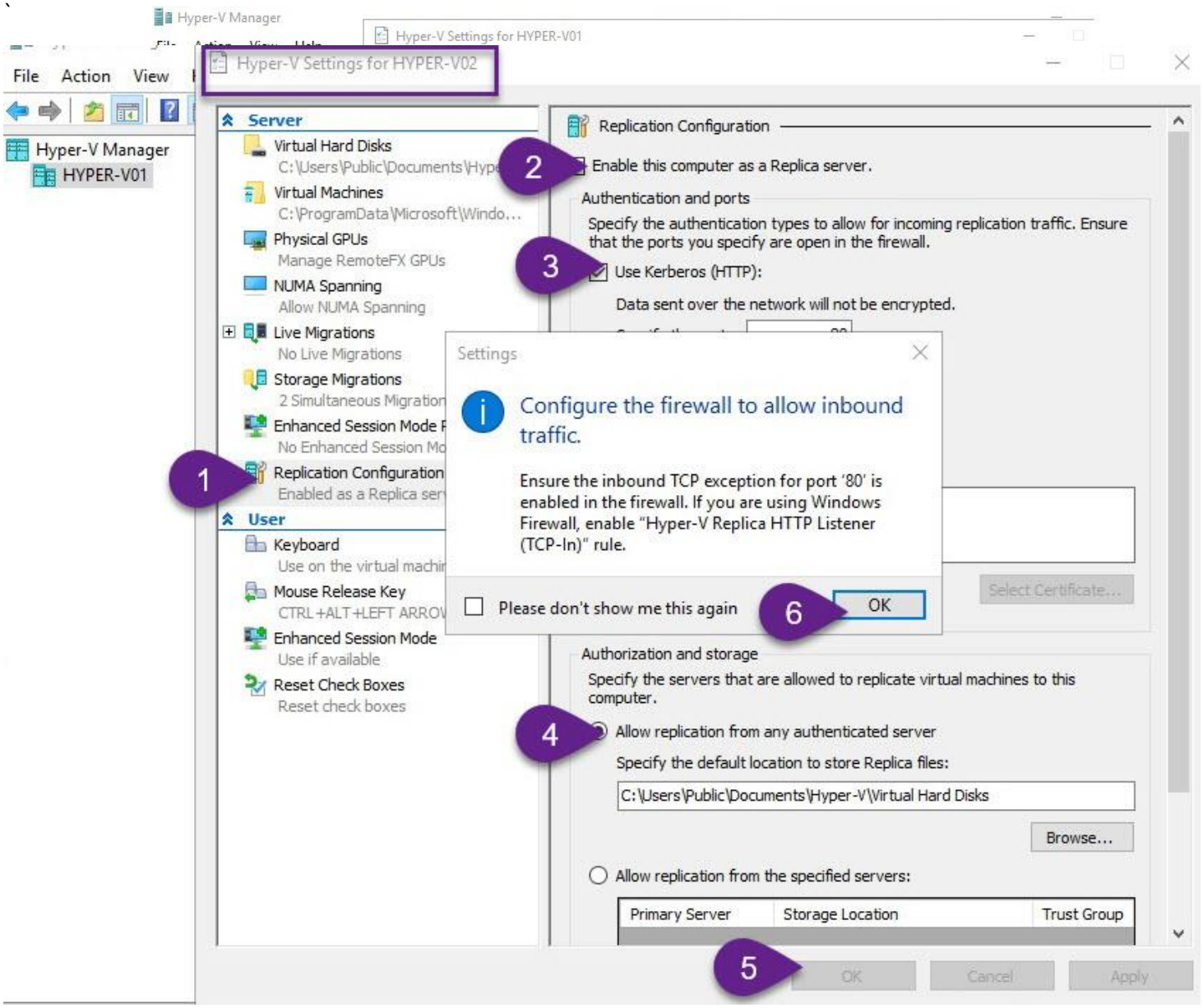
Hyper-V Replication Process

Activate Hyper-V Replication configuration

To facilitate replication of the WebServer VM from the Hyper-V01 server to another server (Hyper-V02), turn on the Hyper-V replication settings on both servers.

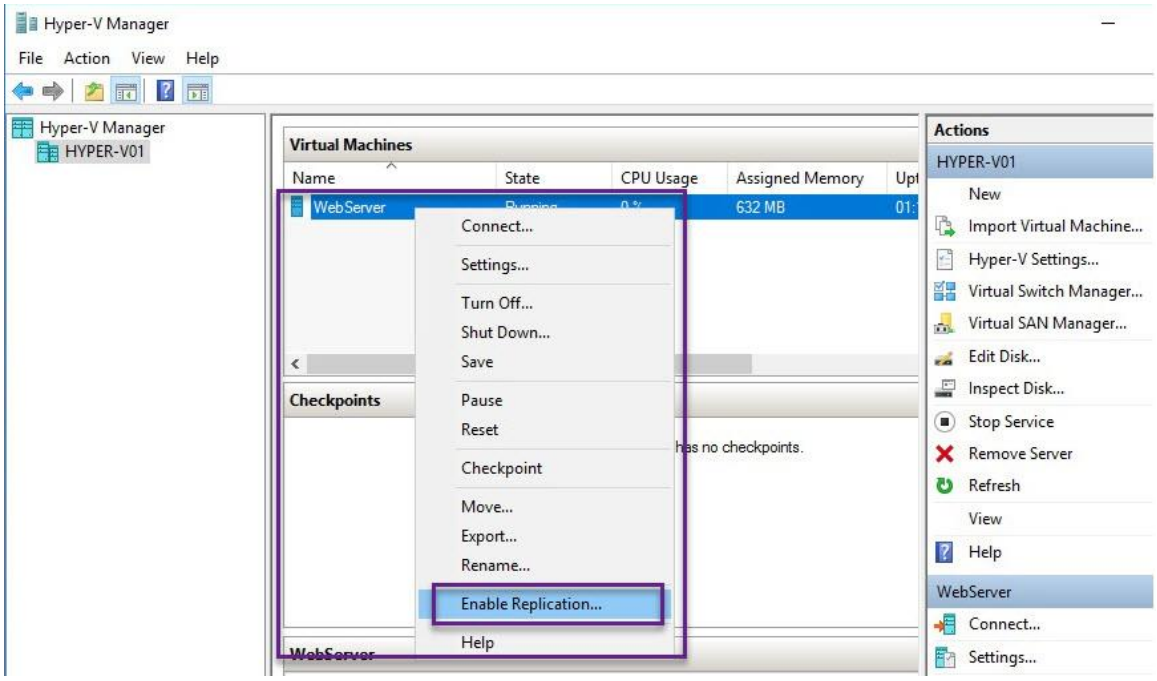


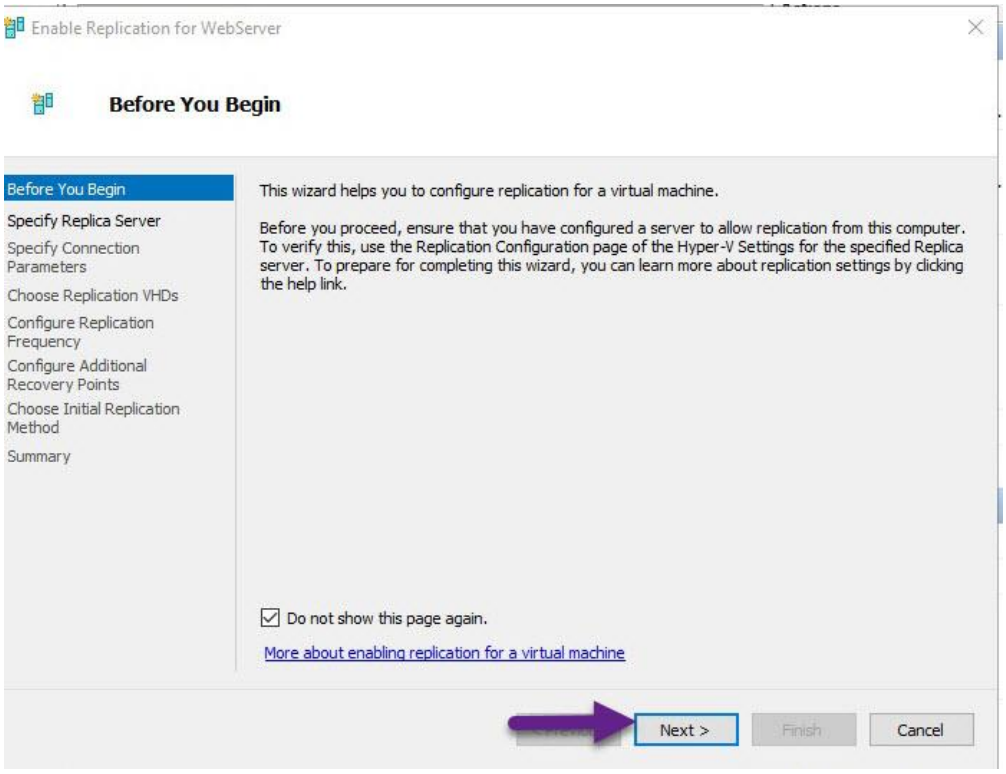
Additionally, apply the same settings to the Hyper-V02 server.



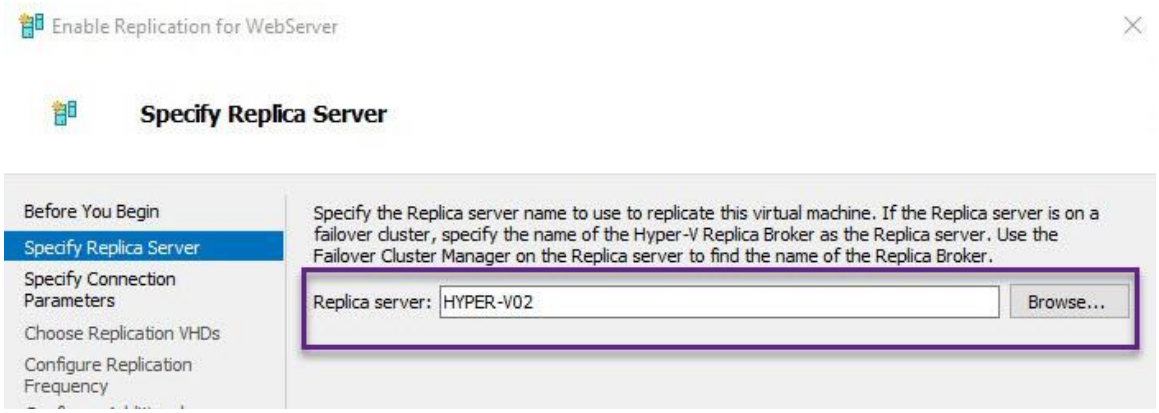
Replication Process

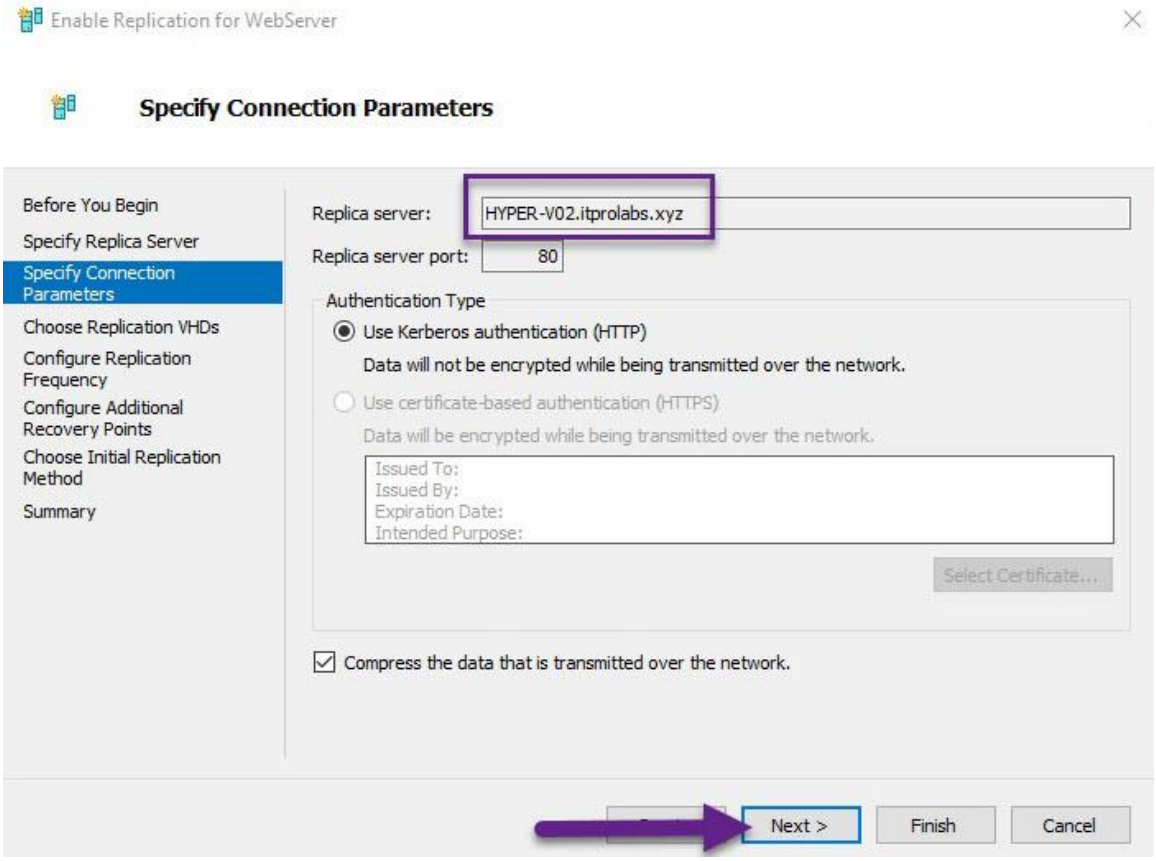
Enable the replication of the WebServer VM from the Hyper-V01 server to the Hyper-V02 server.

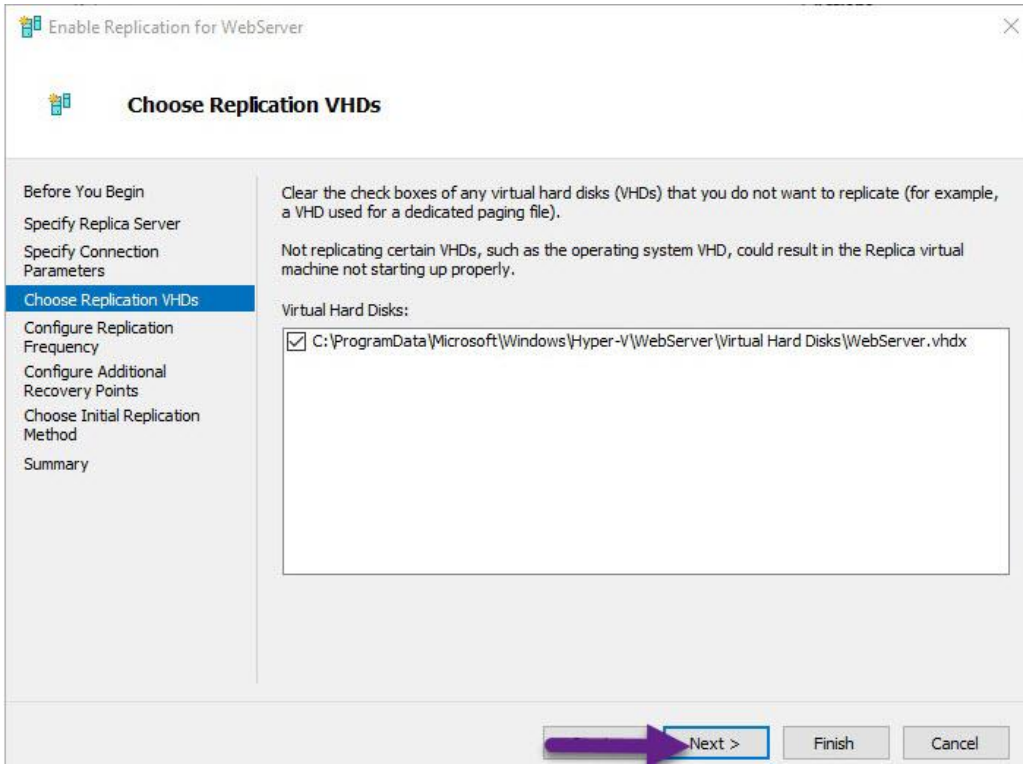


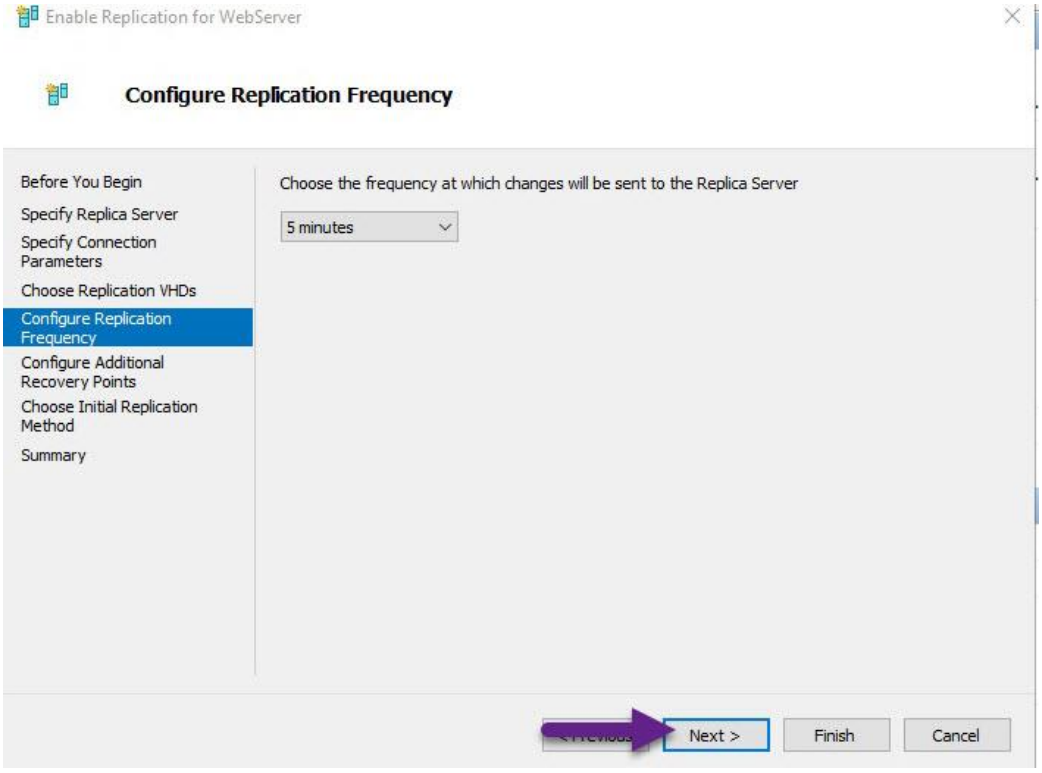


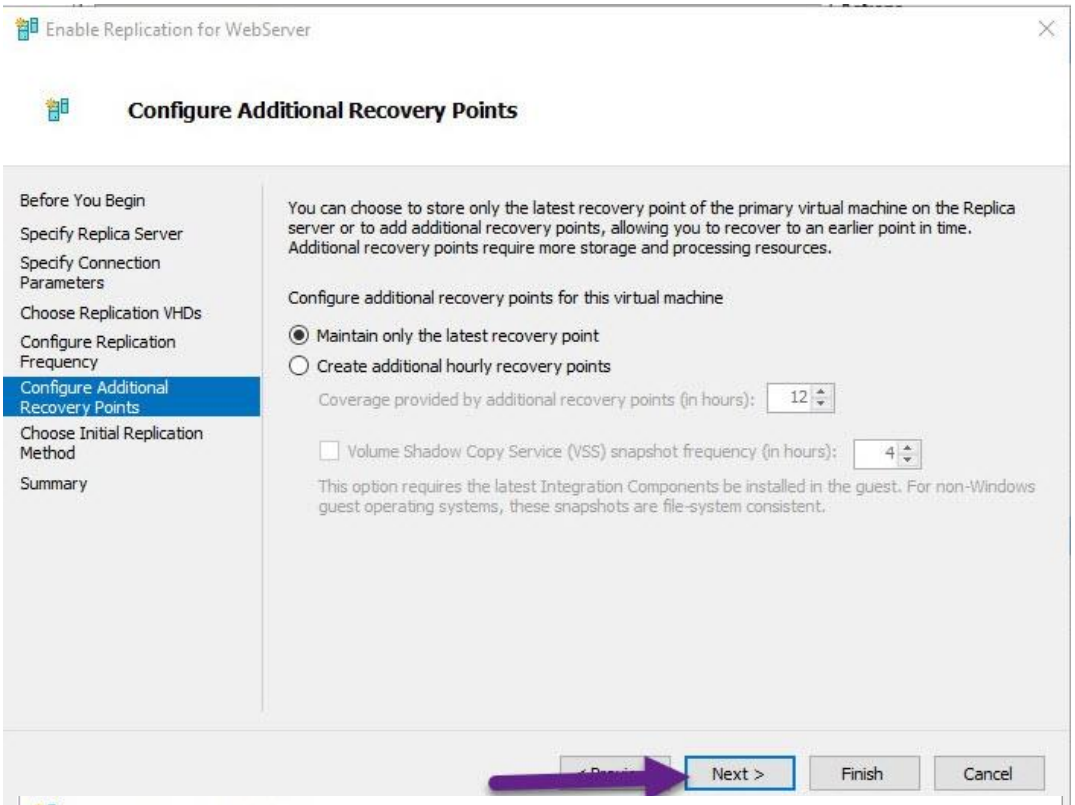
Choose the Hyper-V server for hosting the replicated VM; in this case, the replica server is Hyper-V02.

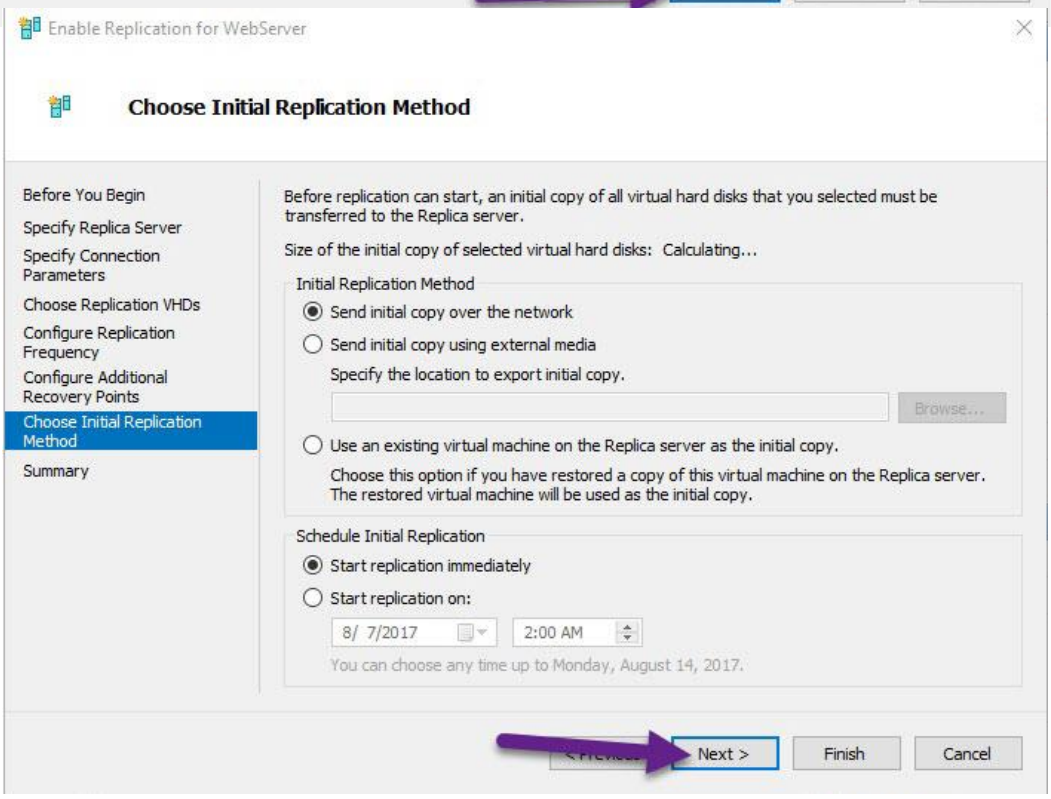




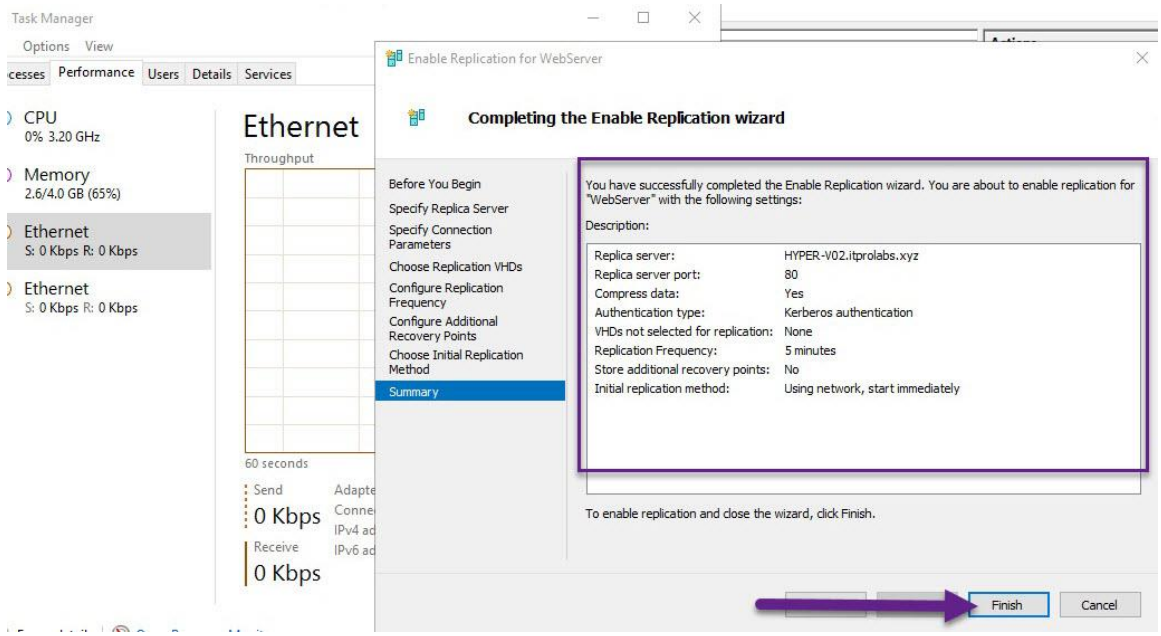

Enable Replication for WebServer
Choose Replication VHDs
Before You Begin
Specify Replica Server
Specify Connection Parameters
Choose Replication VHDs
Configure Replication Frequency
Configure Additional Recovery Points
Choose Initial Replication Method
Summary
Clear the check boxes of any virtual hard disks (VHDs) that you do not want to replicate (for example, a VHD used for a dedicated paging file).
Not replicating certain VHDs, such as the operating system VHD, could result in the Replica virtual machine not starting up properly.
Virtual Hard Disks:
C:\ProgramData\Microsoft\Windows\Hyper-V\WebServer\Virtual Hard Disks\WebServer.vhdx
Next >
Finish
Cancel


Enable Replication for WebServer
Configure Replication Frequency
Before You Begin
Specify Replica Server
Specify Connection Parameters
Choose Replication VHDs
Configure Replication Frequency
Configure Additional Recovery Points
Choose Initial Replication Method
Summary
Choose the frequency at which changes will be sent to the Replica Server
5 minutes
Next >
Finish
Cancel


Enable Replication for WebServer
Configure Additional Recovery Points
Before You Begin
Specify Replica Server
Specify Connection Parameters
Choose Replication VHDs
Configure Replication Frequency
Configure Additional Recovery Points
Choose Initial Replication Method
Summary
You can choose to store only the latest recovery point of the primary virtual machine on the Replica server or to add additional recovery points, allowing you to recover to an earlier point in time. Additional recovery points require more storage and processing resources.
Configure additional recovery points for this virtual machine
Maintain only the latest recovery point
Create additional hourly recovery points
Coverage provided by additional recovery points (in hours): 12
Volume Shadow Copy Service (VSS) snapshot frequency (in hours): 4
This option requires the latest Integration Components be installed in the guest. For non-Windows guest operating systems, these snapshots are file-system consistent.
Next >
Finish
Cancel

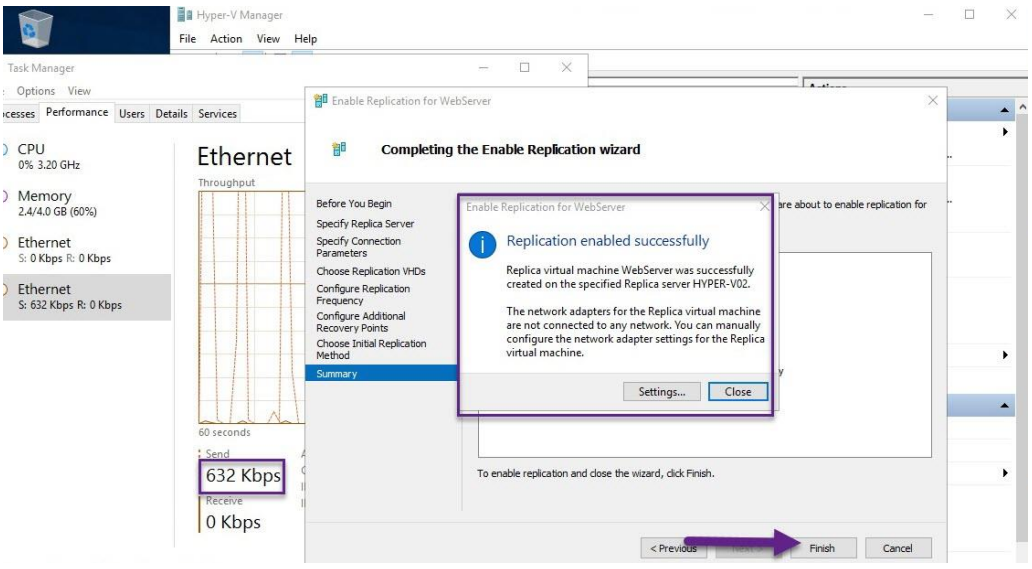

Enable Replication for WebServer
Choose Initial Replication Method
Before You Begin
Specify Replica Server
Specify Connection Parameters
Choose Replication VHDs
Configure Replication Frequency
Configure Additional Recovery Points
Choose Initial Replication Method
Summary
Before replication can start, an initial copy of all virtual hard disks that you selected must be transferred to the Replica server.
Size of the initial copy of selected virtual hard disks: Calculating...
Initial Replication Method
Send initial copy over the network
Send initial copy using external media
Specify the location to export initial copy.
Browse...
Use an existing virtual machine on the Replica server as the initial copy.
Choose this option if you have restored a copy of this virtual machine on the Replica server. The restored virtual machine will be used as the initial copy.
Schedule Initial Replication
Start replication immediately
Start replication on:
8/ 7/2017
2:00 AM
You can choose any time up to Monday, August 14, 2017.
Next >
Finish
Cancel

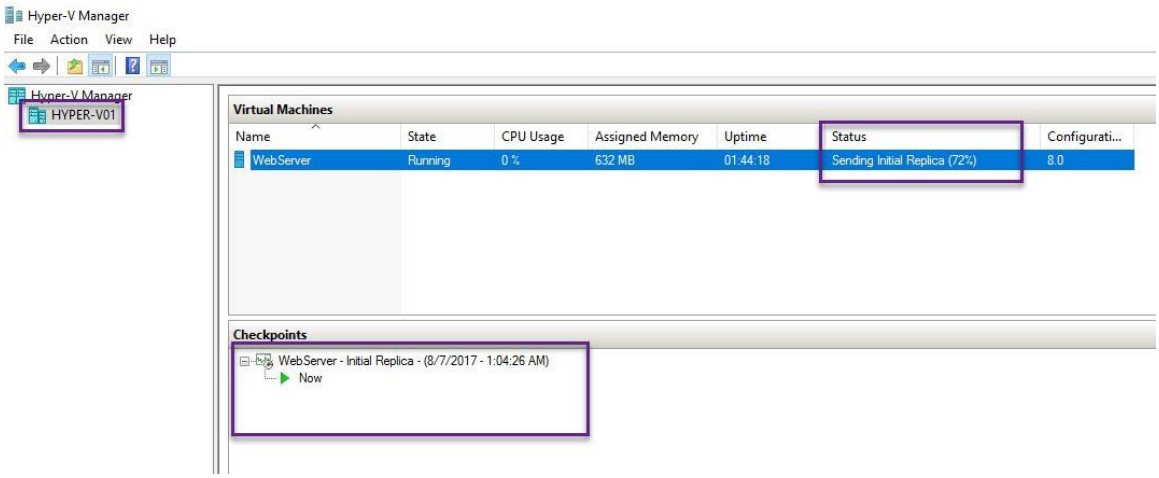
By monitoring network traffic via the task manager, you'll observe that there is no traffic before the replication process commences.



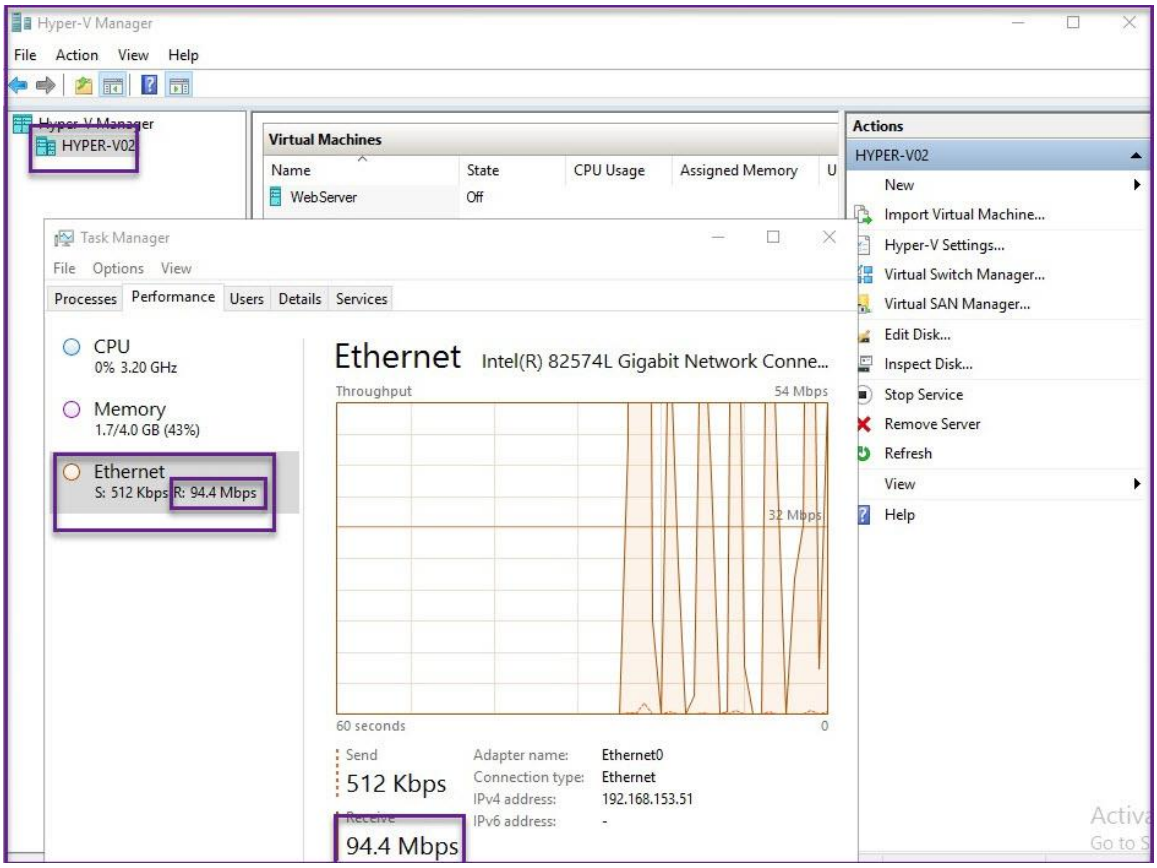
Replication Status

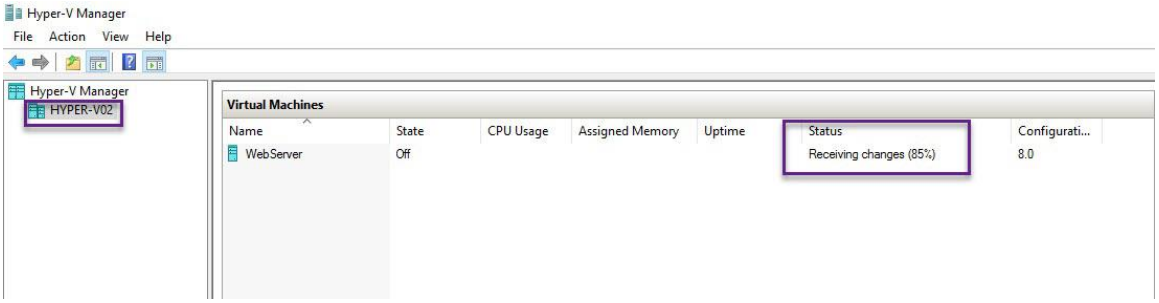
As replication begins, be aware that there will be a surge in network traffic due to the data being transmitted across the network as per our setup.





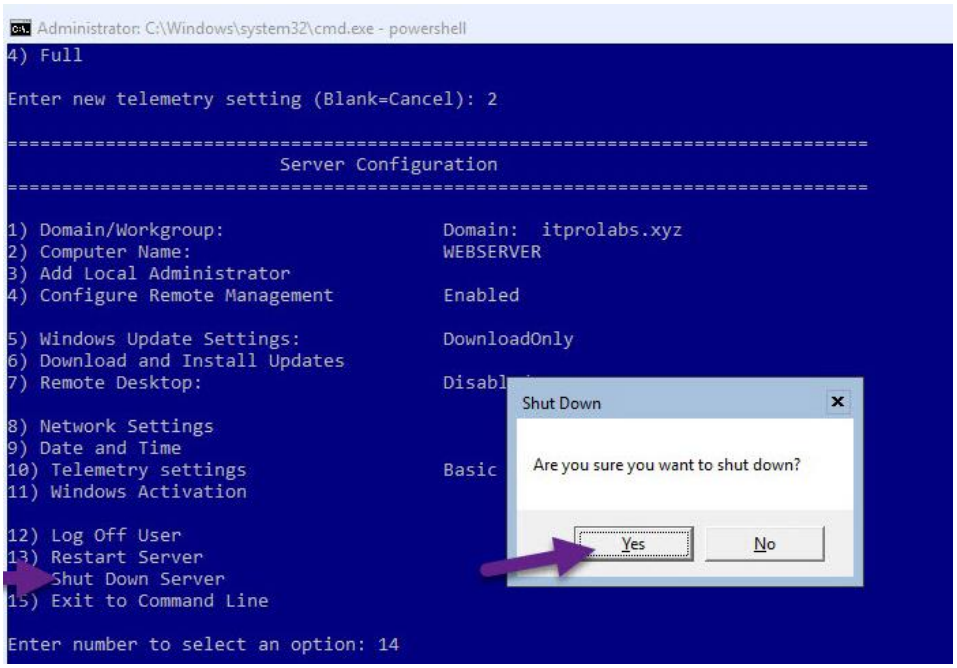
Switch to the alternate Hyper-V server that's accepting the replicated VM and note the uptick in inbound traffic.



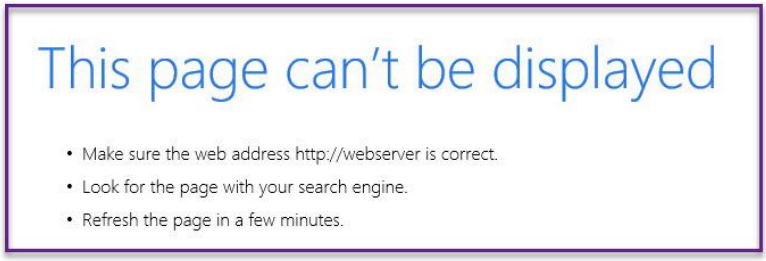


Test replicated VM

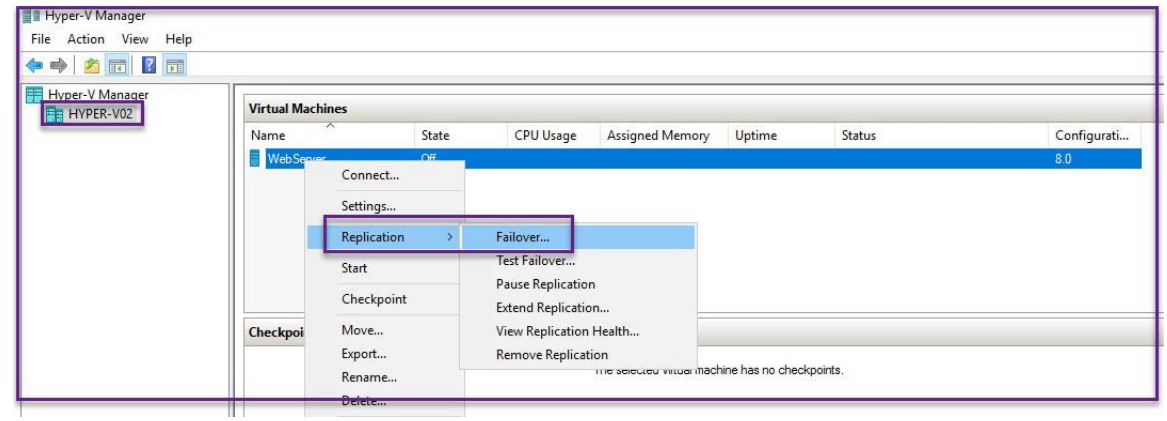
- Turn off the primary web server virtual machine and then attempt to connect to IIS, which is hosted on that server.

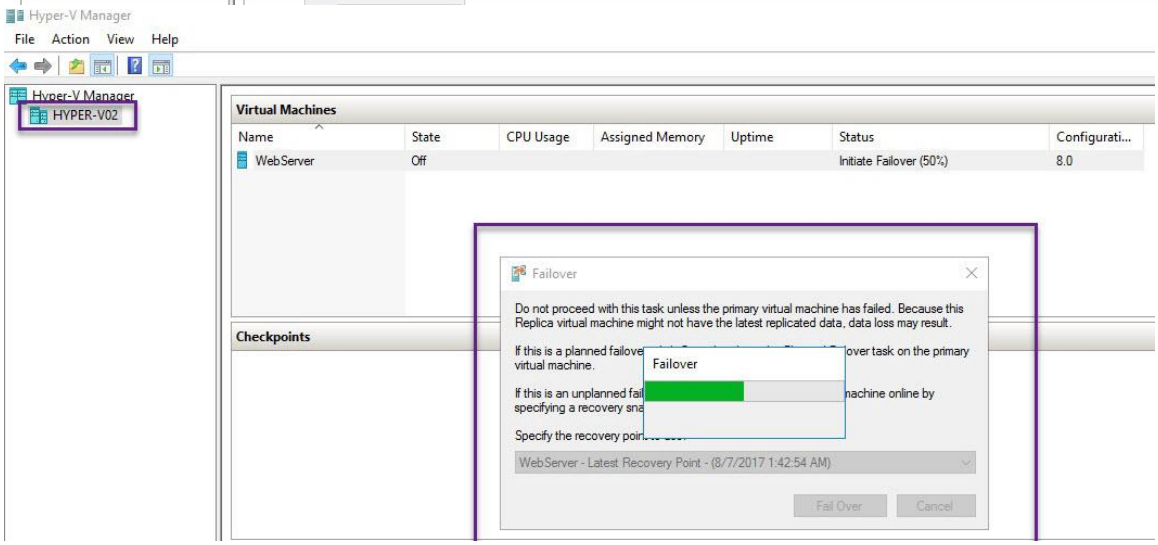


Currently, IIS services are offline.

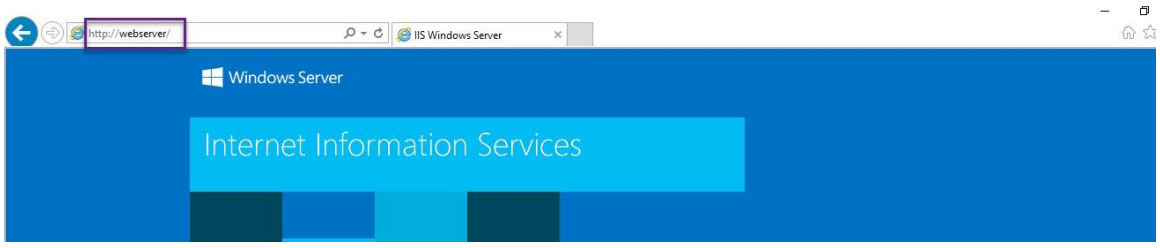


- Navigate to the replicated virtual machine and refer to the figures below for instructions on how to manage it.





Attempt to connect to IIS on the WebServer VM again; it's now functioning via the replicated VM.



IPv6

Number of IPv6 Addresses

IPv4:

- **Total addresses**: 2^{32}
- **Approximate number**: 4.3 billion addresses

IPv6:

- **Total addresses**: 2^{128}
- **Approximate number**: 3.4×10^{38} addresses
- **To visualize**: This is 340 undecillion addresses, a number so large it exceeds the total number of grains of sand on Earth by many orders of magnitude.

Format of IPv6 Addresses

Address Length and Representation

- An IPv6 address is 128 bits long.
- It is written as eight groups of four hexadecimal digits, each group representing 16 bits.
- Groups are separated by colons (:).

Example

- **Full IPv6 Address:** 2001:0db8:85a3:0000:0000:8a2e:0370:7334

Simplification Rules

1. **Leading Zeros Suppression:**
    - Leading zeros in any 16-bit group can be omitted.
    - **Example:** 2001:0db8:85a3:0000:0000:8a2e:0370:7334 becomes 2001:db8:85a3:0:0:8a2e:370:7334
2. `
    - A contiguous sequence of 16-bit groups that are all zeros can be replaced with ::.
    - This compression can only be applied once in an address to avoid ambiguity.
    - **Example:** 2001:0db8:0000:0000:0000:0000:0000:0001 becomes 2001:db8::1
    - **Example:** 2001:0db8:0000:0000:0000:0000:0000:0000 becomes 2001:db8::

Special Cases

- **Loopback Address:**
    - Full notation: 0000:0000:0000:0000:0000:0000:0000:0001
    - Compressed notation: ::1

- **Unspecified Address:**
  - Represents the absence of an address.
  - Full notation: 0000:0000:0000:0000:0000:0000:0000:0000
  - Compressed notation: ::

IPv6 and Ports

- When specifying a port number with an IPv6 address, enclose the address in square brackets.
  - **Example:** [2001:db8::1]:8080

Link-Local Addresses

- Link-local addresses are used for communication within a single network segment.
- They start with the prefix fe80::/10.
  - **Example:** fe80::1ff:fe23:4567:890a

Examples of IPv6 Address Representations

1. **Full Address:**
   - 2001:0db8:0000:0000:0000:ff00:0042:8329
2. **Leading Zeros Suppressed:**
   - 2001:db8:0:0:0:ff00:42:8329
3. **Consecutive Zeros Compressed:**
   - 2001:db8::ff00:42:8329
4. **Combination of Both:**
   - 2001:db8::ff00:42:8329

IPv6 Address Types

1. **Unicast:**
   - Identifies a single interface.
   - **Example:** 2001:db8::1
2. **Multicast:**
   - Identifies multiple interfaces.
   - Prefix starts with ff00::/8.
   - **Example:** ff02::1
3. **Anycast:**
   - Identifies multiple interfaces, but a packet sent to an anycast address is delivered to the nearest interface.
   - Typically uses unicast address format.

Assigning IPv6 Addresses

IPv6 addresses can be assigned using different methods, which can be broadly categorized into stateful and stateless configurations.

1. Stateful Configuration

- **Stateful DHCPv6:**
  - Devices obtain their IPv6 addresses and other network configuration details from a DHCPv6 server.
  - The DHCPv6 server maintains a state, keeping track of which addresses are assigned to which devices.
  - Provides advanced configuration options, such as DNS servers and other network services.
- **Manual Configuration:**
  - IPv6 addresses are manually configured on each device by an administrator.
  - Useful for servers and other devices that require static IP addresses.
  - Allows for precise control over address assignments and network configurations.

2. Stateless Address Autoconfiguration (SLAAC)

- **SLAAC:**
  - Devices configure their own IPv6 addresses using information advertised by routers on the network.
  - No DHCP server is required.
  - Provides basic configuration sufficient to get a device up and running on the network.

SLAAC Process:

1. **Router Advertisement (RA):**
   - Routers periodically send Router Advertisement messages to the all-nodes multicast address (ff02::1).
   - These messages include network prefixes and other configuration parameters.
2. **Address Generation:**
   - The device uses the received prefix to generate its own IPv6 address.
   - Typically combines the prefix with a modified version of its MAC address or a randomly generated interface identifier.
   - Example: If the prefix is 2001:db8::/64 and the device's MAC address is 00:1a:2b:3c:4d:5e, the IPv6 address might be 2001:db8::1a2b:3cff:fe4d:5e.
3. **Duplicate Address Detection (DAD):**
   - The device performs Duplicate Address Detection to ensure the generated address is unique on the network.
   - Sends a Neighbor Solicitation message to the solicited-node multicast address derived from its new address.
   - If no Neighbor Advertisement is received in response, the address is considered unique.

---

4. **Neighbor Solicitation and Advertisement:**
    - Neighbor Solicitation messages are used to discover other devices on the network and to resolve their link-layer addresses.
    - Neighbor Advertisement messages are used to respond to Neighbor Solicitations and to announce changes in link-layer addresses.

Advantages and Limitations of SLAAC:

- **Advantages:**
    - Simple and efficient for basic network configuration.
    - Reduces the need for a centralized DHCP server.
- **Limitations:**
    - Does not support advanced configuration options (e.g., setting DNS servers).
    - Not suitable for environments where precise control over IP address assignments is required.

Hybrid Configuration

- **DHCPv6 for Additional Configuration:**
    - In many networks, SLAAC is used to assign basic IP addresses, while DHCPv6 is used to provide additional configuration details.
    - Devices use SLAAC to generate their addresses and then request additional settings (like DNS server addresses) from a DHCPv6 server.

Examples of IPv6 Addresses with Public DNS Servers

Here are five examples of IPv6 addresses configured with public DNS servers.

1. **Static IPv6 Address Example 1:**
    - **IPv6 Address:** 2001:db8:1::1/64
    - **Gateway:** 2001:db8:1::1
    - **DNS Servers:**
        - 2001:4860:4860::8888 (Google DNS)
        - 2001:4860:4860::8844 (Google DNS)
2. **Static IPv6 Address Example 2:**
    - **IPv6 Address:** 2001:db8:2::2/64
    - **Gateway:** 2001:db8:2::1
    - **DNS Servers:**
        - 2620:119:35::35 (OpenDNS)
        - 2620:119:53::53 (OpenDNS)
3. **Static IPv6 Address Example 3:**
    - **IPv6 Address:** 2001:db8:3::3/64
    - **Gateway:** 2001:db8:3::1
    - **DNS Servers:**
        - 2001:4860:4860::8888 (Google DNS)
        - 2001:4860:4860::8844 (Google DNS)

4. **Static IPv6 Address Example 4:**
    - **IPv6 Address:** 2001:db8:4::4/64
    - **Gateway:** 2001:db8:4::1
    - **DNS Servers:**
        - 2620:119:35::35 (OpenDNS)
        - 2620:119:53::53 (OpenDNS)
5. **Static IPv6 Address Example 5:**
    - **IPv6 Address:** 2001:db8:5::5/64
    - **Gateway:** 2001:db8:5::1
    - **DNS Servers:**
        - 2001:4860:4860::8888 (Google DNS)
        - 2001:4860:4860::8844 (Google DNS)

Pv6 Support

OS Support

- All modern operating systems, including Android and iOS, now support IPv6.

Application Support

- Most applications today support IPv6. You can typically find IPv6 support listed in the feature list of the application.

ISP Support

- IPv6 adoption among ISPs has been slow. To see how slow, refer to statistics on IPv6 content requests:
    - IPv6 test - IPv6/4 connectivity and speed test (ipv6-test.com)
    - World IPv6 Launch Measurements
- Deployment of IPv6 by different ISPs is progressing.

Checking IPv6 Usage

- You can check if a domain uses IPv6 by pinging it with IPv6:

```
ping -6 google.com
```

Router Support

- If your ISP supports IPv6 but your router does not, you won't be able to use IPv6 on your network.

Dual Stack Support

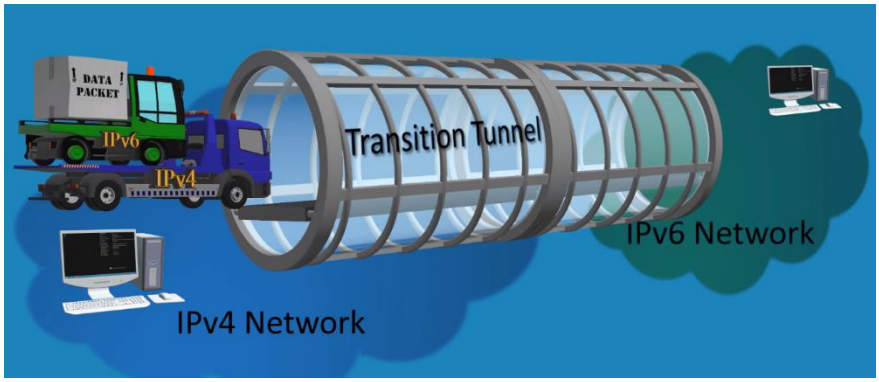
- Dual stack support means your system is configured with both IPv4 and IPv6. Applications will choose to use either IPv4 or IPv6 based on availability.

Tunneling Across IPv4: Two Scenarios

Scenario 1: IPv4-to-IPv6 Communication

- **Description**:
  - One PC is configured only with IPv4 and needs to connect to another PC which uses only IPv6.
- **Process**:

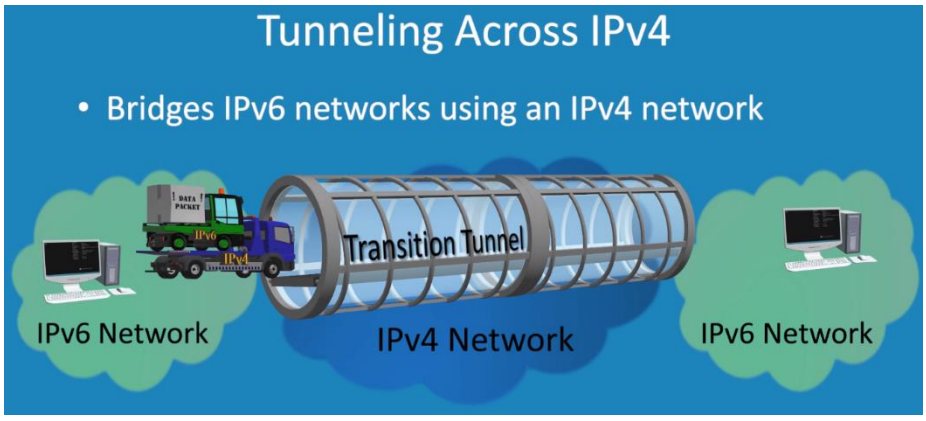
1. The IPv4 packet is encapsulated within an IPv6 packet.
2. The encapsulated packet is routed through the IPv6 network.
3. When the packet arrives at the destination, the IPv6 encapsulation is removed, and the original IPv4 packet is delivered to the IPv6 PC.



Scenario 2: IPv6-to-IPv6 Communication Through IPv4 Network

- **Description**:
  - Two PCs are configured with IPv6 only and need to communicate through an IPv4 network.
- **Process**:

1. The IPv6 packet is encapsulated within an IPv4 packet.
2. The encapsulated packet is sent through the IPv4 network via a tunnel.
3. When the packet arrives at the destination, the IPv4 encapsulation is removed, and the original IPv6 packet is delivered to the IPv6 PC.



IPv6 Command

Display IP Configuration

1. **Show IP Configuration (IPv4 and IPv6)**
   ipconfig /all
2. **Show IPv6 Configuration Only**
   ipconfig /all | findstr /i "ipv6"

Ping

1. **Ping an IPv6 Address**
   ping -6 <IPv6 address>
   ping -6 2001:db8::1

Traceroute

1. **Traceroute to an IPv6 Address**
   tracert -6 <IPv6 address>
   tracert -6 2001:db8::1

DNS Lookup

1. **DNS Lookup (IPv6)**
   nslookup -type=AAAA <hostname>
   nslookup -type=AAAA example.com

Reset Network Configuration

1. **Reset IPv6 Network Configuration**
   netsh int ipv6 reset
2. **Reset IPv4 and IPv6 Network Configuration and Winsock**
   netsh int ip reset
   netsh winsock reset

Renew IP Configuration

1. **Renew IPv6 Address**
   ipconfig /renew6
2. **Release IPv6 Address**
   ipconfig /release6

DNS Cache Management

1. **Show DNS Cache**
   ipconfig /displaydns
2. **Flush DNS Cache**
   ipconfig /flushdns
