Windows Server 2019

Implementing an Active Directory Infrastructure and Common Server Roles

Contents

Module 1: Install Windows Servers in host and compute environments

Determine Windows Server 2019 installation requirements

Processor
Processor performance depends not only on the clock frequency of the processor, but also on the number of processor cores and the size of the processor cache. The following are the processor requirements for this product:

Minimum:
1.4 GHz 64-bit processor
Compatible with x64 instruction set
Supports NX and DEP
Supports CMPXCHG16b, LAHF/SAHF, and PrefetchW
Supports Second Level Address Translation (EPT or NPT)

RAM
The following are the estimated RAM requirements for this product:

Minimum:
512 MB (2 GB for Server with Desktop Experience installation option)
ECC (Error Correcting Code) type or similar technology, for physical host deployments

Storage controller and disk space requirements
Computers that run Windows Server 2019 must include a storage adapter that is compliant with the PCI Express architecture specification. Persistent storage devices on servers classified as hard disk drives must not be PATA. Windows Server 2019 does not allow ATA/PATA/IDE/EIDE for boot, page, or data drives.

The following are the estimated minimum disk space requirements for the system partition.

Minimum: 32 GB

Determine appropriate Windows Server 2019 editions per workloads

Locks and Limits

Locks and Limits	**Windows Server 2019 Standard**	**Windows Server 2019 Datacenter**
Maximum number of users	Based on CALs	Based on CALs
Maximum SMB connections	16,777,216	16,777,216
Maximum RRAS connections	unlimited	unlimited
Maximum IAS connections	2,147,483,647	2,147,483,647
Maximum RDS connections	65,535	65,535
Maximum number of cores	unlimited	unlimited
Maximum RAM	24 TB	24 TB
Can be used as virtualization guest	Yes; 2 vm, +1 Hyper-V host per license	Yes; unlimited vm, +1 Hyper-V host per license
Server can join a domain	yes	yes
Edge network protection/firewall	no	no
DirectAccess	yes	yes

Server roles

Windows Server roles available	Role services	Standard	Datacenter
Active Directory Certificate Services		Yes	Yes
Active Directory Domain Services		Yes	Yes
Active Directory Federation Services		Yes	Yes
AD Lightweight Directory Services		Yes	Yes
AD Rights Management Services		Yes	Yes
Device Health Attestation		Yes	Yes
DHCP Server		Yes	Yes
DNS Server		Yes	Yes
Fax Server		Yes	Yes
File Server		Yes	Yes
BranchCache for Network Files		Yes	Yes
Data Deduplication		Yes	Yes
DFS Namespaces		Yes	Yes
DFS Replication		Yes	Yes
File Server Resource Manager		Yes	Yes
File Server VSS Agent Service		Yes	Yes
iSCSI Target Server		Yes	Yes
iSCSI Target Storage Provider		Yes	Yes
Server for NFS		Yes	Yes
Work Folders		Yes	Yes
Storage Services		Yes	Yes
Host Guardian Service		Yes	Yes
Hyper-V		Yes	Yes; including Shielded Virtual Machines
Network Controller		No	Yes
Print and Document Services		Yes	Yes
Remote Access		Yes	Yes
Remote Desktop Services		Yes	Yes
Volume Activation Services		Yes	Yes
Web Services (IIS)		Yes	Yes
Windows Server Update Services		Yes	Yes

Features

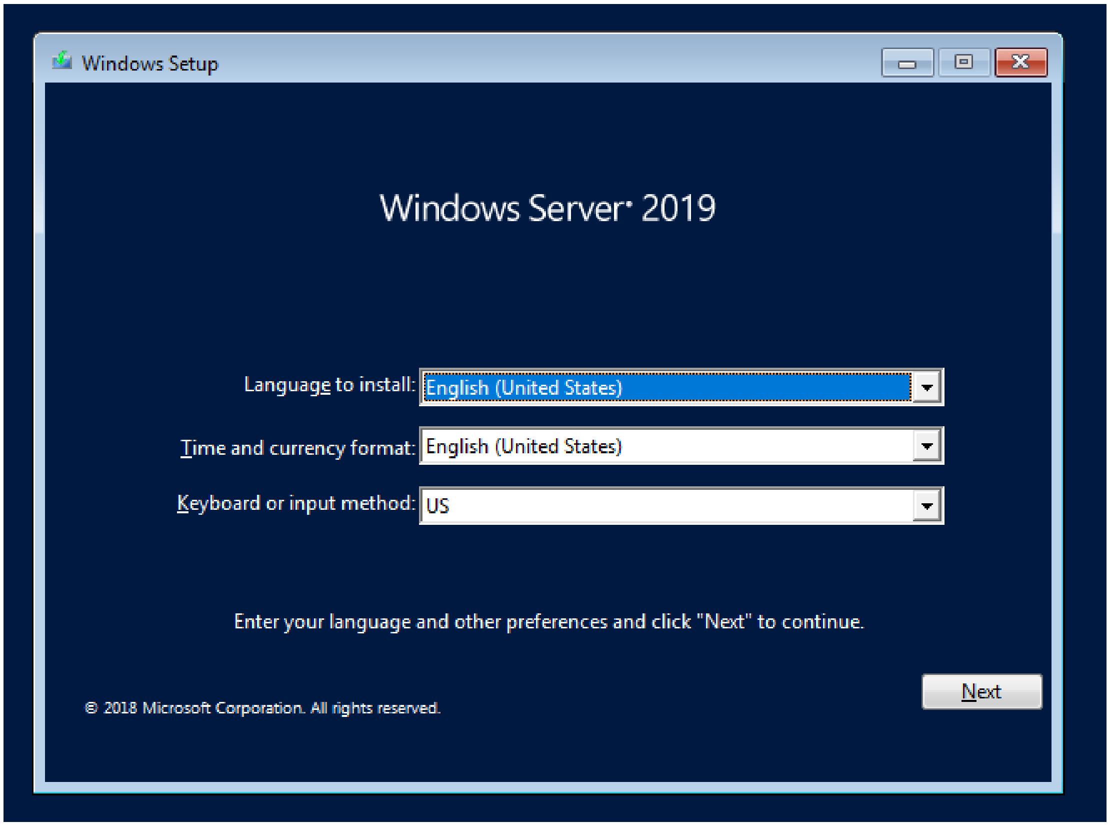
Windows Server Features	Standard	Datacenter
.NET Framework 3.5	Yes	Yes
.NET Framework 4.7	Yes	Yes
Background Intelligent Transfer Service (BITS)	Yes	Yes
BitLocker Drive Encryption	Yes	Yes
BranchCache	Yes	Yes
Client for NFS	Yes	Yes
Data Center Bridging	Yes	Yes
Enhanced Storage	Yes	Yes
Failover Clustering	Yes	Yes
Group Policy Management	Yes	Yes
Host Guardian Hyper-V Support	No	Yes
I/O Quality of Service	Yes	Yes
IIS Hostable Web Core	Yes	Yes

Windows Server Features	**Standard**	**Datacenter**
IPAM Server	Yes	Yes
iSNS Server service	Yes	Yes
Management OData IIS Extension	Yes	Yes
Media Foundation	Yes	Yes
Message Queueing	Yes	Yes
Multipath I/O	Yes	Yes
MultiPoint Connector	Yes	Yes
Network Load Balancing	Yes	Yes
Peer Name Resolution Protocol	Yes	Yes
Quality Windows Audio Video Experience	Yes	Yes
Remote Assistance	Yes, (Desktop Experience)	Yes, (Desktop Experience)
Remote Differential Compression	Yes	Yes
RSAT	Yes	Yes
RPC over HTTP Proxy	Yes	Yes
Setup and Boot Event Collection	Yes	Yes
Simple TCP/IP Services	Yes	Yes
SMB 1.0/CIFS File Sharing Support	Installed	Installed
SMB Bandwidth Limit	Yes	Yes
SMTP Server	Yes	Yes
SNMP Service	Yes	Yes
Software Load Balancer	Yes	Yes
Storage Replica	Yes	Yes
Telnet Client	Yes	Yes
TFTP Client	Yes	Yes
VM Shielding Tools for Fabric Management	Yes	Yes
WebDAV Redirector	Yes	Yes
Windows Biometric Framework	Yes	Yes
Windows Defender features	Installed	Installed
Windows Identity Foundation 3.5	Yes	Yes
Windows Internal Database	Yes	Yes
Windows PowerShell	Installed	Installed
Windows Process Activation Service	Yes	Yes
Windows Search Service	Yes	Yes
Windows Server Backup	Yes	Yes
Windows Server Migration Tools	Yes	Yes
Windows Standards-Based Storage Mgmt	Yes	Yes
WinRM IIS Extension	Yes	Yes
WINS Server	Yes	Yes
Wireless LAN Service	Yes	Yes
WoW64 support	Installed	Installed
XPS Viewer	Yes	Yes

Features available generally	**Standard**	**Datacenter**
Best Practices Analyzer	Yes	Yes
Direct Access	Yes	Yes
Dynamic Memory (in virtualization)	Yes	Yes
Hot Add/Replace RAM	Yes	Yes
Microsoft Management Console	Yes	Yes
Minimal Server Interface	Yes	Yes

Network Load Balancing	Yes	Yes
Windows PowerShell	Yes	Yes
Server Core installation option	Yes	Yes
Server Manager	Yes	Yes
SMB Direct and SMB over RDMA	Yes	Yes
Software-defined Networking	No	Yes
Storage Migration Service	Yes	Yes
Storage Replica	Yes (1 partnership and 1 resource group with a single 2TB volume)	Yes, unlimited
Storage Spaces	Yes	Yes
Storage Spaces Direct	No	Yes
Volume Activation Services	Yes	Yes
VSS (Volume Shadow Copy Service) integration	Yes	Yes
Windows Server Update Services	Yes	Yes
Windows System Resource Manager	Yes	Yes
Server license logging	Yes	Yes
Inherited activation	As guest(hosted on Datacenter)	Can be a host or a guest
Work Folders	Yes	Yes

Install Windows Server 2019



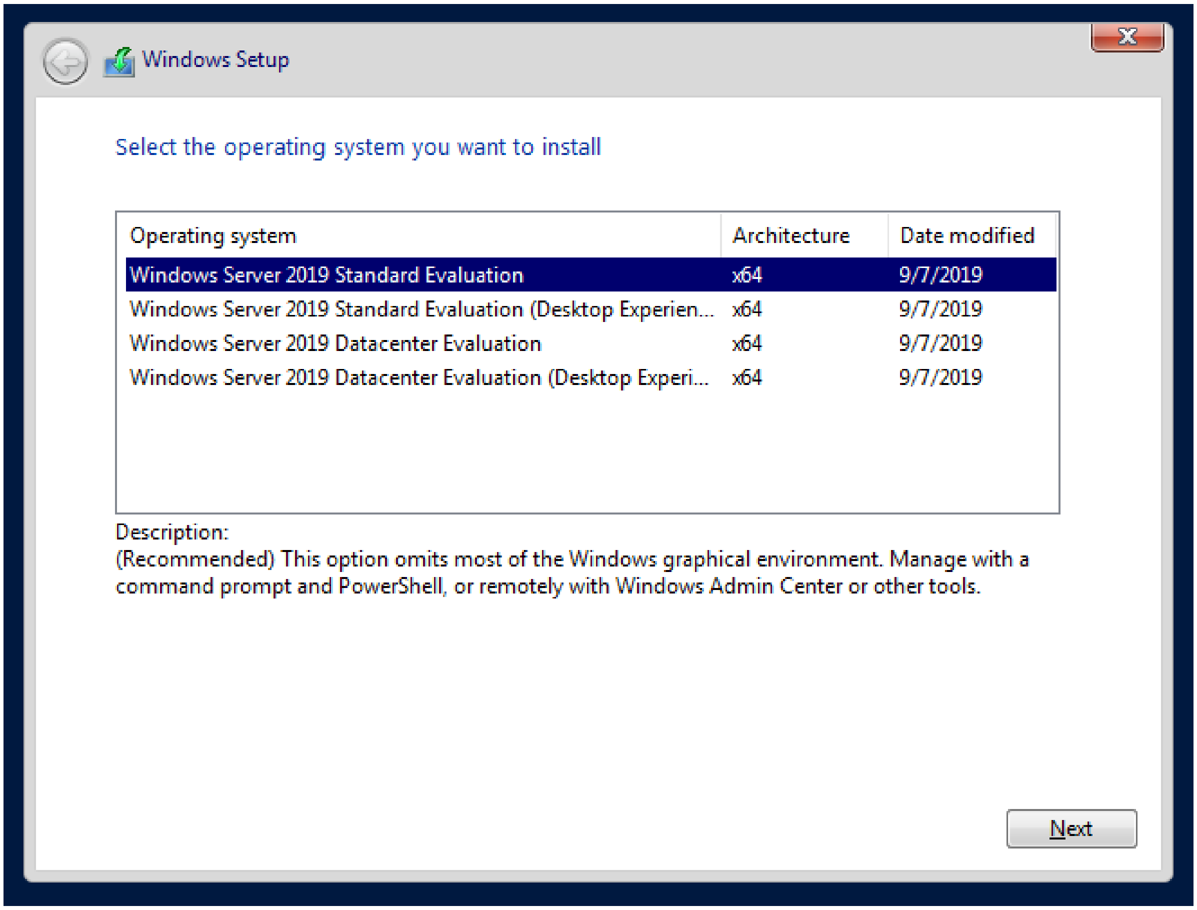
Language to install: English (United States)

Time and currency format: English (United States)

Keyboard or input method: US

Enter your language and other preferences and click "Next" to continue.

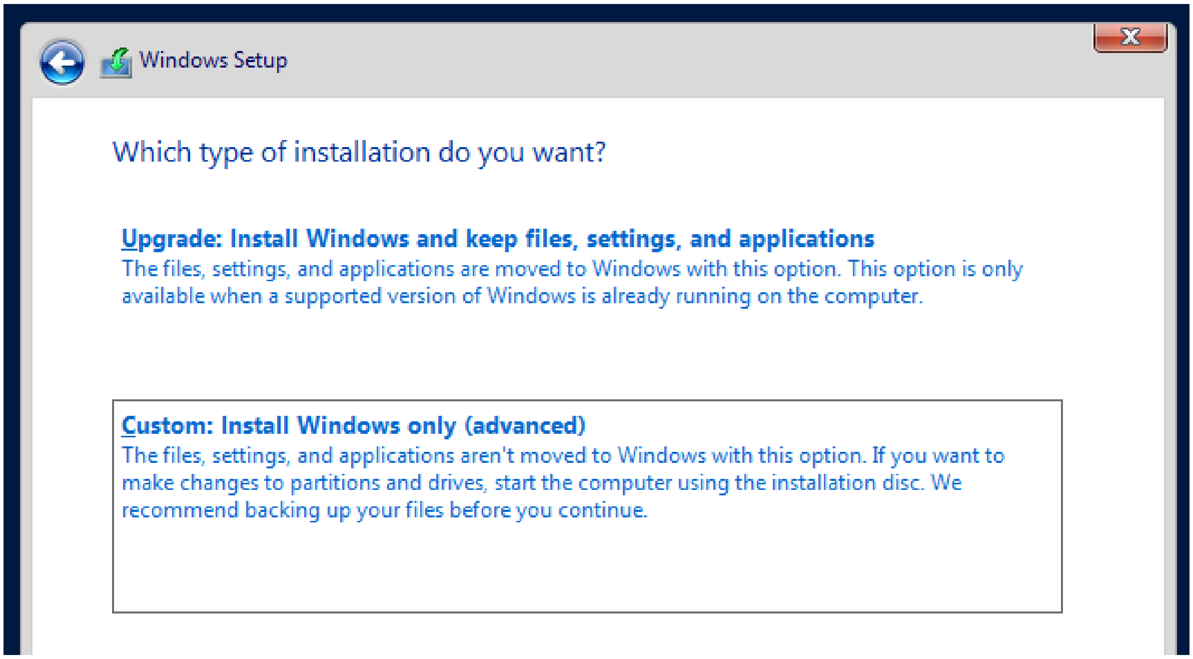
© 2018 Microsoft Corporation. All rights reserved.



Select the operating system you want to install

Operating system	Architecture	Date modified
Windows Server 2019 Standard Evaluation	x64	9/7/2019
Windows Server 2019 Standard Evaluation (Desktop Experien...	x64	9/7/2019
Windows Server 2019 Datacenter Evaluation	x64	9/7/2019
Windows Server 2019 Datacenter Evaluation (Desktop Experi...	x64	9/7/2019

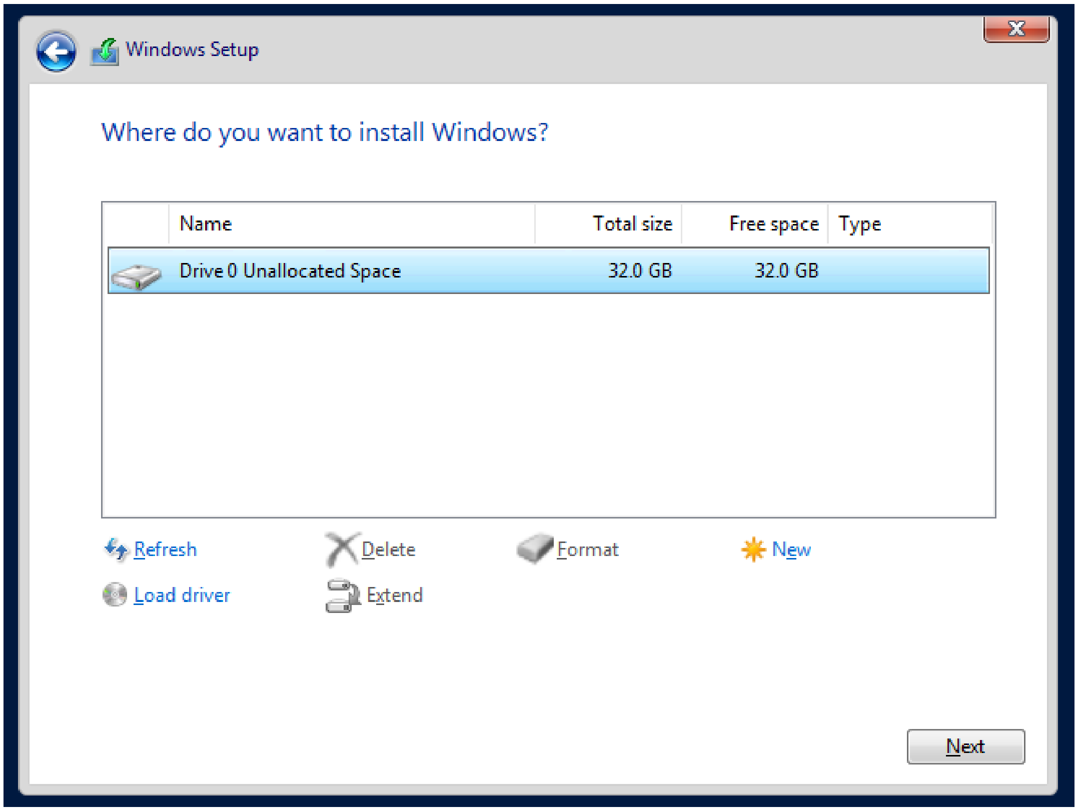
Description:
(Recommended) This option omits most of the Windows graphical environment. Manage with a command prompt and PowerShell, or remotely with Windows Admin Center or other tools.



Which type of installation do you want?

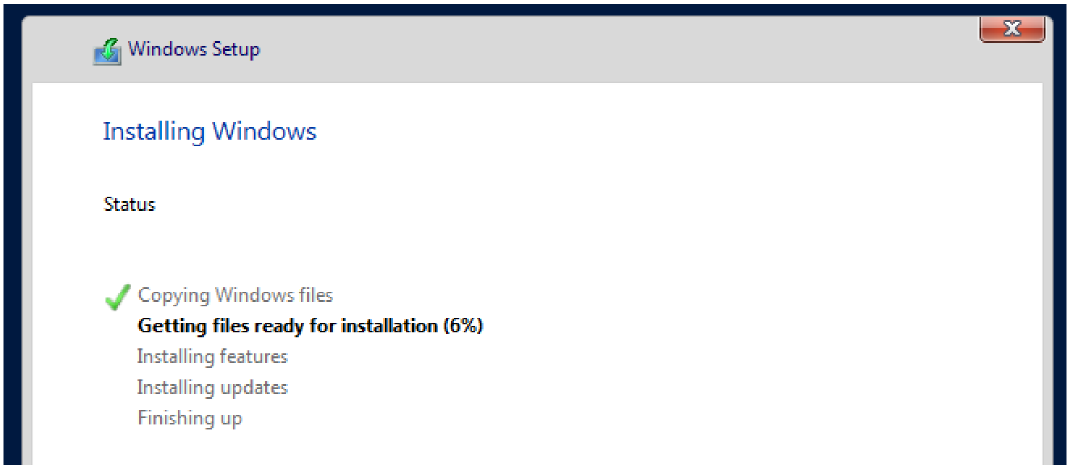
Upgrade: Install Windows and keep files, settings, and applications
The files, settings, and applications are moved to Windows with this option. This option is only available when a supported version of Windows is already running on the computer.

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.



Where do you want to install Windows?

	Name	Total size	Free space	Type
	Drive 0 Unallocated Space	32.0 GB	32.0 GB	



Installing Windows

Status

✓ Copying Windows files

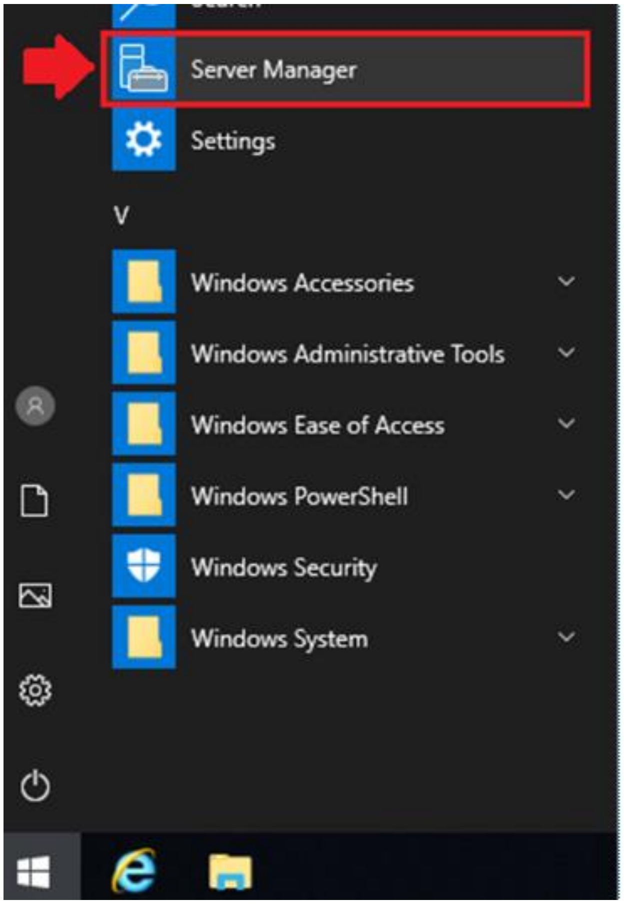
Getting files ready for installation (6%)

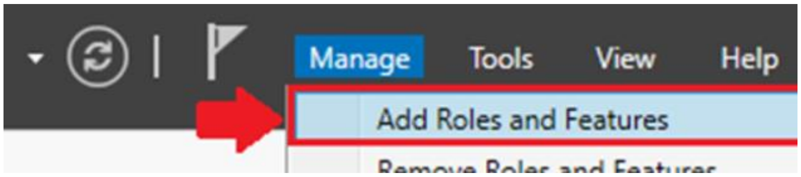
Installing features

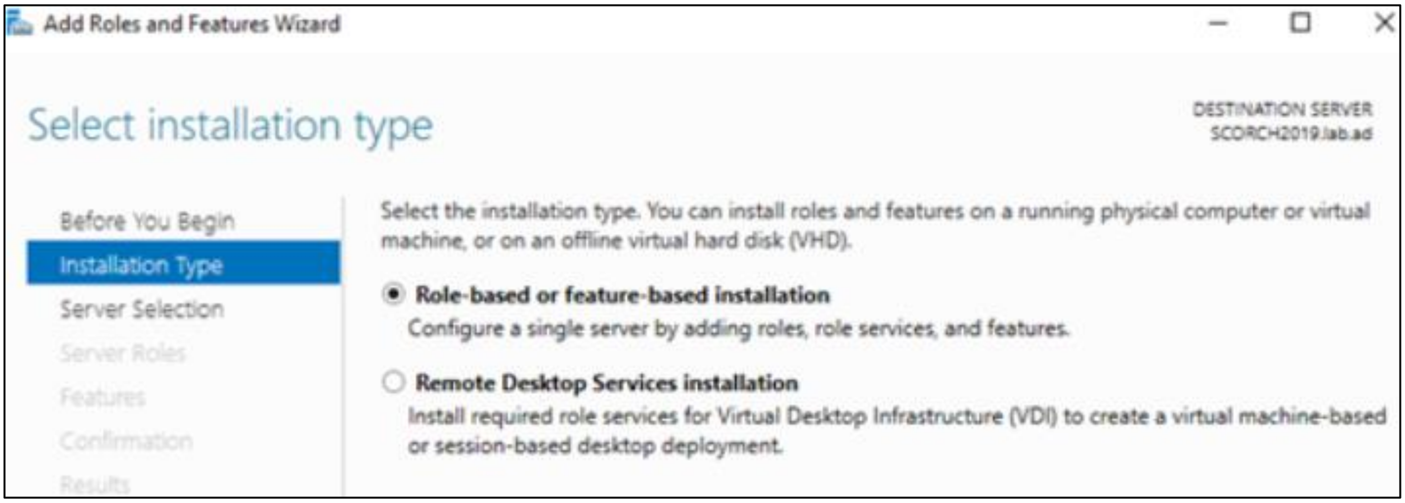
Installing updates

Finishing up

Install Windows Server 2019 features and roles







Add Roles and Features Wizard

Select installation type

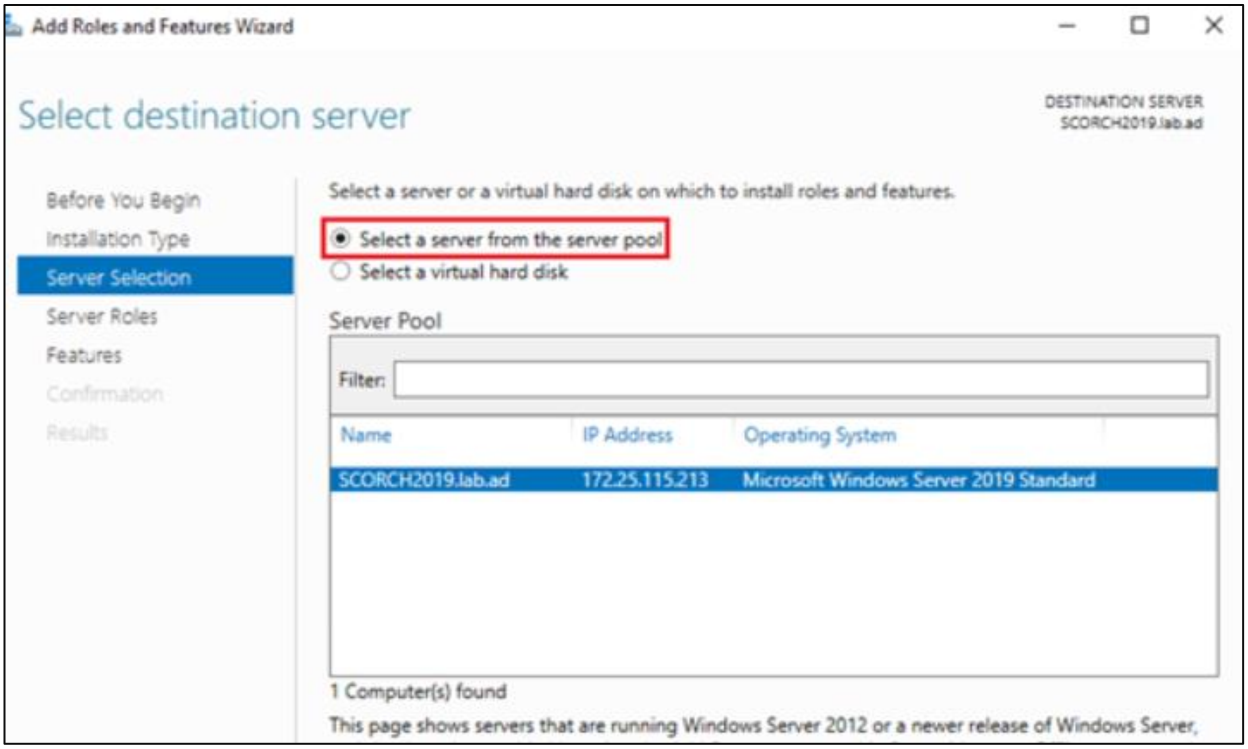
DESTINATION SERVER
SCORCH2019.lab.ad

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.



Select destination server

DESTINATION SERVER
SCORCH2019.lab.ad

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

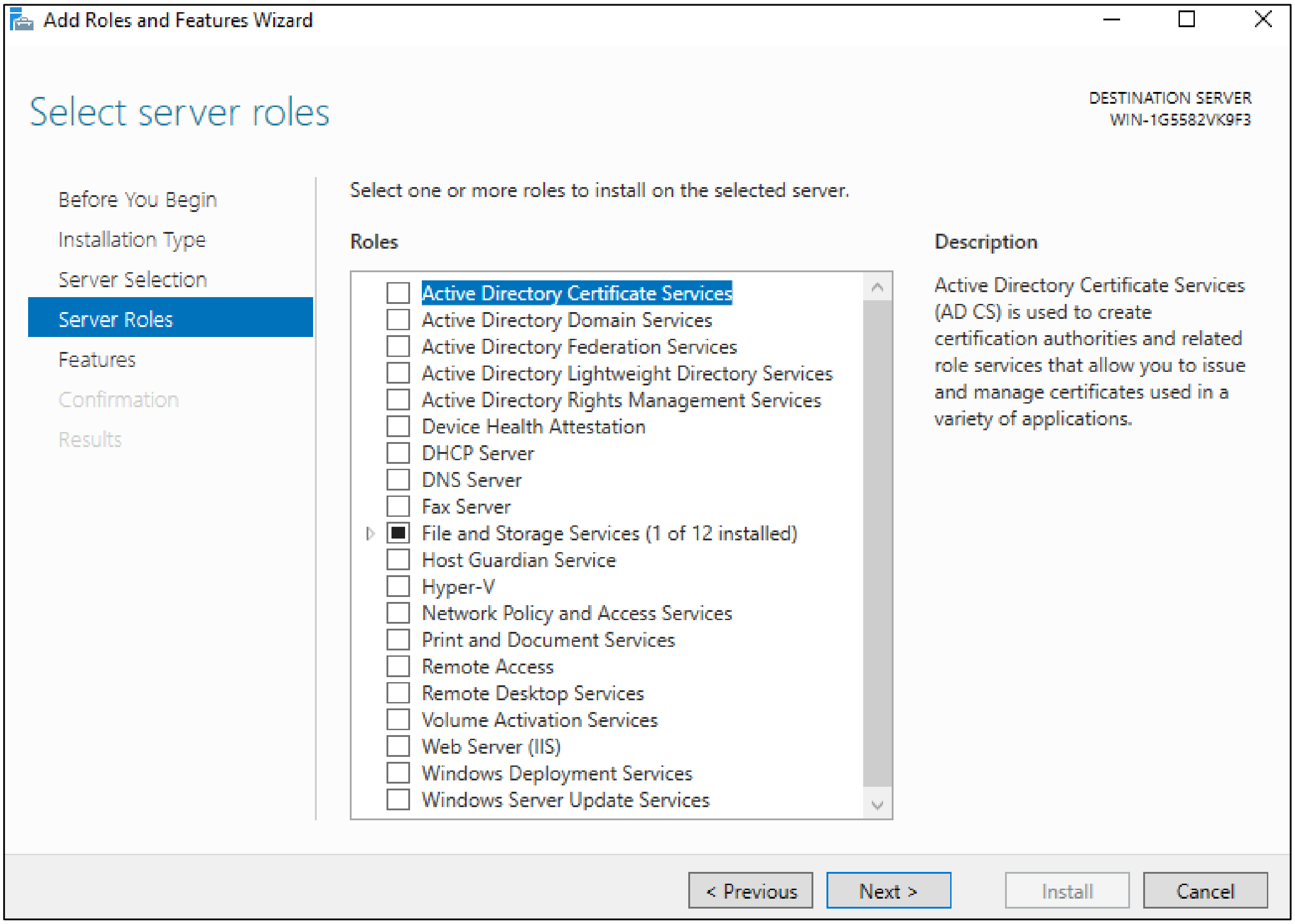
Server Pool

Filter:

Name	IP Address	Operating System
SCORCH2019.lab.ad	172.25.115.213	Microsoft Windows Server 2019 Standard

1 Computer(s) found

This page shows servers that are running Windows Server 2012 or a newer release of Windows Server,



Select server roles

DESTINATION SERVER
WIN-1G5582VK9F3

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

Roles

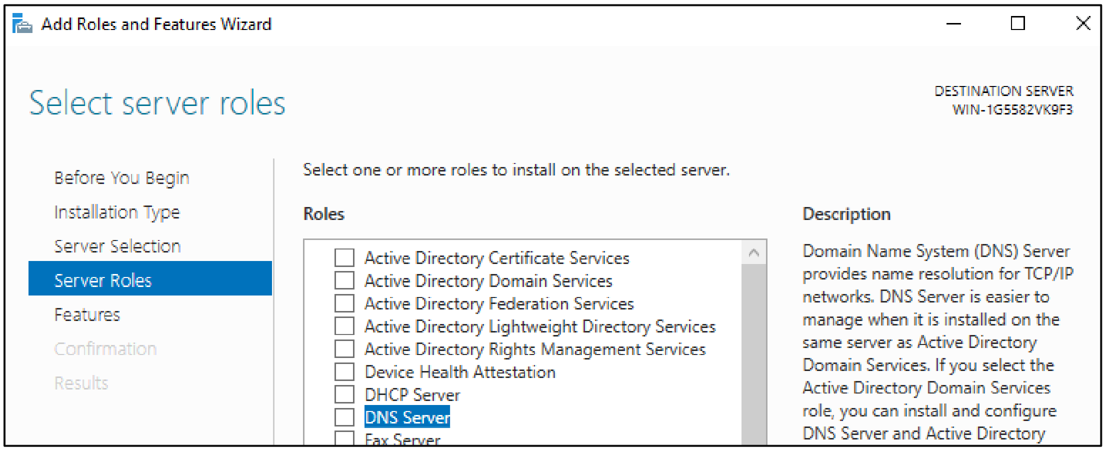
- □ Active Directory Certificate Services
- □ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Device Health Attestation
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- ■ File and Storage Services (1 of 12 installed)
- □ Host Guardian Service
- □ Hyper-V
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services
- □ Volume Activation Services
- □ Web Server (IIS)
- □ Windows Deployment Services
- □ Windows Server Update Services

Description

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

Module 2: Implement and Administrate an Active Directory Infrastructure

Installing Domain Naming Service (DNS) role



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
WIN-1G5582VK9F3

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Confirmation
- Results

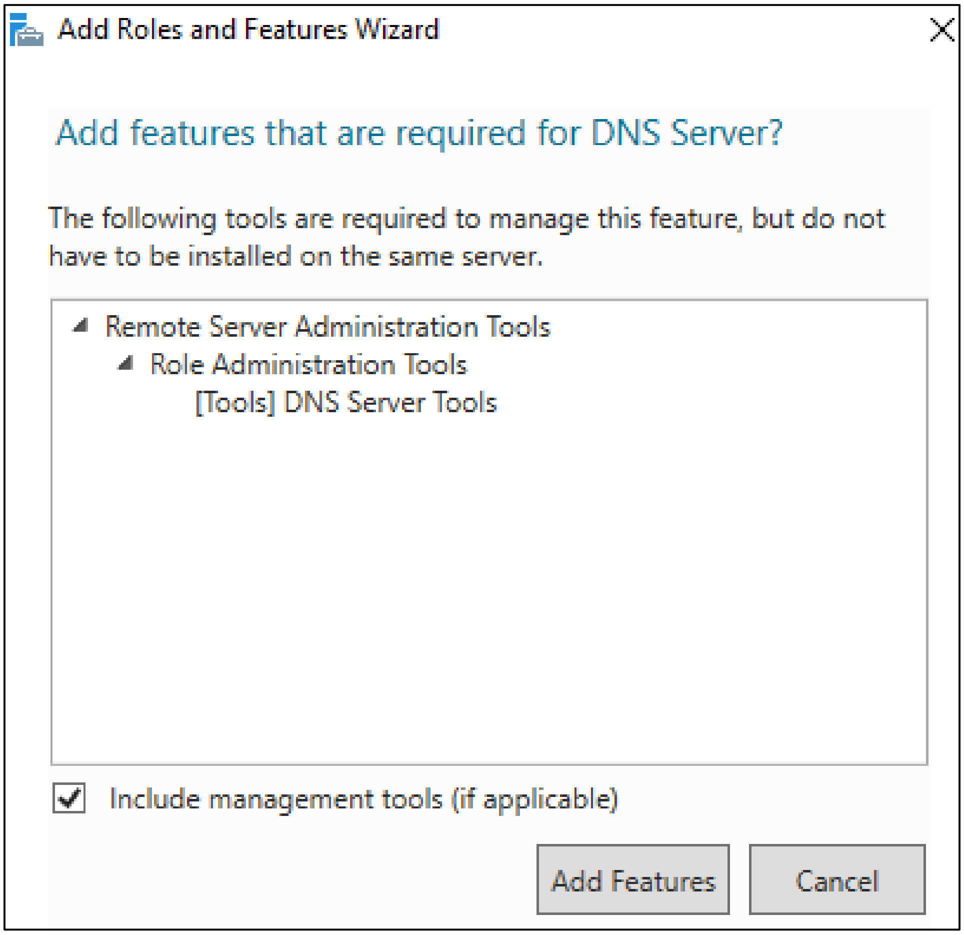
Select one or more roles to install on the selected server.

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

Description

Domain Name System (DNS) Server provides name resolution for TCP/IP networks. DNS Server is easier to manage when it is installed on the same server as Active Directory Domain Services. If you select the Active Directory Domain Services role, you can install and configure DNS Server and Active Directory



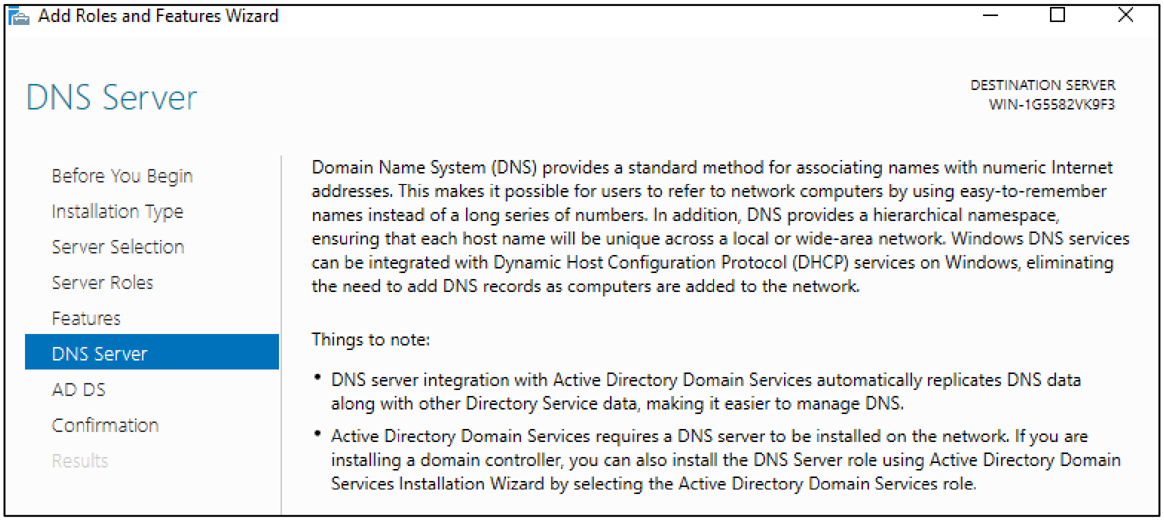
Add Roles and Features Wizard

Add features that are required for DNS 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] DNS Server Tools

☑ Include management tools (if applicable)



DNS Server

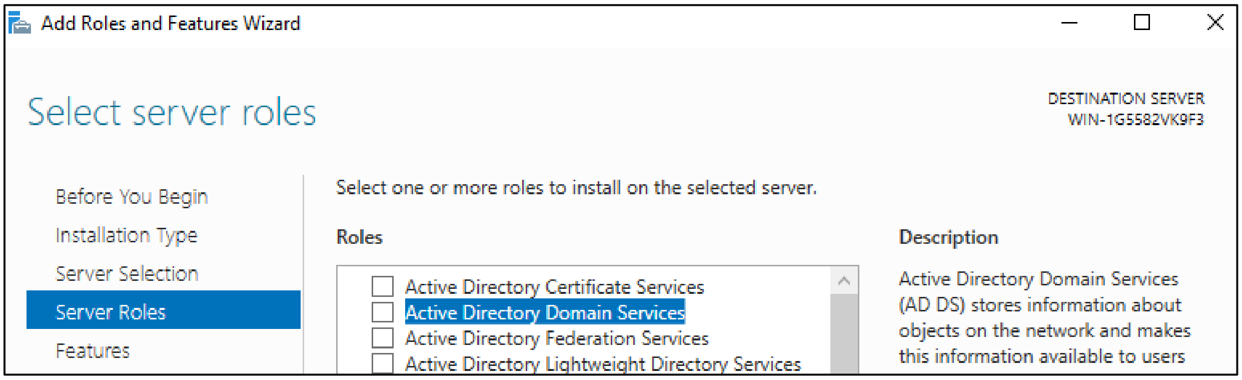
DESTINATION SERVER
WIN-1G5582VK9F3

Domain Name System (DNS) provides a standard method for associating names with numeric Internet addresses. This makes it possible for users to refer to network computers by using easy-to-remember names instead of a long series of numbers. In addition, DNS provides a hierarchical namespace, ensuring that each host name will be unique across a local or wide-area network. Windows DNS services can be integrated with Dynamic Host Configuration Protocol (DHCP) services on Windows, eliminating the need to add DNS records as computers are added to the network.

Things to note:

- DNS server integration with Active Directory Domain Services automatically replicates DNS data along with other Directory Service data, making it easier to manage DNS.
- Active Directory Domain Services requires a DNS server to be installed on the network. If you are installing a domain controller, you can also install the DNS Server role using Active Directory Domain Services Installation Wizard by selecting the Active Directory Domain Services role.

Installing Active Directory Domain Services role



Select server roles

DESTINATION SERVER
WIN-1G5582VK9F3

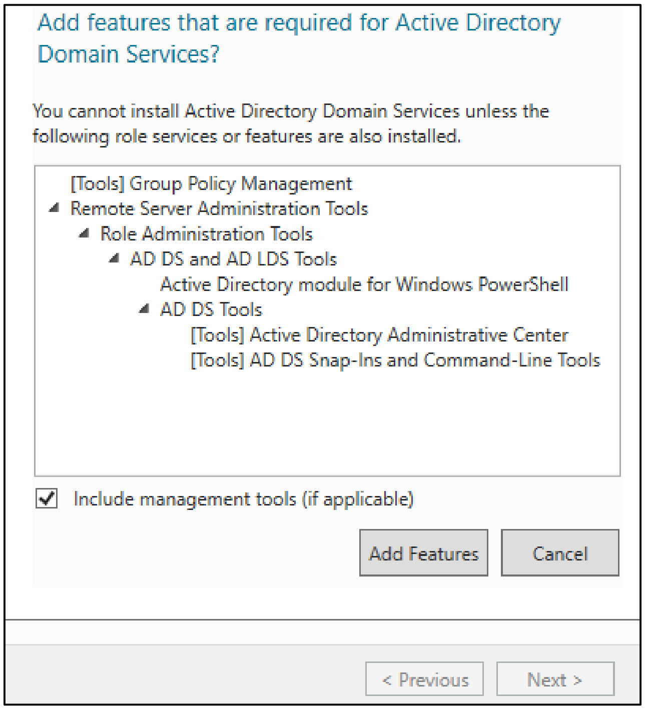
Select one or more roles to install on the selected server.

Roles

- ☐ Active Directory Certificate Services
- ☐ Active Directory Domain Services
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services

Description

Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users

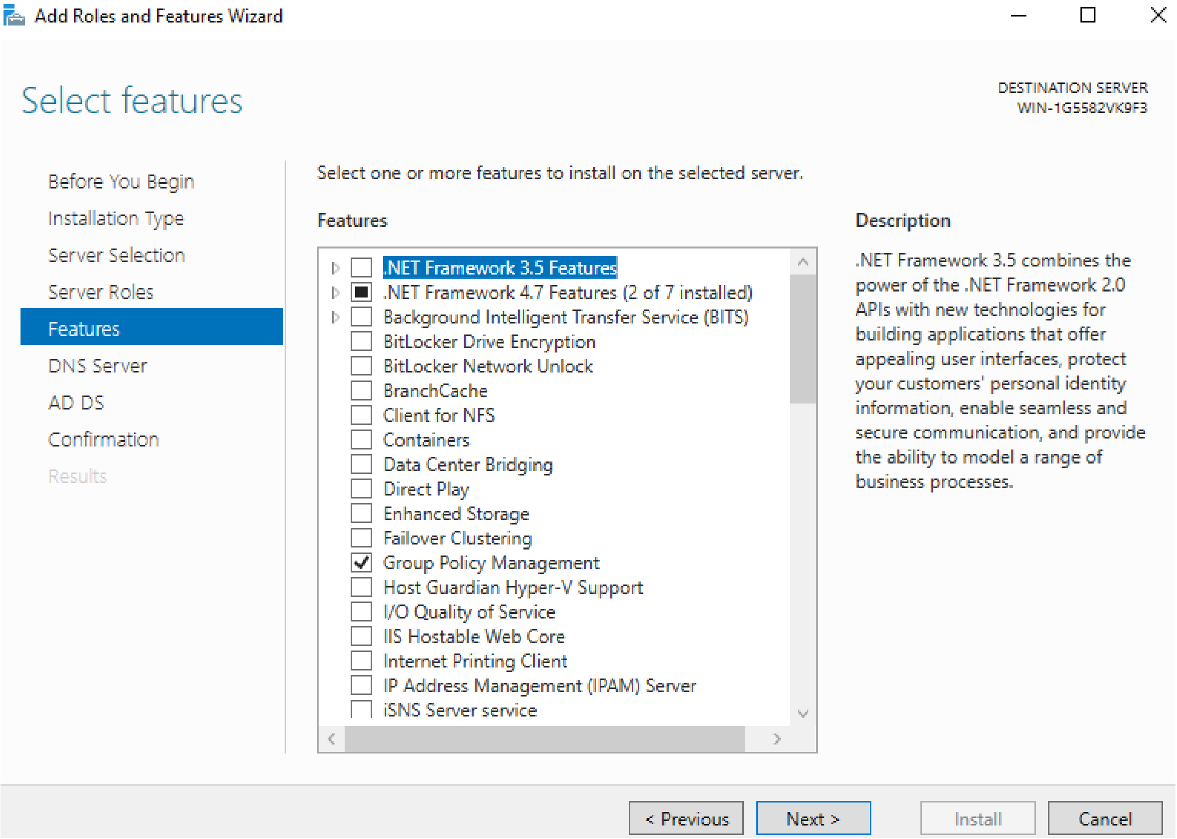

Add features that are required for Active Directory Domain Services?

You cannot install Active Directory Domain Services unless the following role services or features are also installed.

```
   [Tools] Group Policy Management
◢ Remote Server Administration Tools
    ◢ Role Administration Tools
        ◢ AD DS and AD LDS Tools
              Active Directory module for Windows PowerShell
            ◢ AD DS Tools
                  [Tools] Active Directory Administrative Center
                  [Tools] AD DS Snap-Ins and Command-Line Tools
```

☑ Include management tools (if applicable)

On the select features section, skip this part as the features needed had already been added from the previous screen.



Select features

DESTINATION SERVER
WIN-1G5582VK9F3

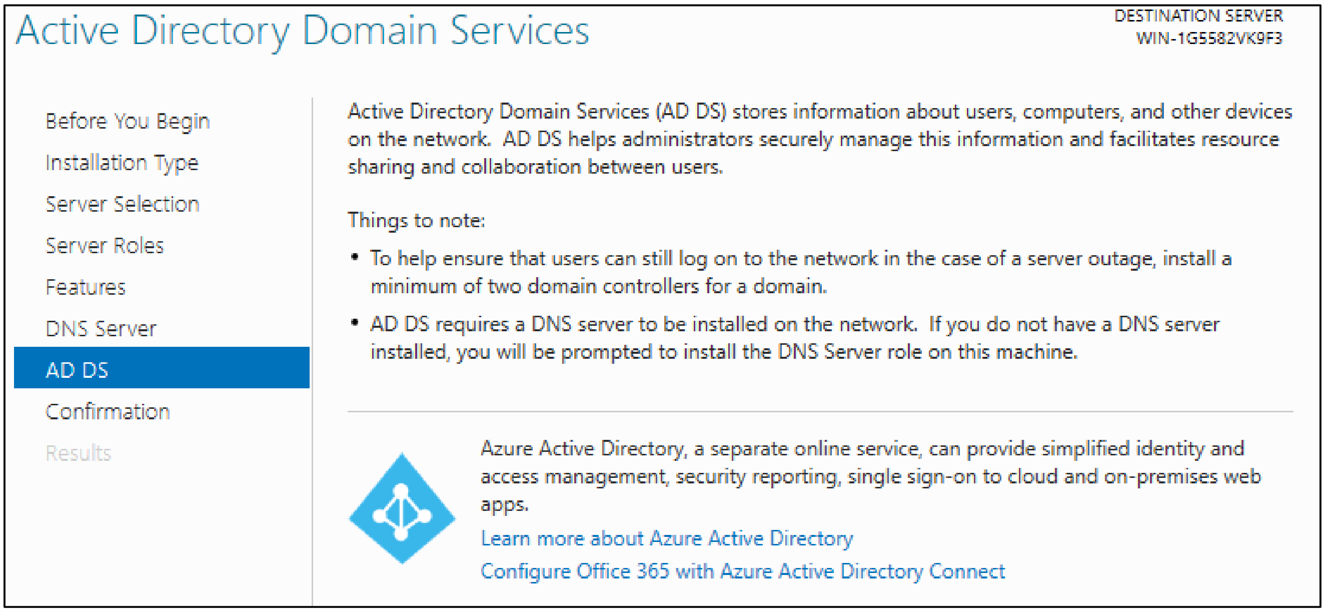
Select one or more features to install on the selected server.

Features

- □ .NET Framework 3.5 Features
- ■ .NET Framework 4.7 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.



Active Directory Domain Services

DESTINATION SERVER
WIN-1G5582VK9F3

Active Directory Domain Services (AD DS) stores information about users, computers, and other devices on the network. AD DS helps administrators securely manage this information and facilitates resource sharing and collaboration between users.

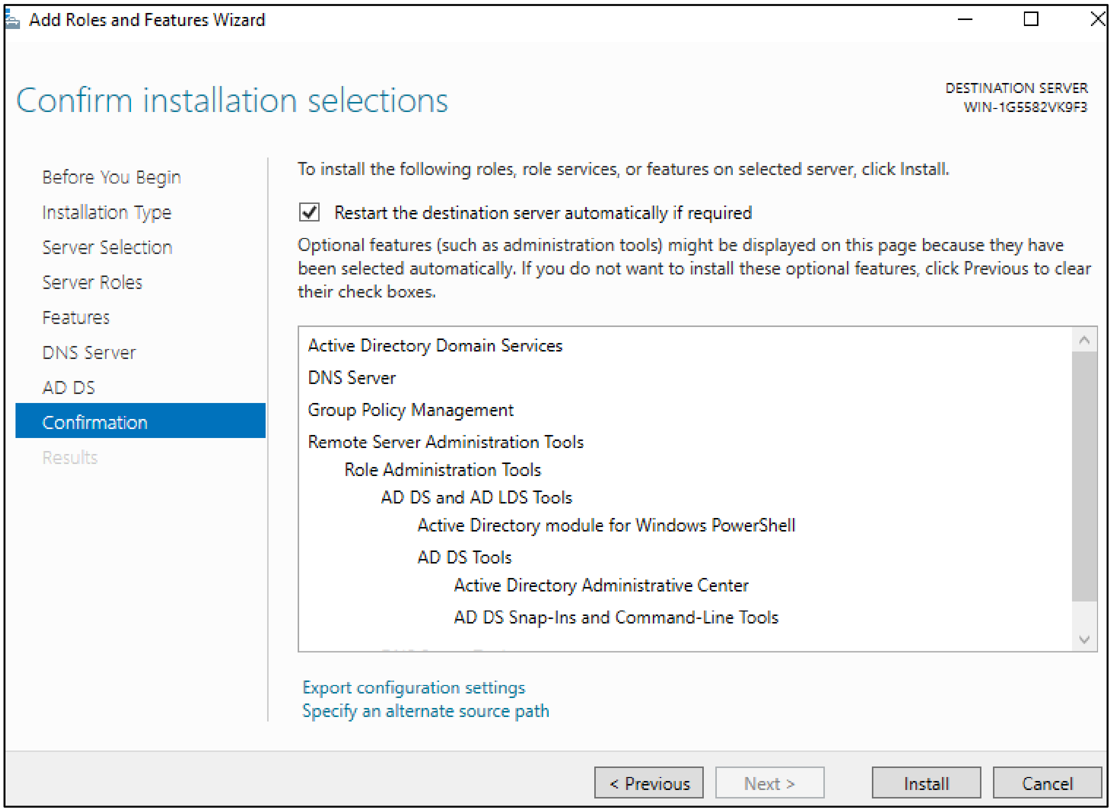
Things to note:

- To help ensure that users can still log on to the network in the case of a server outage, install a minimum of two domain controllers for a domain.
- AD DS requires a DNS server to be installed on the network. If you do not have a DNS server installed, you will be prompted to install the DNS Server role on this machine.

Azure Active Directory, a separate online service, can provide simplified identity and access management, security reporting, single sign-on to cloud and on-premises web apps.

Learn more about Azure Active Directory

Configure Office 365 with Azure Active Directory Connect



Confirm installation selections

DESTINATION SERVER
WIN-1G5582VK9F3

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.

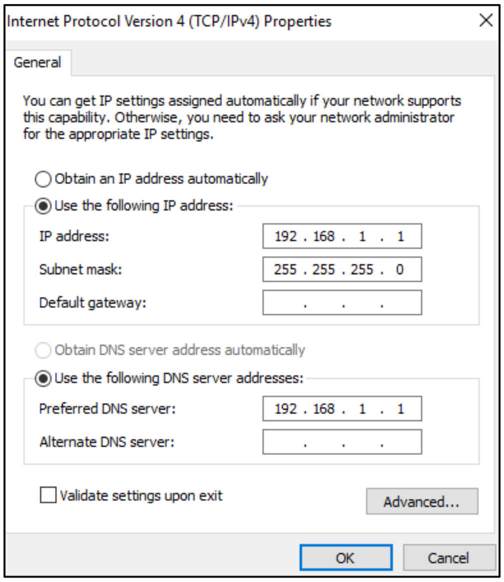
Active Directory Domain Services
DNS Server
Group Policy Management
Remote Server Administration Tools
    Role Administration Tools
        AD DS and AD LDS Tools
            Active Directory module for Windows PowerShell
            AD DS Tools
                Active Directory Administrative Center
                AD DS Snap-Ins and Command-Line Tools

Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel

Promoting a Domain Controller

1. Provide a distinguishable computer name for your server via the system properties. Reboot for the computer name to properly take effect.
2. Correct or set your time zone.
3. It is recommended to provide a static IP address to the active network interface of your server. The primary DNS address should be pointing to your DNS Server (if the DNS Server is installed on the same server as the one you will be promoting as a domain controller, you may use the loopback address 127.0.0.1, or statically point to its own IP)

   Ex:



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

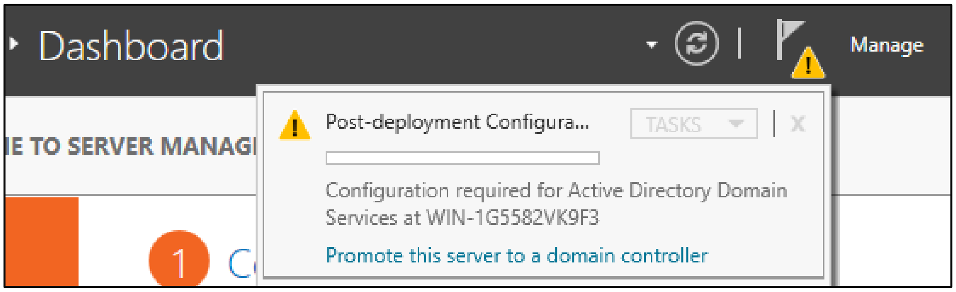
IP address: 192 . 168 . 1 . 1
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 1 . 1
Alternate DNS server: . . .

□ Validate settings upon exit

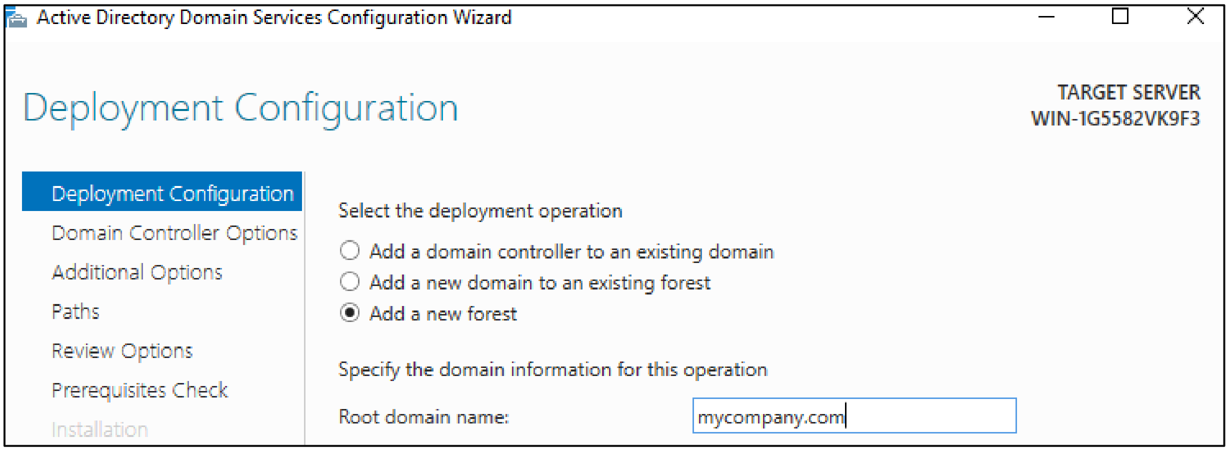
4. The active directory domain services role must then be installed.
5. In the server manager:



Post-deployment Configura...

Configuration required for Active Directory Domain Services at WIN-1G5582VK9F3

Promote this server to a domain controller



Deployment Configuration

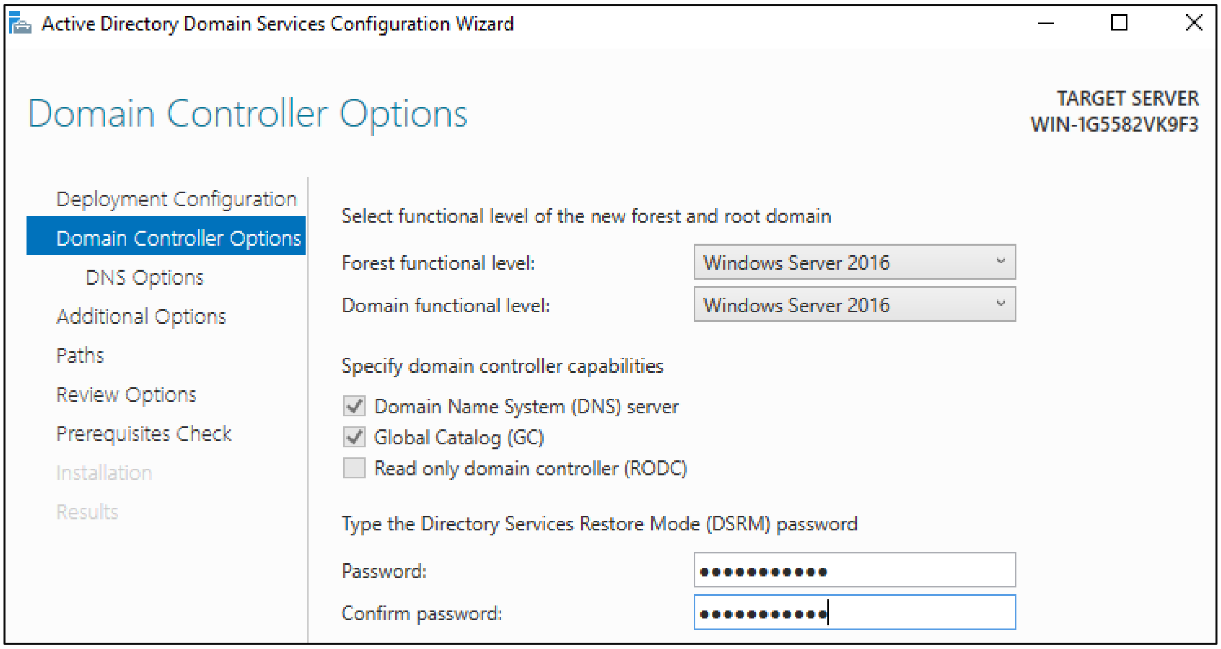
TARGET SERVER
WIN-1G5582VK9F3

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

Root domain name: mycompany.com



Domain Controller Options

TARGET SERVER
WIN-1G5582VK9F3

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2016

Domain functional level: Windows Server 2016

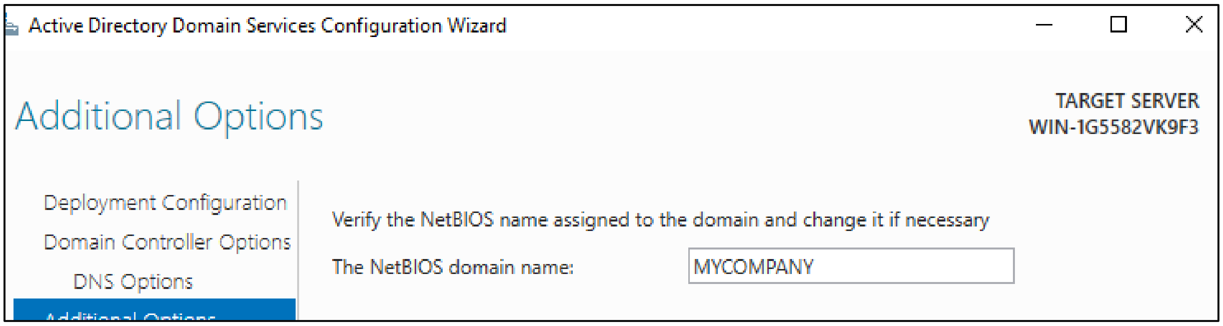
Specify domain controller capabilities

☑ Domain Name System (DNS) server
☑ Global Catalog (GC)
☐ Read only domain controller (RODC)

Type the Directory Services Restore Mode (DSRM) password

Password: ●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●

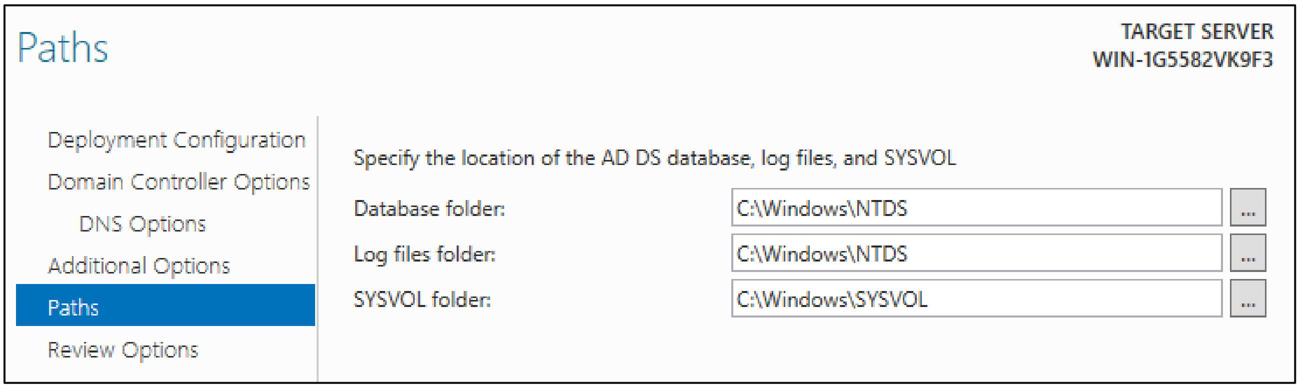

Active Directory Domain Services Configuration Wizard
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options

Additional Options

TARGET SERVER
WIN-1G5582VK9F3

Verify the NetBIOS name assigned to the domain and change it if necessary

The NetBIOS domain name: MYCOMPANY



Paths

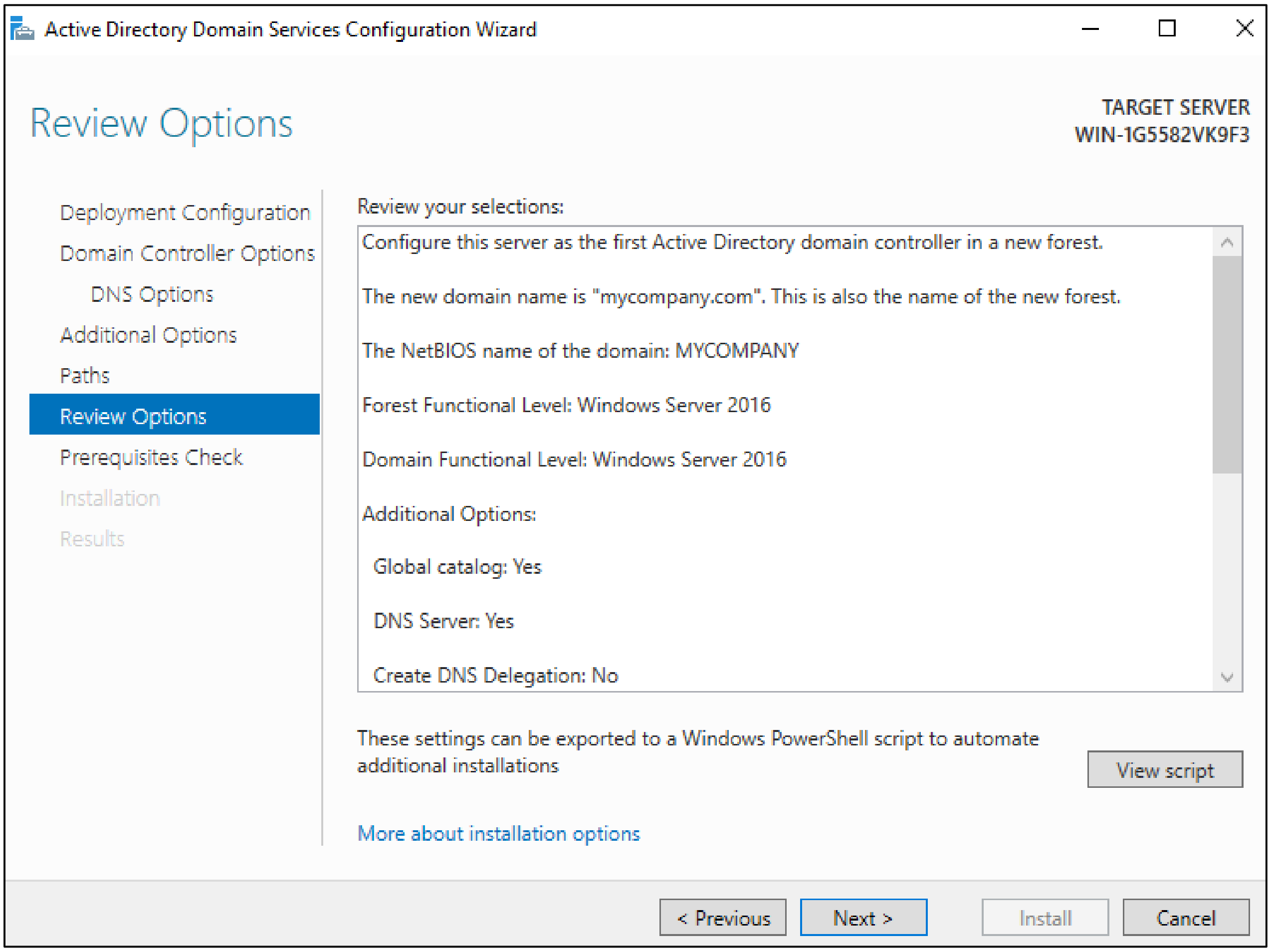
TARGET SERVER
WIN-1G5582VK9F3

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



Review Options

TARGET SERVER
WIN-1G5582VK9F3

Review your selections:

Configure this server as the first Active Directory domain controller in a new forest.

The new domain name is "mycompany.com". This is also the name of the new forest.

The NetBIOS name of the domain: MYCOMPANY

Forest Functional Level: Windows Server 2016

Domain Functional Level: Windows Server 2016

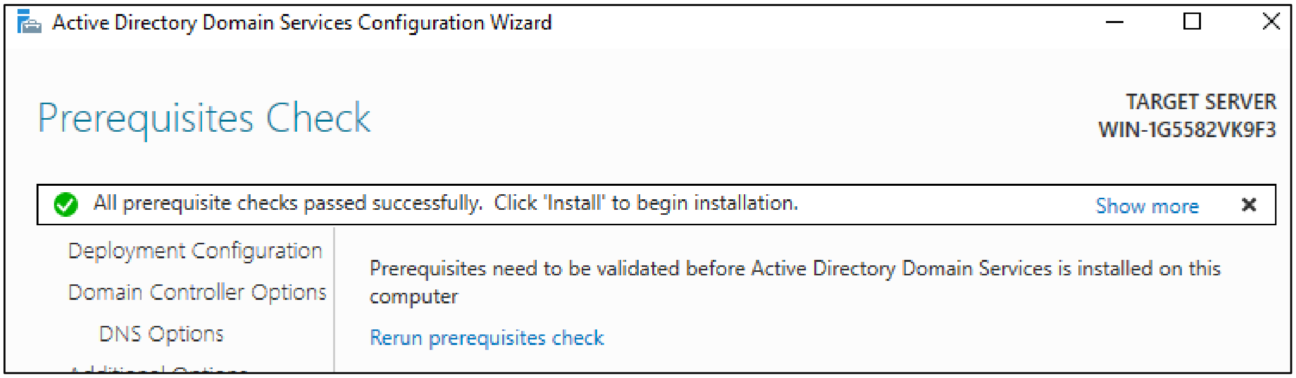
Additional Options:

Global catalog: Yes

DNS Server: Yes

Create DNS Delegation: No

These settings can be exported to a Windows PowerShell script to automate additional installations



Active Directory Domain Services Configuration Wizard

Prerequisites Check

TARGET SERVER
WIN-1G5582VK9F3

All prerequisite checks passed successfully. Click 'Install' to begin installation.

Prerequisites need to be validated before Active Directory Domain Services is installed on this computer

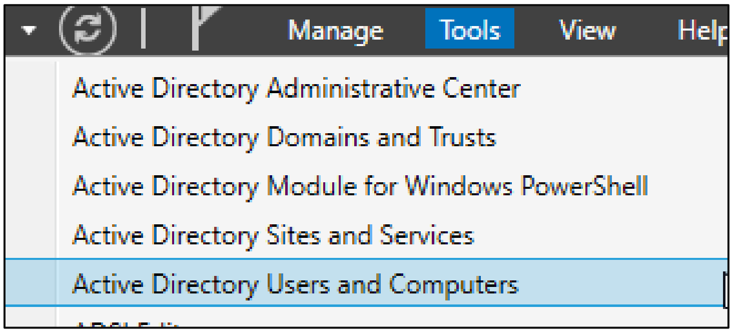
Setting up additional Domain Controllers

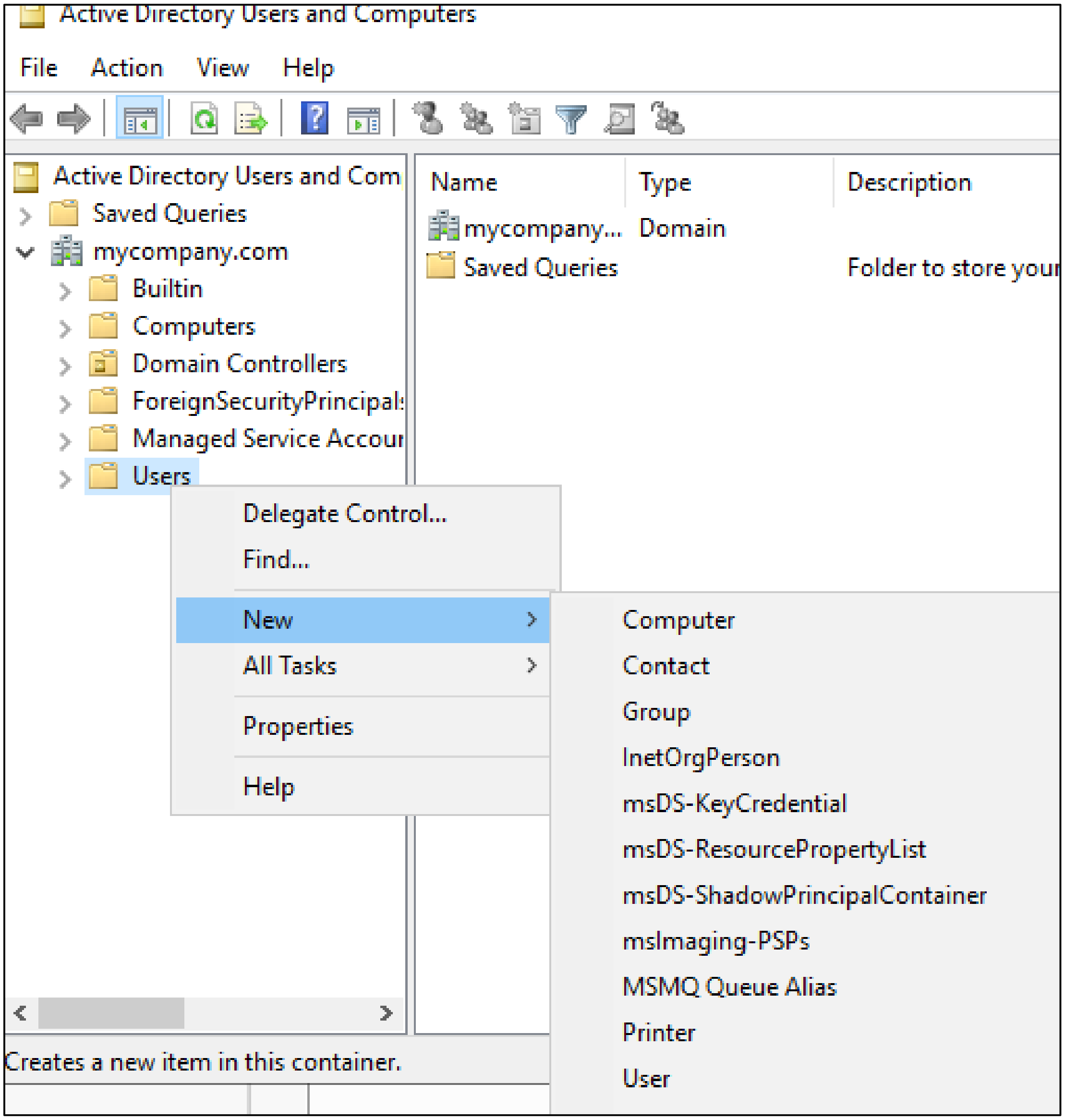
- Initial configuration tasks
  a. (change admin password) **net user administrator ***
  b. (set static ipv4 configuration) **netsh interface ipv4**
  c. (join a domain) **netdom**
  d. (install optional components -role, feature, service, etc.) **Ocsetup <package>**
  e. (display installed- role, feature, service, etc) **Oclist**
  f. (enable remote desktop) **Cscript c:\windows\system32\scregedit.wsf /AR 0**
  g. (promote a domain controller) **dcpromo**
  h. (dcpromo /? Or dcpromo /?:promotion)
  i. (configure DNS) **dnscmd**
- Using server configuration **(sconfig)**
- Activity
  a. Rename server using **netdom rename computer %computername% /newname:server2** or **sconfig**
  b. Set ipv4 address and dns using
     - **Netsh interface ipv4 set address name=”Local Area Connection” source=static address=192.168.5.22 mask=255.255.255.0 gateway=192.168.5.1 1**
     - **Netsh interface ipv4 set dnsserver name=”Local Area Connection” source=static address=192.168.5.20 primary**
     - **Or by using sconfig**
  c. Verify ip **ipconfig**
  d. Restart by **shutdown /r /t 0**
  e. *Join the domain **netdom join %computername% /domain:contoso.com**
  f. *Restart by **shutdown /r /t 0**
  g. Promote

     dcpromo /unattend
     /replicaOrNewDomain:replica
     /replicationDomainDNSName:contoso.com
     /ConfirmGC:yes
     /UserName:Administrator
     /userDomain:Contoso
     /Password:*
     /safeModeAdminPassword:restore$123
  h. To remove a domain controller

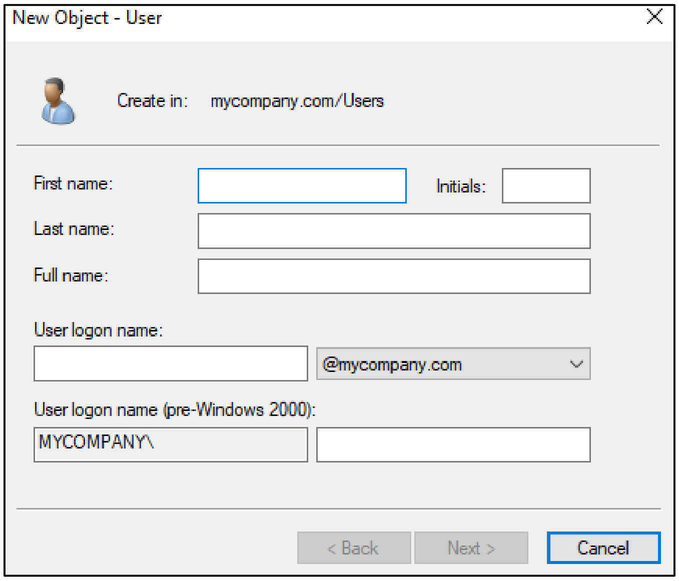
     Dcpromo /unattend /AdministratorPassword:password$123

Creating users using AD Users and Computers Tool


Manage
Tools
View
Help
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers



Creates a new item in this container.



New Object - User

Create in: mycompany.com/Users

First name: Initials:

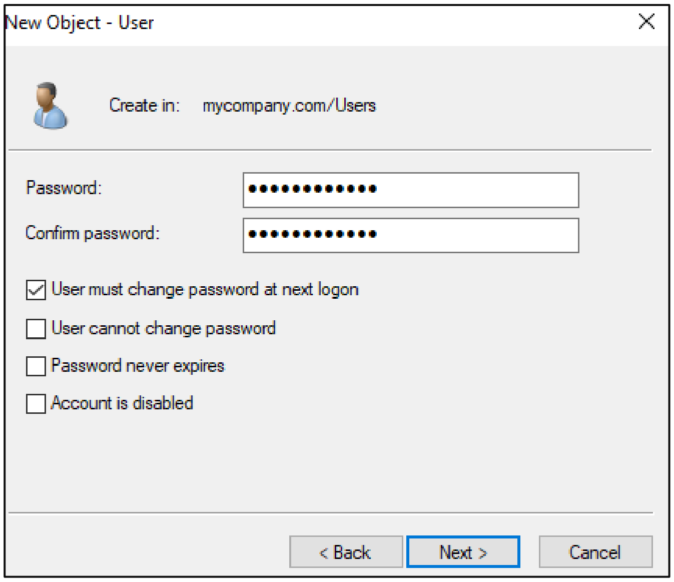
Last name:

Full name:

User logon name: @mycompany.com

User logon name (pre-Windows 2000): MYCOMPANY\

< Back | Next > | Cancel



New Object - User

Create in: mycompany.com/Users

Password: ••••••••••••

Confirm password: ••••••••••••

☑ User must change password at next logon

□ User cannot change password

□ Password never expires

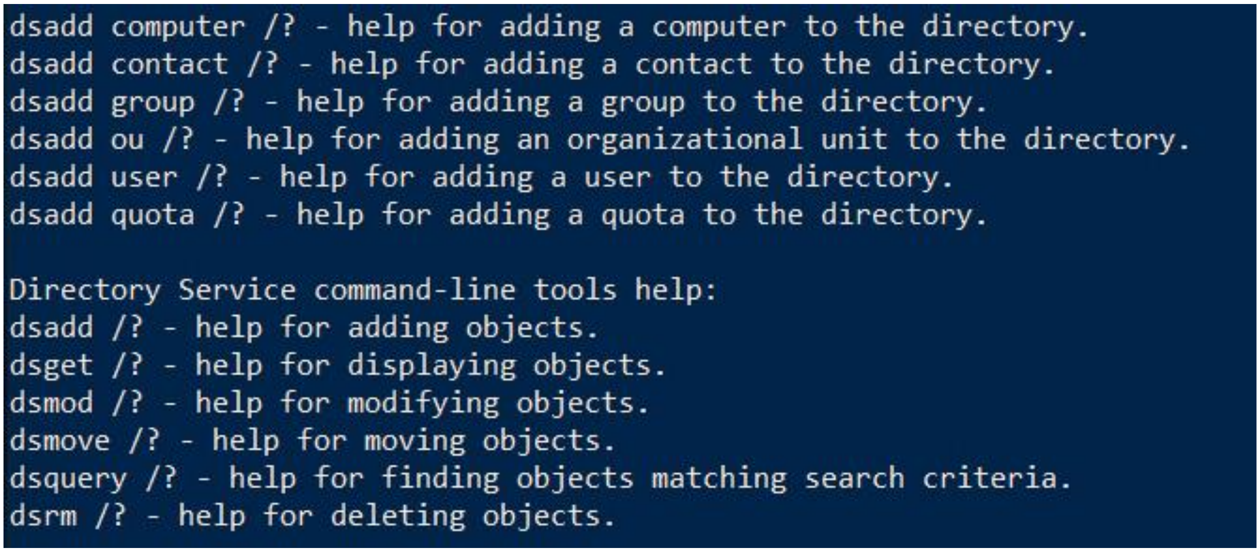
□ Account is disabled

< Back | Next > | Cancel

Creating users using Powershell and Command-Line Tools

1. Using the “ds” command line tool

   \> dsadd user “CN=user2,CN=Users,DC=mycompany,DC=com” -pwd {<password>|*} -disabled {yes|no}



```
dsadd computer /? - help for adding a computer to the directory.
dsadd contact /? - help for adding a contact to the directory.
dsadd group /? - help for adding a group to the directory.
dsadd ou /? - help for adding an organizational unit to the directory.
dsadd user /? - help for adding a user to the directory.
dsadd quota /? - help for adding a quota to the directory.

Directory Service command-line tools help:
dsadd /? - help for adding objects.
dsget /? - help for displaying objects.
dsmod /? - help for modifying objects.
dsmove /? - help for moving objects.
dsquery /? - help for finding objects matching search criteria.
dsrm /? - help for deleting objects.
```

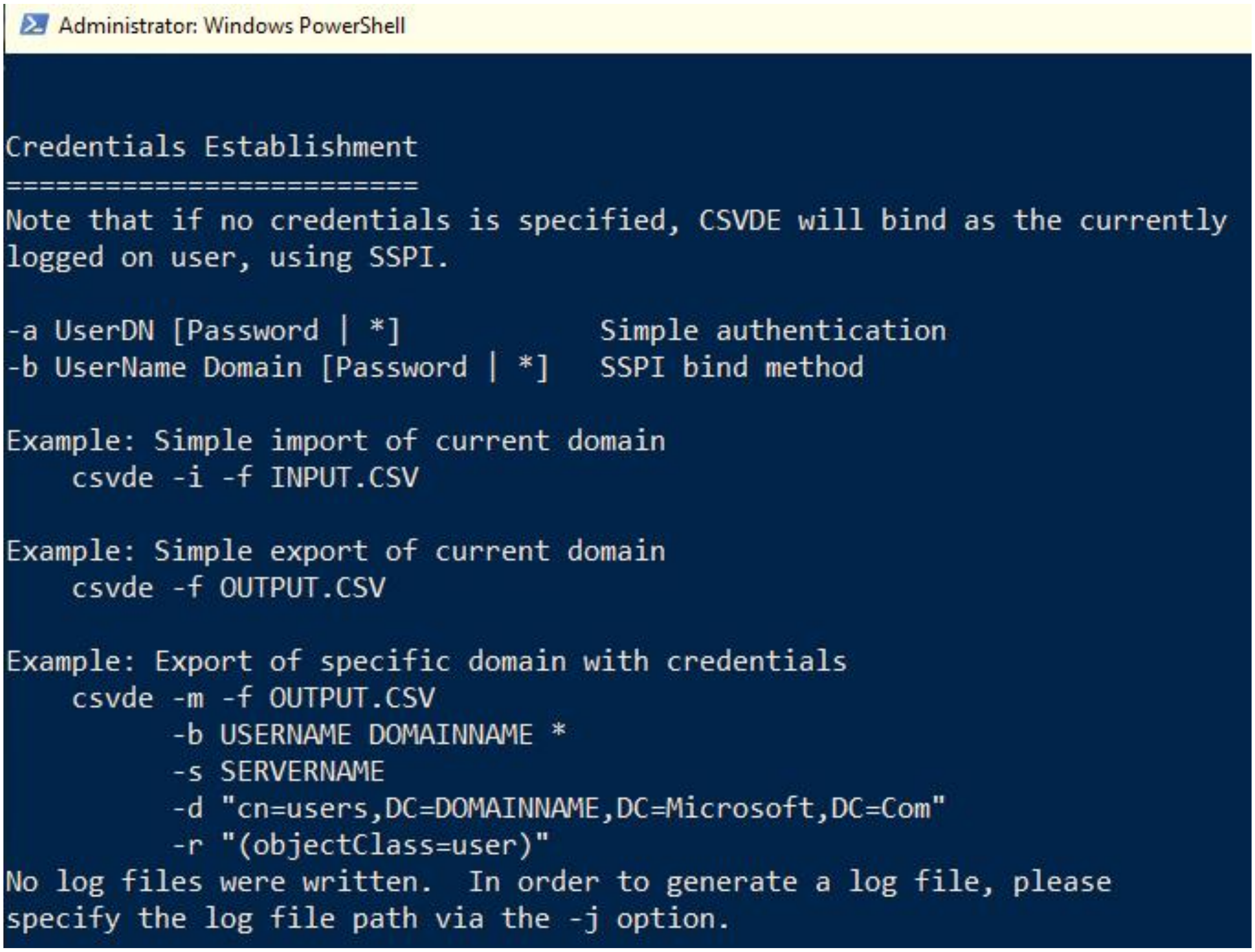
2. Using “csvde” to import/export users from/to a csv file

   Export objects in a container
   \> csvde -f c:\users.csv -d “cn=users,dc=mycompany,dc=com”

   Import objects from csvde
   \>csvde -i -f c:\newusers.csv

[newusers.csv]

```
objectClass,dn,sAMAccountName,userPrincipalName
user,”cn=user20,cn=Users,dc=contoso,dc=com”,user20,user20@mycompany.com
user,”cn=user21,ou=marketing,dc=contoso,dc=com”,user21,user21@mycompany.com
```



```
Credentials Establishment
=========================
Note that if no credentials is specified, CSVDE will bind as the currently
logged on user, using SSPI.

-a UserDN [Password | *]            Simple authentication
-b UserName Domain [Password | *]   SSPI bind method

Example: Simple import of current domain
    csvde -i -f INPUT.CSV

Example: Simple export of current domain
    csvde -f OUTPUT.CSV

Example: Export of specific domain with credentials
    csvde -m -f OUTPUT.CSV
          -b USERNAME DOMAINNAME *
          -s SERVERNAME
          -d "cn=users,DC=DOMAINNAME,DC=Microsoft,DC=Com"
          -r "(objectClass=user)"
No log files were written.  In order to generate a log file, please
specify the log file path via the -j option.
```

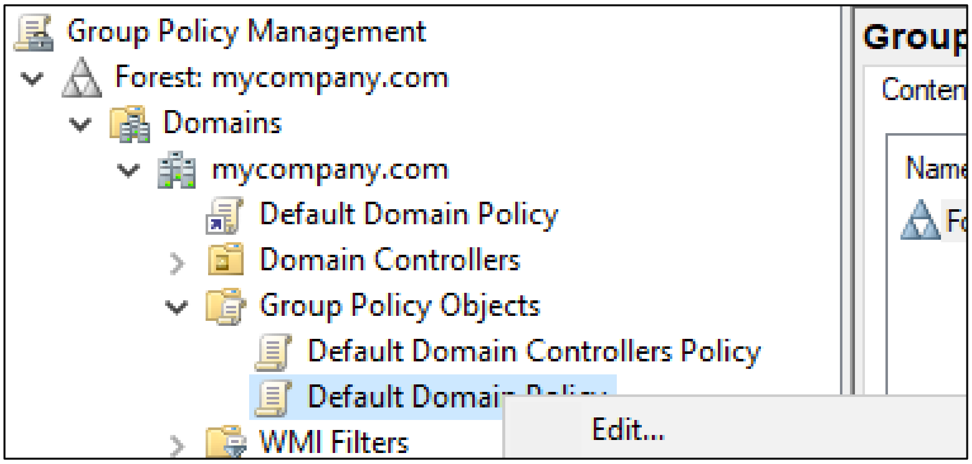
3. Using powershell

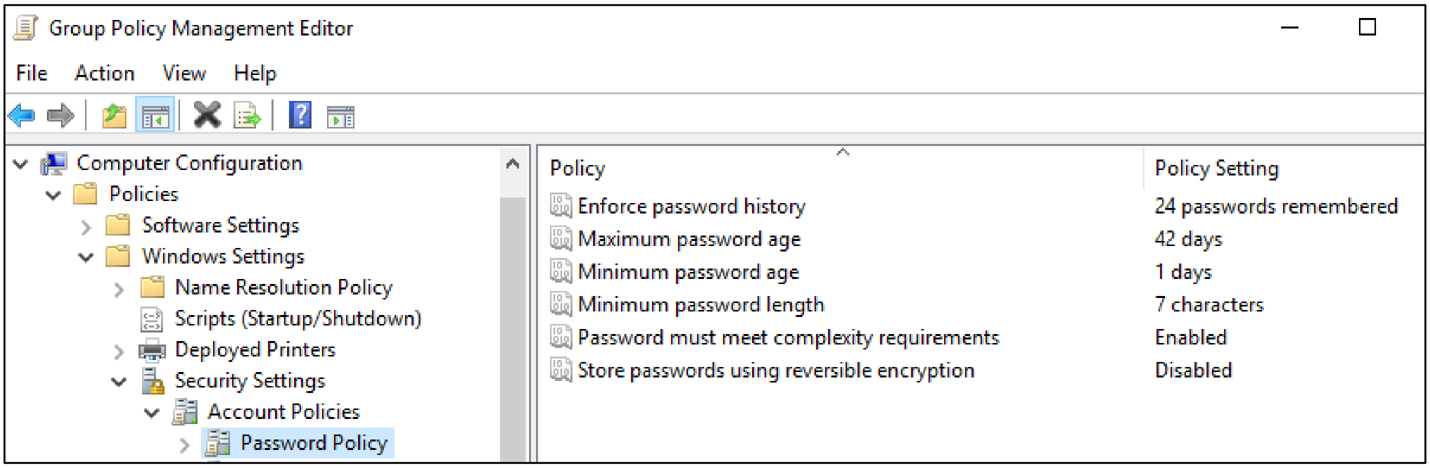
```
PS\> Import-Module ActiveDirectory
PS\> Get-Command New-ADUser –Syntax
PS\> New-AdUser “user5”
PS\> Get-ADUser -Filter * -Properties samAccountName | select samAccountName
```

```
PS\> New-ADUser -Name "Jack Robinson" -GivenName "Jack" -Surname "Robinson" -SamAccountName "J.Robinson" -
UserPrincipalName "J.Robinson@enterprise.com" -Path "OU=Managers,DC=enterprise,DC=com" -
AccountPassword(Read-Host -AsSecureString "Input Password") -Enabled $true
```

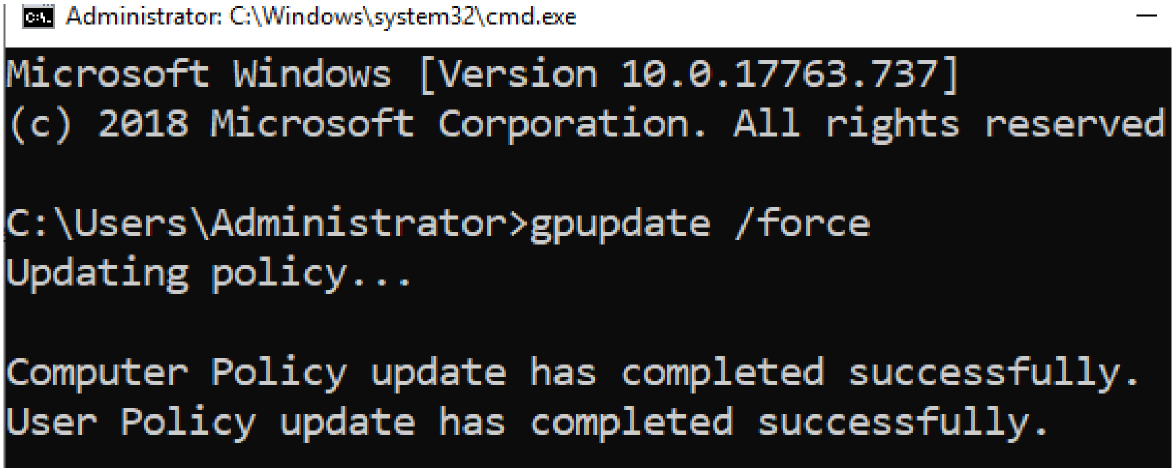
Modifying password policies

Serevr Manager→Group Policy Management→Edit both default domain controllers policy and default domain policy





Policy	Policy Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

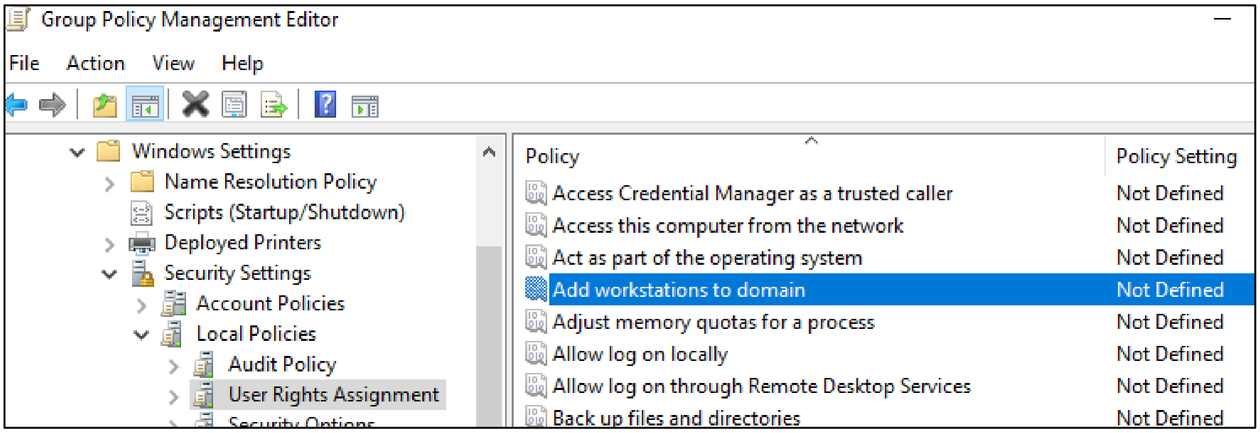

Administrator: C:\Windows\system32\cmd.exe

```
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved

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

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

Joining workstation computers

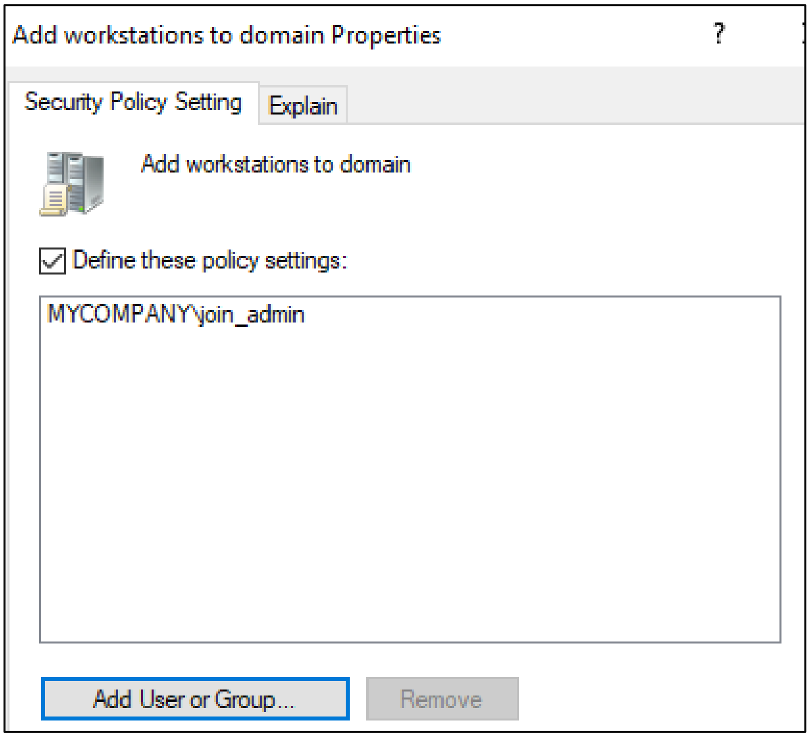
It is highly recommended to create a separate user (not the server's admin account) that will be used for joining the workstations to the domain

1. On the AD Server, create a new user for this specific task (or select an existing user that will be performing the workstation join)
2. Go to server manager→tools→group policy management
3. Navigate to default domain policy and go the following setting:



- Windows Settings
  - Name Resolution Policy
  - Scripts (Startup/Shutdown)
  - Deployed Printers
  - Security Settings
    - Account Policies
    - Local Policies
      - Audit Policy
      - User Rights Assignment
      - Security Options

Policy	Policy Setting
Access Credential Manager as a trusted caller	Not Defined
Access this computer from the network	Not Defined
Act as part of the operating system	Not Defined
Add workstations to domain	Not Defined
Adjust memory quotas for a process	Not Defined
Allow log on locally	Not Defined
Allow log on through Remote Desktop Services	Not Defined
Back up files and directories	Not Defined



Add workstations to domain

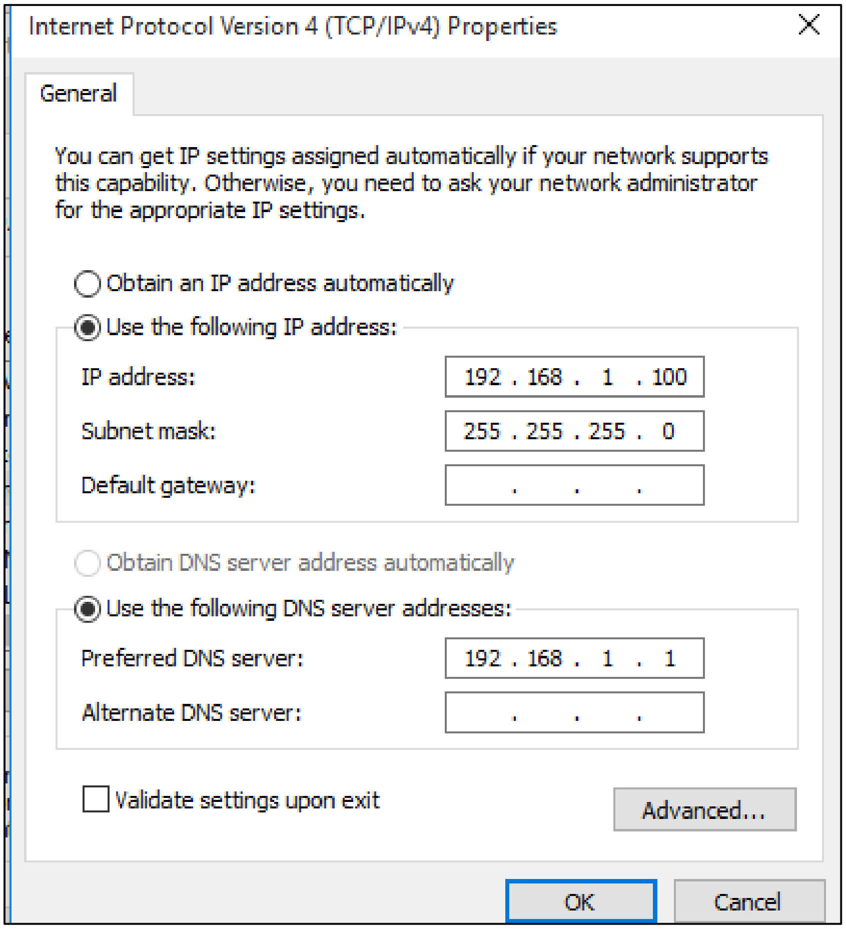
☑ Define these policy settings:

MYCOMPANY\join_admin

Don't forget to perform a GPUPDATE /FORCE afterwards to implement the changes in the settings.

On the workstation PCs that you will be joining on to the domain, do the following:

1. Set / correct timezone
2. Make sure the domain controller where you will be connecting is reachable on the network
3. Set a distinguishable name for your workstation, reboot as necessary
4. Set the IP (static or dynamic). the DNS server IP setting should be pointing to the IP of your DNS Server



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address:	192 . 168 . 1 . 100
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	. . .

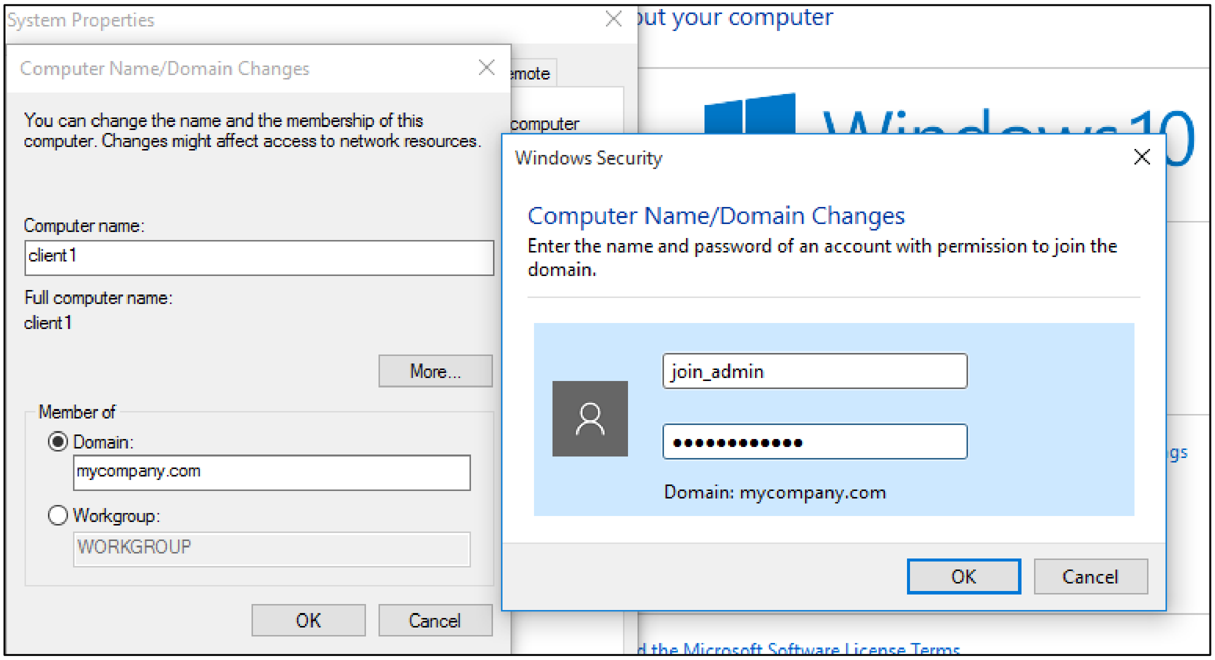
○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server:	192 . 168 . 1 . 1
Alternate DNS server:	. . .

□ Validate settings upon exit

5. You may join the domain using the workstation system properties



Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name: client1

Full computer name: client1

Member of

● Domain: mycompany.com

○ Workgroup: WORKGROUP

Windows Security

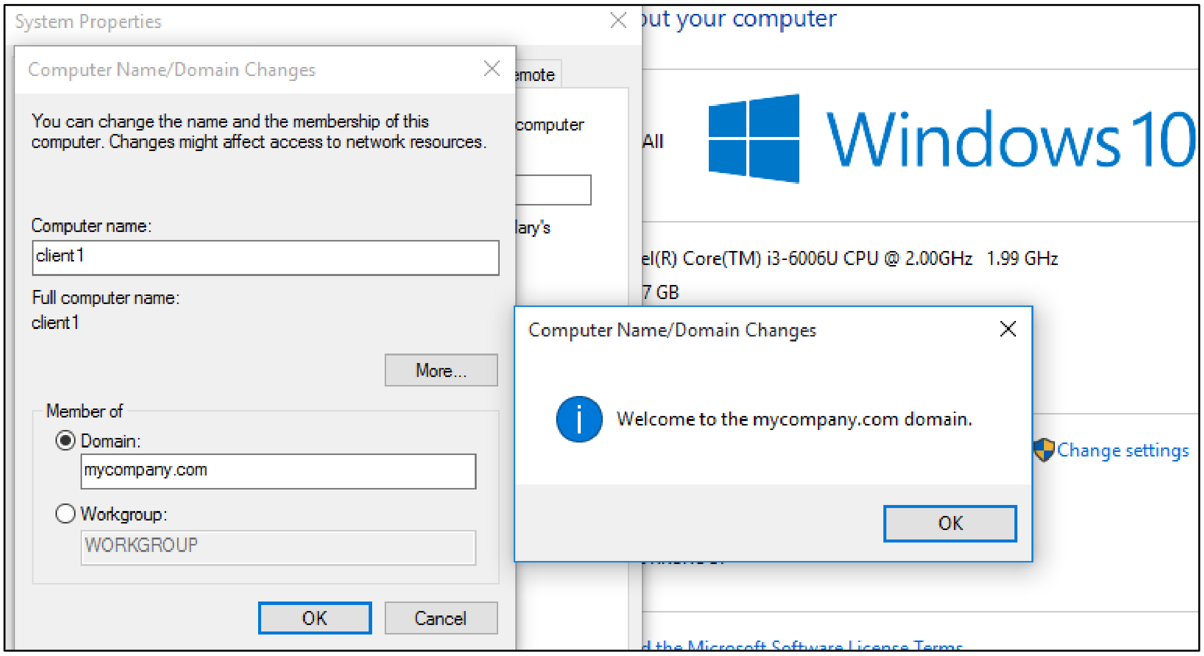
Computer Name/Domain Changes

Enter the name and password of an account with permission to join the domain.

join_admin

••••••••••••

Domain: mycompany.com



Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name: client1

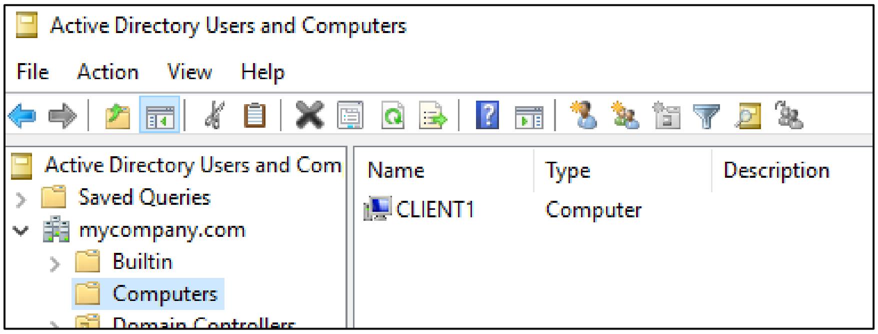
Full computer name: client1

Member of
● Domain: mycompany.com
○ Workgroup: WORKGROUP

Computer Name/Domain Changes

Welcome to the mycompany.com domain.

6. Verify workstation membership

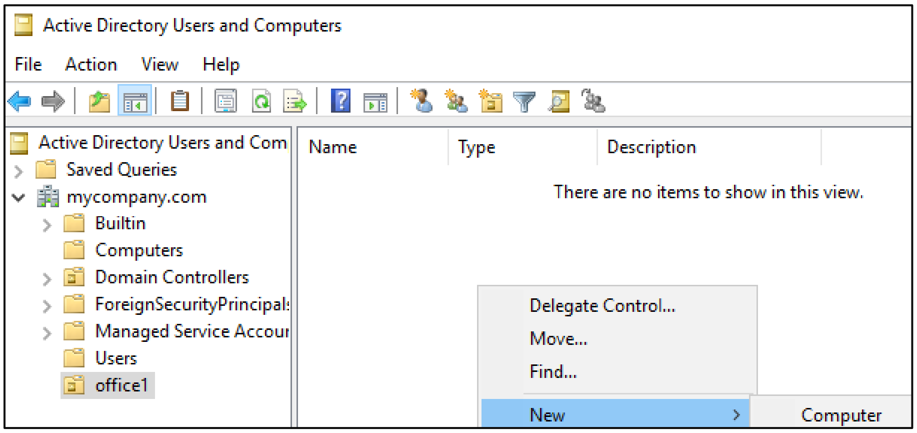


Name	Type	Description
CLIENT1	Computer	

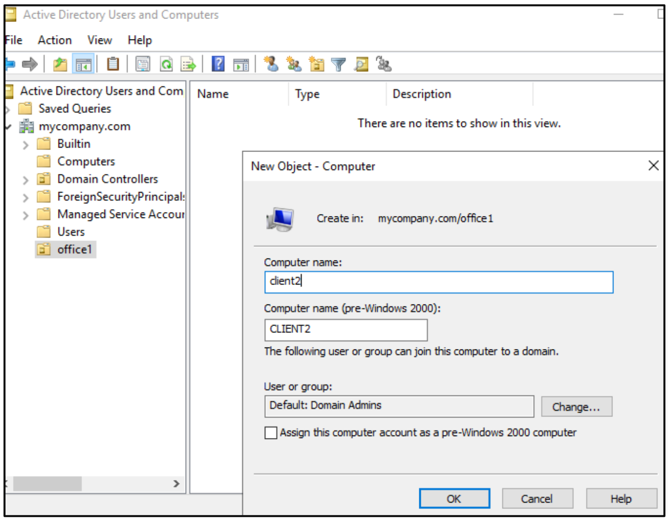
Pre-staging workstation domain members

By default, domain computer members will appear in the Computers container of Active Directory Users and Computers. It is also possible to create other containers (recommended: Organizational Units) first then pre-create computer accounts bearing the same computer names as the ones that will be joining.

Create new organizational unit (ex. “office 1”) then create a computer account inside



There are no items to show in this view.



Create in: mycompany.com/office1

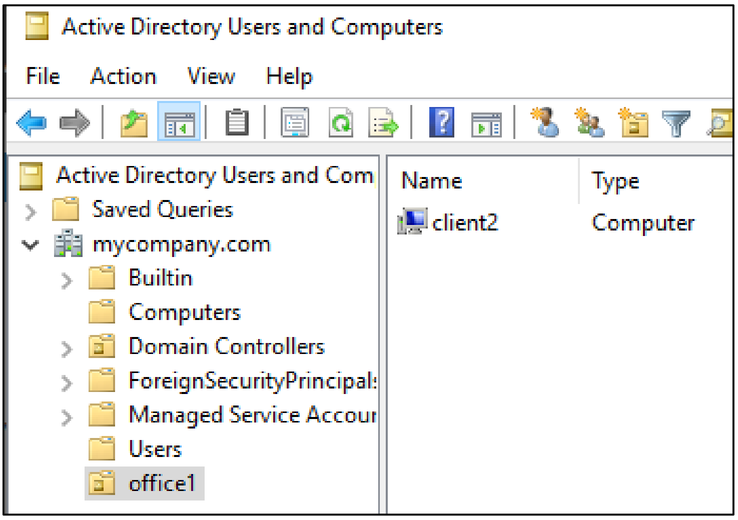
Computer name: client2

Computer name (pre-Windows 2000): CLIENT2

The following user or group can join this computer to a domain.

User or group: Default: Domain Admins

□ Assign this computer account as a pre-Windows 2000 computer

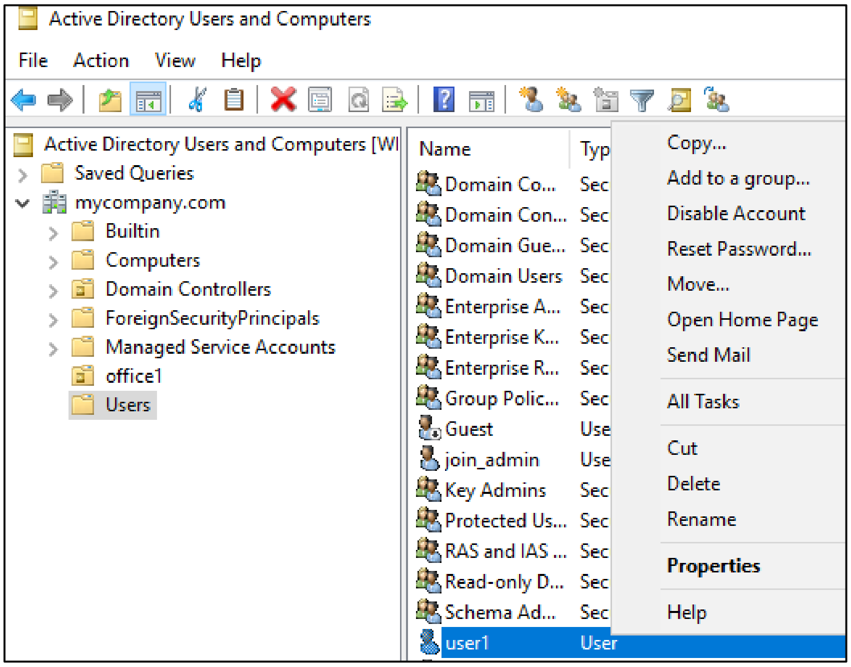


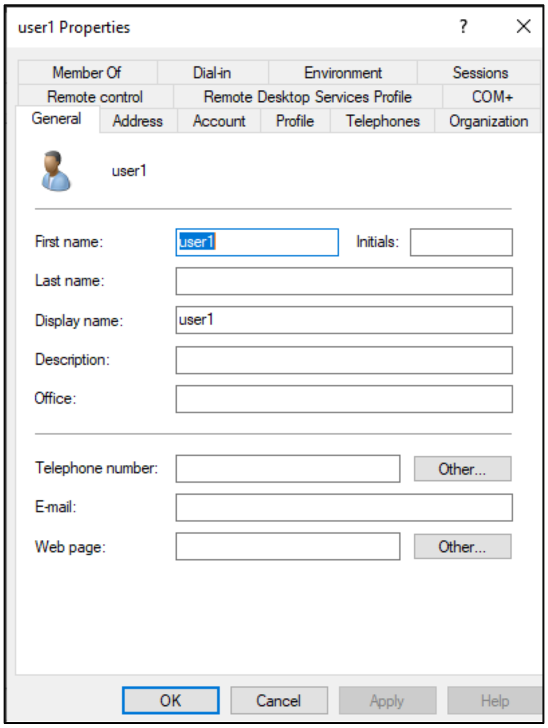
*note: you may also use the REDIRCMP command to redirect joining computers to a specific OU using the container's distinguished name. On the active directory server:

```
\> redircmp “ou=office1,dc=mycompany,dc=com”
```

Account management

Active Directory Objects all have their own specific properties that you can manage in the Active Directory Users and Computers Tool





user1

First name: user1

Initials:

Last name:

Display name: user1

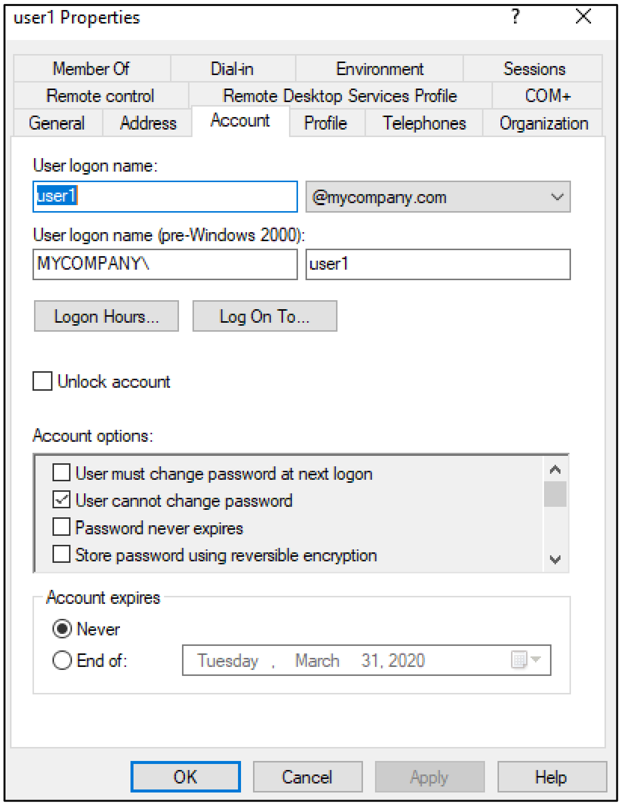
Description:

Office:

Telephone number:

E-mail:

Web page:



User logon name: user1 @mycompany.com

User logon name (pre-Windows 2000): MYCOMPANY\ user1

□ Unlock account

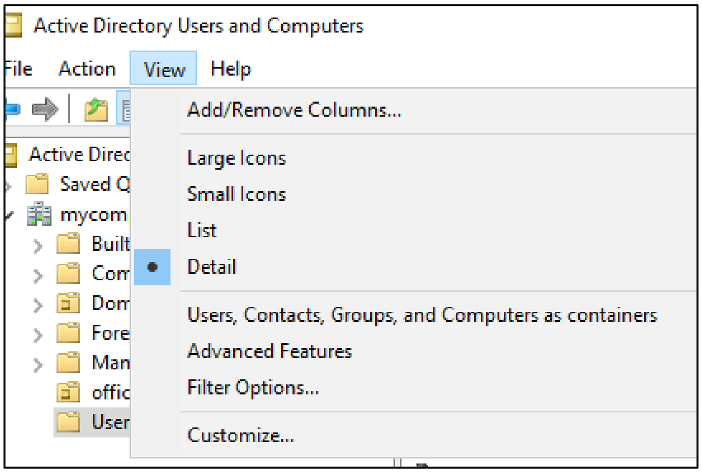
Account options:

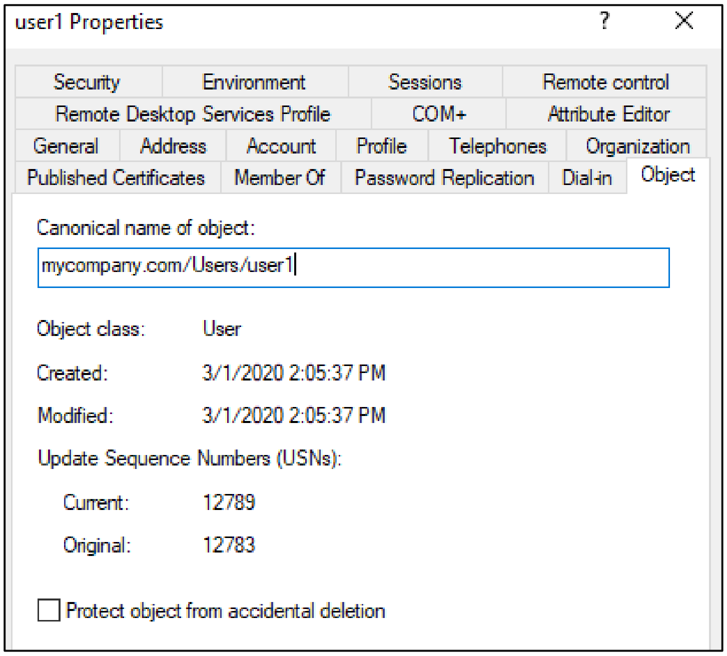
- □ User must change password at next logon
- ☑ User cannot change password
- □ Password never expires
- □ Store password using reversible encryption

Account expires

- ● Never
- ○ End of: Tuesday , March 31, 2020

You can also open advanced features to see more options like protecting objects from accidental deletion





Canonical name of object: mycompany.com/Users/user1

Object class: User

Created: 3/1/2020 2:05:37 PM

Modified: 3/1/2020 2:05:37 PM

Update Sequence Numbers (USNs):

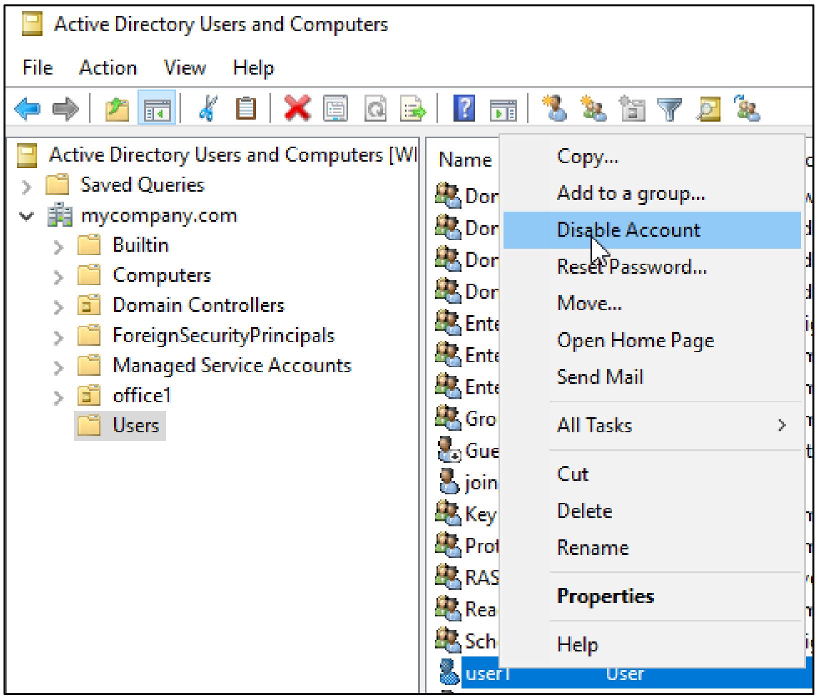
Current: 12789

Original: 12783

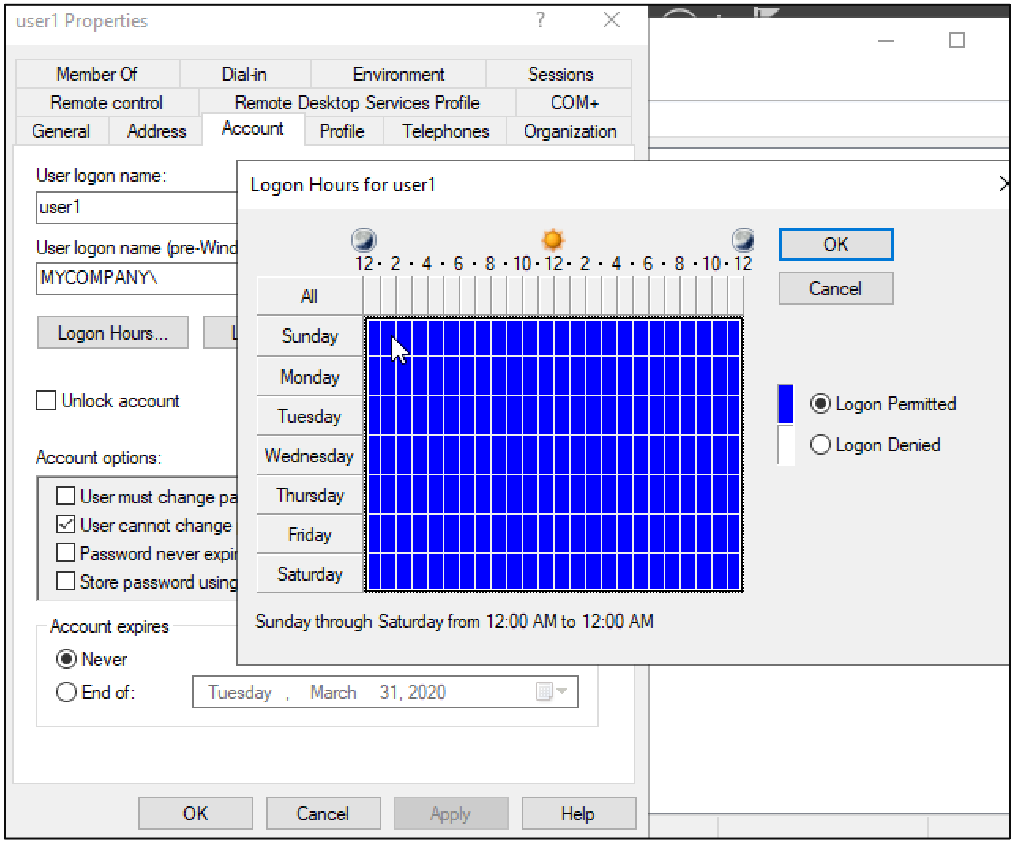
□ Protect object from accidental deletion

Setting Login Restrictions

1. Disabling / reenabling users and computers



2. Account logon hours



User logon name: user1

User logon name (pre-Wind: MYCOMPANY\

☐ Unlock account

Account options:

☐ User must change pa
☑ User cannot change
☐ Password never expi
☐ Store password using

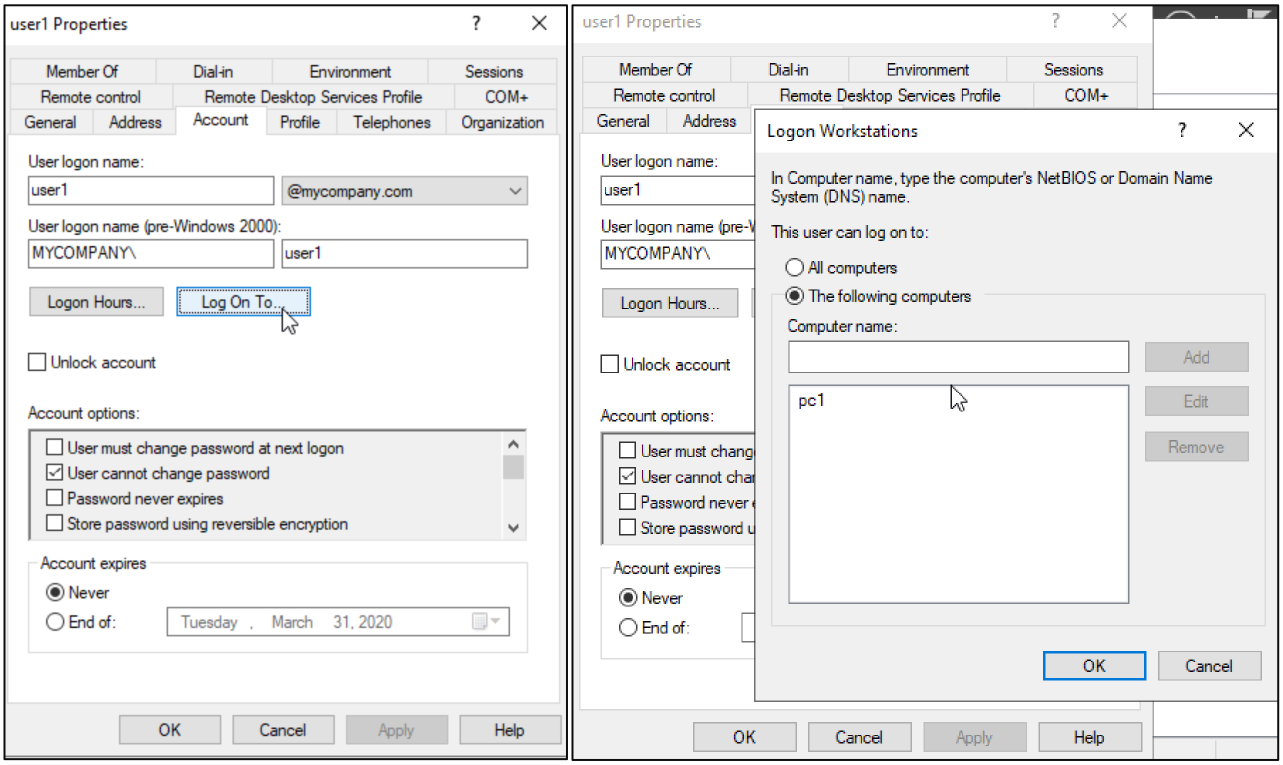
Account expires

● Never
○ End of: Tuesday , March 31, 2020

🟦 ● Logon Permitted
☐ ○ Logon Denied

Sunday through Saturday from 12:00 AM to 12:00 AM

3. Account workstation restriction



User logon name: user1 @mycompany.com

User logon name (pre-Windows 2000): MYCOMPANY\ user1

□ Unlock account

Account options:

□ User must change password at next logon
☑ User cannot change password
□ Password never expires
□ Store password using reversible encryption

Account expires

● Never
○ End of: Tuesday , March 31, 2020

In Computer name, type the computer's NetBIOS or Domain Name System (DNS) name.

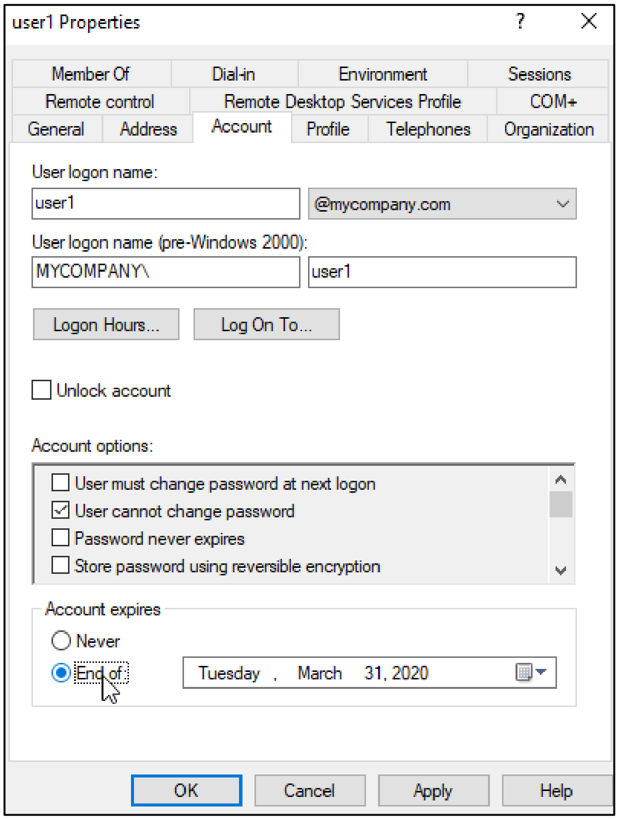
This user can log on to:

○ All computers
● The following computers

Computer name:

pc1

4. Account expiration



User logon name: user1 @mycompany.com

User logon name (pre-Windows 2000): MYCOMPANY\ user1

□ Unlock account

Account options:

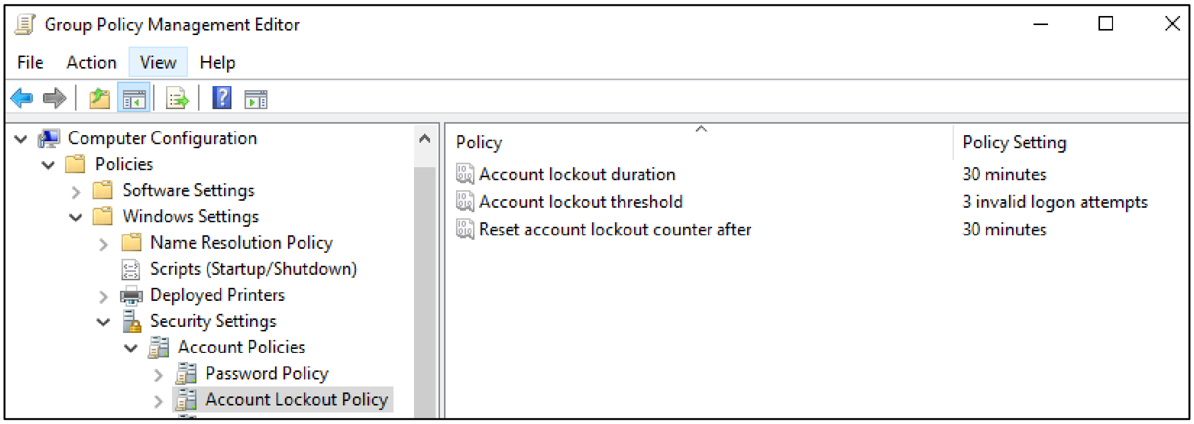
□ User must change password at next logon
☑ User cannot change password
□ Password never expires
□ Store password using reversible encryption

Account expires

○ Never
● End of: Tuesday , March 31, 2020

5. Enabling account lockouts for invalid logon attempts

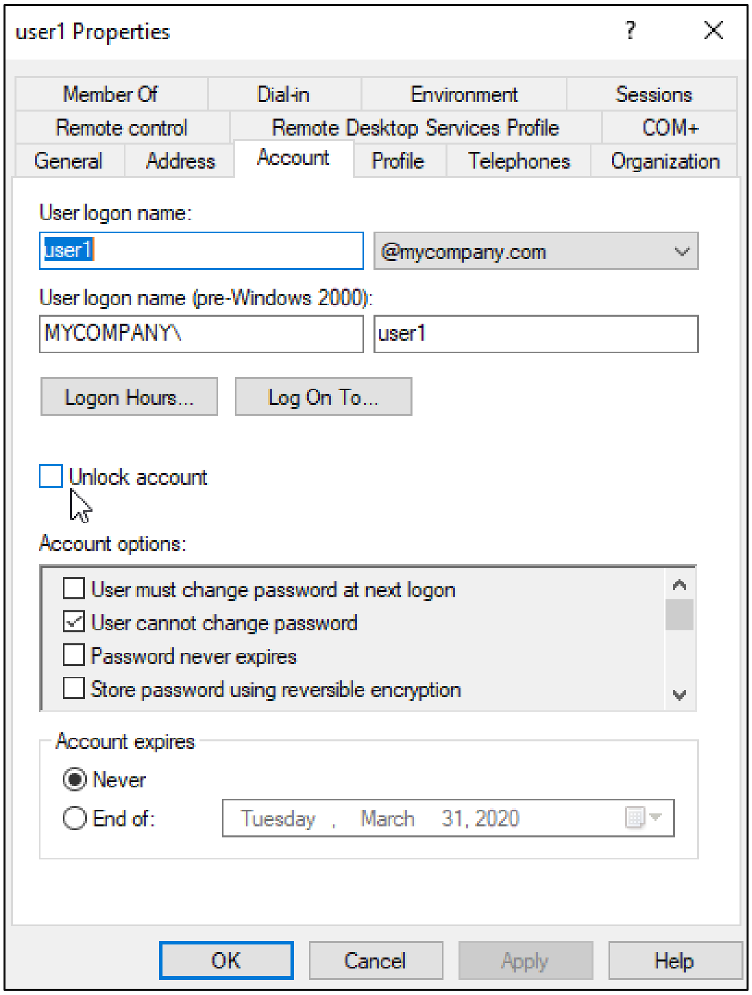
   a. Server manager→tools→group policy management→gpo objects→default domain policy(edit)



Policy	Policy Setting
Account lockout duration	30 minutes
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	30 minutes

   b. Cmd→ gpupdate /force

   To manually unlock locked-out accounts in active directory users and computers→user properties



User logon name: user1 @mycompany.com

User logon name (pre-Windows 2000): MYCOMPANY\ user1

□ Unlock account

Account options:

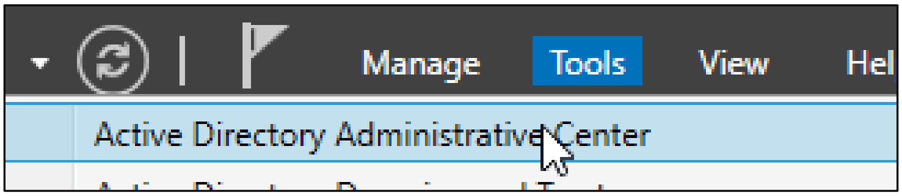
□ User must change password at next logon
☑ User cannot change password
□ Password never expires
□ Store password using reversible encryption

Account expires

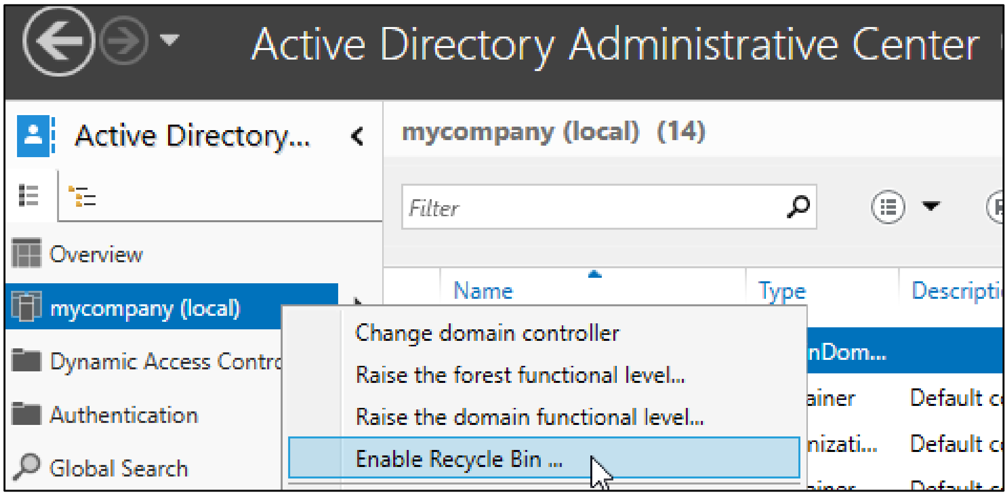
● Never
○ End of: Tuesday , March 31, 2020

Enabling and Using Active Directory Recycle Bin

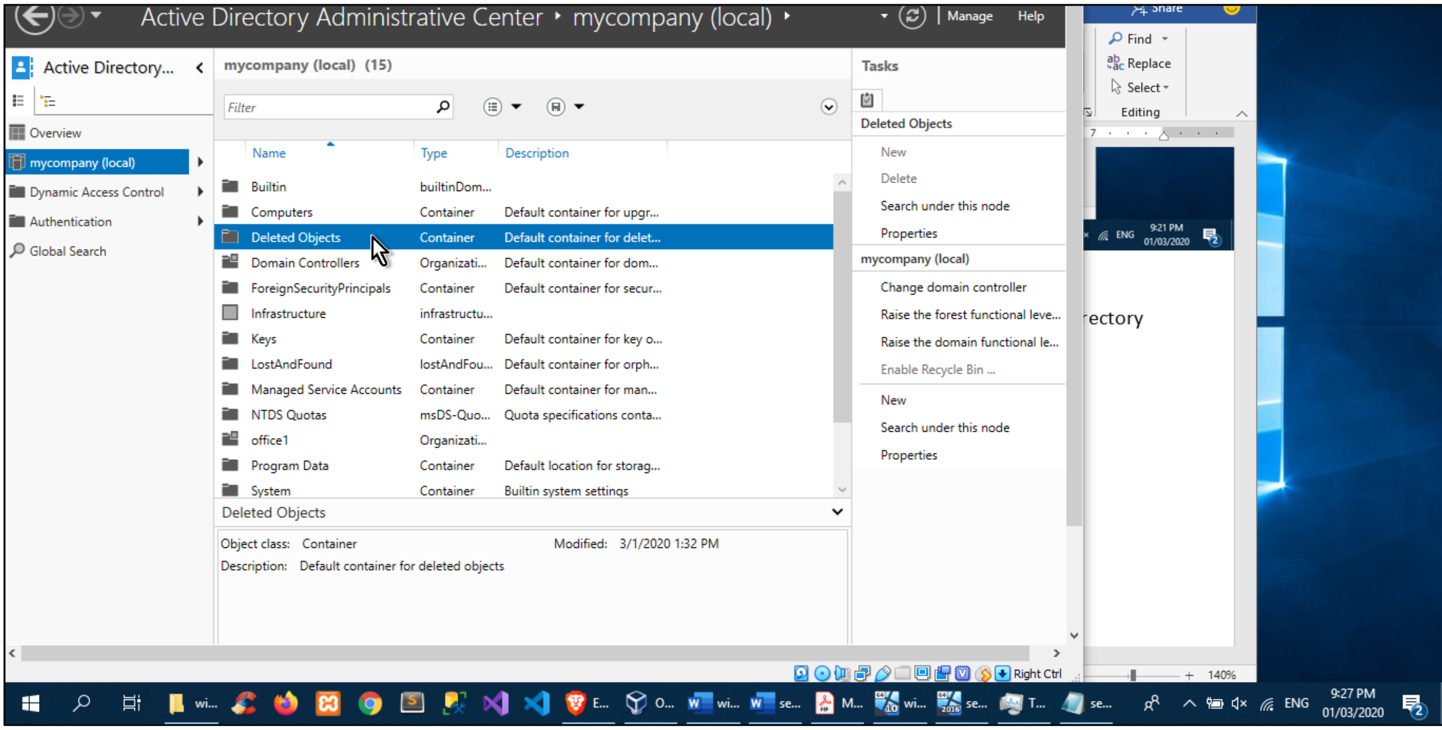
1. Open up active directory administrative center



2. In the Active Directory, Administrative Center Click on the "Enable Recycle Bin" on the right pane (or rclick your domain from the left pane). Once Recycle Bin has been enabled, it cannot be disabled.



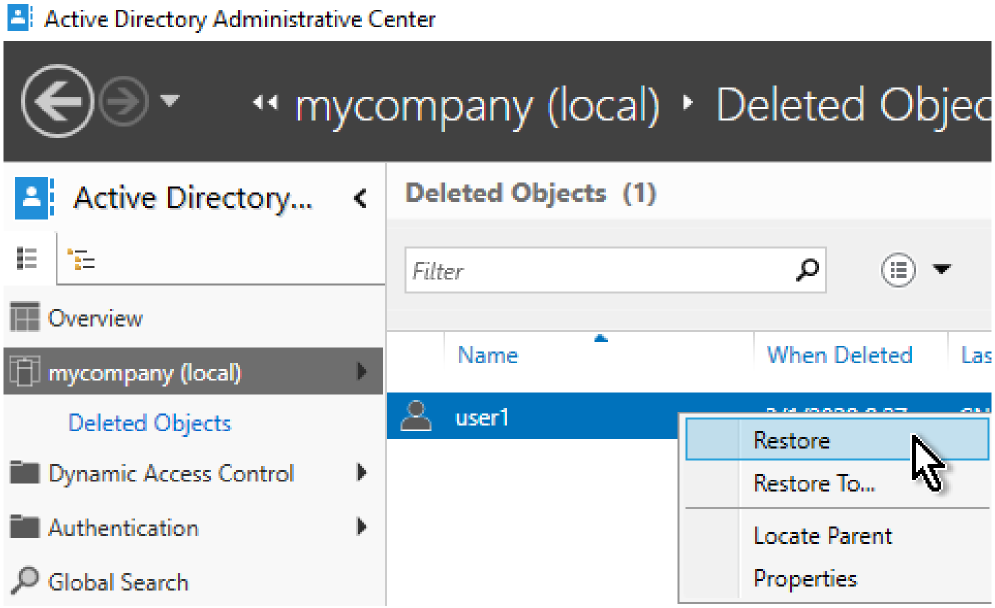
3. Try deleting an object in the Active Directory users and computers (ex. Try deleting a user account)
4. After Enable of Recycle Bin, All deleted objects moved inside the Deleted Objects container in Active Directory Administrative Center.



Name	Type	Description
Builtin	builtinDom...	
Computers	Container	Default container for upgr...
Deleted Objects	Container	Default container for delet...
Domain Controllers	Organizati...	Default container for dom...
ForeignSecurityPrincipals	Container	Default container for secur...
Infrastructure	infrastructu...	
Keys	Container	Default container for key o...
LostAndFound	lostAndFou...	Default container for orph...
Managed Service Accounts	Container	Default container for man...
NTDS Quotas	msDS-Quo...	Quota specifications conta...
office1	Organizati...	
Program Data	Container	Default location for storag...
System	Container	Builtin system settings

Deleted Objects

Object class: Container   Modified: 3/1/2020 1:32 PM
Description: Default container for deleted objects



Understanding Built-in Security Groups

Enterprise Admins

The Enterprise Admins (EA) group is located in the forest root domain, and by default, it is a member of the built-in Administrators group in every domain in the forest. The Built-in Administrator account in the forest root domain is the only default member of the EA group. EAs are granted rights and permissions that allow them to affect forest-wide changes. These are changes that affect all domains in the forest, such as adding or removing domains, establishing forest trusts, or raising forest functional levels. In a properly designed and implemented delegation model, EA membership is required only when first constructing the forest or when making certain forest-wide changes such as establishing an outbound forest trust.

The EA group is located by default in the Users container in the forest root domain, and it is a universal security group, unless the forest root domain is running in Windows 2000 Server mixed mode, in which case the group is a global security group. Although some rights are granted directly to the EA group, many of this group's rights are actually inherited by the EA group because it is a member of the Administrators group in each domain in the forest. Enterprise Admins have no default rights on workstations or member servers.

Domain Admins

Each domain in a forest has its own Domain Admins (DA) group, which is a member of that domain's built-in Administrators (BA) group in addition to a member of the local Administrators group on every computer that is joined to the domain. The only default member of the DA group for a domain is the Built-in Administrator account for that domain.

DAs are all-powerful within their domains, while EAs have forest-wide privilege. In a properly designed and implemented delegation model, DA membership should be required only in "break glass" scenarios, which are situations in which an account with high levels of privilege on every computer in the domain is needed, or when certain domain wide changes must be made. Although native Active Directory delegation mechanisms do allow delegation to the extent that it is possible to use DA accounts only in emergency scenarios, constructing an effective delegation model can be time consuming, and many organizations use third-party applications to expedite the process.

The DA group is a global security group located in the Users container for the domain. There is one DA group for each domain in the forest, and the only default member of a DA group is the domain's Built-in Administrator account. Because a domain's DA group is nested in the domain's BA group and every domain-joined system's local Administrators group, DAs not only have permissions that are specifically granted to Domain Admins, but they also inherit all rights and permissions granted to the domain's Administrators group and the local Administrators group on all systems joined to the domain.

Administrators

The built-in Administrators (BA) group is a domain local group in a domain's Built-in container into which DAs and EAs are nested, and it is this group that is granted many of the direct rights and permissions in the directory and on domain controllers. However, the Administrators group for a domain does not have any privileges on member servers or on workstations. Membership in domain-joined computers' local Administrators group is where local privilege is granted; and of the groups discussed, only DAs are members of all domain-joined computers' local Administrators groups by default.

The Administrators group is a domain-local group in the domain's Built-in container. By default, every domain's BA group contains the local domain's Built-in Administrator account, the local domain's DA group, and the forest root domain's EA group. Many user rights in Active Directory and on domain controllers are granted specifically to the Administrators group, not to EAs or DAs. A domain's BA group is granted full control permissions on most directory objects, and can take ownership of directory objects. Although EA and DA groups are granted certain object-specific permissions in the forest and domains, much of the power of groups is actually "inherited" from their membership in BA groups.

Schema Admins

The Schema Admins (SA) group is a universal group in the forest root domain and has only that domain's Built-in Administrator account as a default member, similar to the EA group. Although membership in the SA group can allow an attacker to compromise the Active Directory schema, which is the framework for the entire Active Directory forest, SAs have few default rights and permissions beyond the schema.

You should carefully manage and monitor membership in the SA group, but in some respects, this group is "less privileged" than the three highest privileged groups described earlier because the scope of its privilege is very narrow; that is, SAs have no administrative rights anywhere other than the schema.

Access Control Assistance Operators (Active Directory in Windows Server 2012)

Members of this group can remotely query authorization attributes and permissions for resources on this computer.

- Inherited user rights:
- Access this computer from the network
- Add workstations to domain
- Bypass traverse checking
- Increase a process working set

Account Operators

Members can administer domain user and group accounts.

Inherited user rights:
Access this computer from the network
Add workstations to domain
Bypass traverse checking
Increase a process working set

Administrator account

Built-in account for administering the domain.
Inherited user rights:
Access this computer from the network
Add workstations to domain
Adjust memory quotas for a process
Allow log on locally
Allow log on through Remote Desktop Services
Back up files and directories
Bypass traverse checking
Change the system time
Change the time zone
Create a pagefile
Create global objects
Create symbolic links
Debug programs
Enable computer and user accounts to be trusted for delegation
Force shutdown from a remote system
Impersonate a client after authentication
Increase a process working set
Increase scheduling priority
Load and unload device drivers
Log on as a batch job
Manage auditing and security log
Modify firmware environment values
Perform volume maintenance tasks
Profile single process
Profile system performance
Remove computer from docking station
Restore files and directories
Shut down the system
Take ownership of files or other objects

Administrators group

Administrators have complete and unrestricted access to the domain.
Direct user rights:
Access this computer from the network
Adjust memory quotas for a process
Allow log on locally
Allow log on through Remote Desktop Services
Back up files and directories
Bypass traverse checking
Change the system time
Change the time zone
Create a pagefile
Create global objects
Create symbolic links
Debug programs
Enable computer and user accounts to be trusted for delegation

Force shutdown from a remote system
Impersonate a client after authentication
Increase scheduling priority
Load and unload device drivers
Log on as a batch job
Manage auditing and security log
Modify firmware environment values
Perform volume maintenance tasks
Profile single process
Profile system performance
Remove computer from docking station
Restore files and directories
Shut down the system
Take ownership of files or other objects

Inherited user rights:
Access this computer from the network
Add workstations to domain
Bypass traverse checking
Increase a process working set

Allowed RODC Password Replication Group
Members in this group can have their passwords replicated to all read-only domain controllers in the domain.
Inherited user rights:
Access this computer from the network
Add workstations to domain
Bypass traverse checking
Increase a process working set

Backup Operators
Backup Operators can override security restrictions for the sole purpose of backing up or restoring files.

Direct user rights:
Allow log on locally
Back up files and directories
Log on as a batch job
Restore files and directories
Shut down the system

Inherited user rights:
Access this computer from the network
Add workstations to domain
Bypass traverse checking
Increase a process working set

Cert Publishers
Members of this group are permitted to publish certificates to the directory.
Inherited user rights:
Access this computer from the network
Add workstations to domain

Bypass traverse checking
Increase a process working set

Certificate Service DCOM Access

If Certificate Services is installed on a domain controller (not recommended), this group grants DCOM enrollment access to Domain Users and Domain Computers.
Inherited user rights:
Access this computer from the network
Add workstations to domain
Bypass traverse checking
Increase a process working set

Cloneable Domain Controllers (AD DS in Windows Server 2012AD DS)

Members of this group that are domain controllers may be cloned.
Inherited user rights:
Access this computer from the network
Add workstations to domain
Bypass traverse checking
Increase a process working set

Cryptographic Operators

Members are authorized to perform cryptographic operations.
Inherited user rights:
Access this computer from the network
Add workstations to domain
Bypass traverse checking
Increase a process working set

Denied RODC Password Replication Group

Members in this group cannot have their passwords replicated to any read-only domain controllers in the domain.
Inherited user rights:
Access this computer from the network
Add workstations to domain
Bypass traverse checking
Increase a process working set

DHCP Administrators

Members of this group have administrative access to the DHCP Server service.
Inherited user rights:
Access this computer from the network
Add workstations to domain
Bypass traverse checking
Increase a process working set

DHCP Users

Members of this group have view-only access to the DHCP Server service.
Inherited user rights:
Access this computer from the network
Add workstations to domain
Bypass traverse checking

Increase a process working set

Distributed COM Users

Members of this group are allowed to launch, activate, and use distributed COM objects on this computer.
Inherited user rights:
Access this computer from the network
Add workstations to domain
Bypass traverse checking
Increase a process working set

DnsAdmins

Members of this group have administrative access to the DNS Server service.
Inherited user rights:
Access this computer from the network
Add workstations to domain
Bypass traverse checking
Increase a process working set

DnsUpdateProxy

Members of this group are DNS clients who are permitted to perform dynamic updates on behalf of clients that cannot themselves perform dynamic updates. Members of this group are typically DHCP servers.
Inherited user rights:
Access this computer from the network
Add workstations to domain
Bypass traverse checking
Increase a process working set

Domain Admins

Designated administrators of the domain; Domain Admins is a member of every domain-joined computer's local Administrators group and receives rights and permissions granted to the local Administrators group, in addition to the domain's Administrators group.
Inherited user rights:
Access this computer from the network
Add workstations to domain
Adjust memory quotas for a process
Allow log on locally
Allow log on through Remote Desktop Services
Back up files and directories
Bypass traverse checking
Change the system time
Change the time zone
Create a pagefile
Create global objects
Create symbolic links
Debug programs
Enable computer and user accounts to be trusted for delegation
Force shutdown from a remote system
Impersonate a client after authentication
Increase a process working set
Increase scheduling priority

Load and unload device drivers
Log on as a batch job
Manage auditing and security log
Modify firmware environment values
Perform volume maintenance tasks
Profile single process
Profile system performance
Remove computer from docking station
Restore files and directories
Shut down the system
Take ownership of files or other objects

Domain Computers
All workstations and servers that are joined to the domain are by default members of this group.
Inherited user rights:
Access this computer from the network
Add workstations to domain
Bypass traverse checking
Increase a process working set

Domain Controllers
All domain controllers in the domain. Note: Domain controllers are not a member of the Domain Computers group.
Inherited user rights:
Access this computer from the network
Add workstations to domain
Bypass traverse checking
Increase a process working set

Domain Guests
All guests in the domain
Inherited user rights:
Access this computer from the network
Add workstations to domain
Bypass traverse checking
Increase a process working set

Domain Users
All users in the domain
Inherited user rights:
Access this computer from the network
Add workstations to domain
Bypass traverse checking
Increase a process working set

Enterprise Admins (exists only in forest root domain)
Enterprise Admins have permissions to change forest-wide configuration settings; Enterprise Admins is a member of every domain's Administrators group and receives rights and permissions granted to that group.
Inherited user rights:
Access this computer from the network
Add workstations to domain

Adjust memory quotas for a process
Allow log on locally
Allow log on through Remote Desktop Services
Back up files and directories
Bypass traverse checking
Change the system time
Change the time zone
Create a pagefile
Create global objects
Create symbolic links
Debug programs
Enable computer and user accounts to be trusted for delegation
Force shutdown from a remote system
Impersonate a client after authentication
Increase a process working set
Increase scheduling priority
Load and unload device drivers
Log on as a batch job
Manage auditing and security log
Modify firmware environment values
Perform volume maintenance tasks
Profile single process
Profile system performance
Remove computer from docking station
Restore files and directories
Shut down the system
Take ownership of files or other objects

Enterprise Read-only Domain Controllers
This group contains the accounts for all read-only domain controllers in the forest.
Inherited user rights:
Access this computer from the network
Add workstations to domain
Bypass traverse checking
Increase a process working set

Event Log Readers
Members of this group in can read the event logs on domain controllers.
Inherited user rights:
Access this computer from the network
Add workstations to domain
Bypass traverse checking
Increase a process working set

Group Policy Creator Owners
Members of this group can create and modify Group Policy Objects in the domain.
Inherited user rights:
Access this computer from the network
Add workstations to domain
Bypass traverse checking

Increase a process working set

Guest

This is the only account in an AD DS domain that does not have the Authenticated Users SID added to its access token. Therefore, any resources that are configured to grant access to the Authenticated Users group will not be accessible to this account. This behavior is not true of members of the Domain Guests and Guests groups, however- members of those groups do have the Authenticated Users SID added to their access tokens.
Inherited user rights:
Access this computer from the network
Bypass traverse checking
Increase a process working set

Guests

Guests have the same access as members of the Users group by default, except for the Guest account, which is further restricted as described earlier.
Inherited user rights:
Access this computer from the network
Add workstations to domain
Bypass traverse checking
Increase a process working set

Hyper-V Administrators

Members of this group have complete and unrestricted access to all features of Hyper-V.
Inherited user rights:
Access this computer from the network
Add workstations to domain
Bypass traverse checking
Increase a process working set

IIS_IUSRS

Built-in group used by Internet Information Services.
Inherited user rights:
Access this computer from the network
Add workstations to domain
Bypass traverse checking
Increase a process working set

Incoming Forest Trust Builders (exists only in forest root domain)

Members of this group can create incoming, one-way trusts to this forest. (Creation of outbound forest trusts is reserved for Enterprise Admins.)
Inherited user rights:
Access this computer from the network
Add workstations to domain
Bypass traverse checking
Increase a process working set

Krbtgt

The Krbtgt account is the service account for the Kerberos Key Distribution Center in the domain. This account has access to all accounts' credentials stored in Active Directory. This account is disabled by default and should never be enabled

Network Configuration Operators

Members of this group are granted privileges that allow them to manage configuration of networking features.
Inherited user rights:
Access this computer from the network
Add workstations to domain
Bypass traverse checking
Increase a process working set

Performance Log Users

Members of this group can schedule logging of performance counters, enable trace providers, and collect event traces locally and via remote access to the computer.
Direct user rights:
Log on as a batch job
Inherited user rights:
Access this computer from the network
Add workstations to domain
Bypass traverse checking
Increase a process working set

Performance Monitor Users

Members of this group can access performance counter data locally and remotely.
Inherited user rights:
Access this computer from the network
Add workstations to domain
Bypass traverse checking
Increase a process working set

Pre-Windows 2000 Compatible Access

This group exists for backward compatibility with operating systems prior to Windows 2000 Server, and it provides the ability for members to read user and group information in the domain.
Direct user rights:
Access this computer from the network
Bypass traverse checking
Inherited user rights:
Add workstations to domain
Increase a process working set

Print Operators

Members of this group can administer domain printers.
Direct user rights:
Allow log on locally
Load and unload device drivers
Shut down the system
Inherited user rights:
Access this computer from the network
Add workstations to domain
Bypass traverse checking
Increase a process working set

RAS and IAS Servers

Servers in this group can read remote access properties on user accounts in the domain.
Inherited user rights:
Access this computer from the network
Add workstations to domain
Bypass traverse checking
Increase a process working set

RDS Endpoint Servers
Servers in this group run virtual machines and host sessions where users RemoteApp programs and personal virtual desktops run. This group needs to be populated on servers running RD Connection Broker. RD Session Host servers and RD Virtualization Host servers used in the deployment need to be in this group.
Inherited user rights:
Access this computer from the network
Add workstations to domain
Bypass traverse checking
Increase a process working set

RDS Management Servers
Servers in this group can perform routine administrative actions on servers running Remote Desktop Services. This group needs to be populated on all servers in a Remote Desktop Services deployment. The servers running the RDS Central Management service must be included in this group.
Inherited user rights:
Access this computer from the network
Add workstations to domain
Bypass traverse checking
Increase a process working set

RDS Remote Access Servers
Servers in this group enable users of RemoteApp programs and personal virtual desktops access to these resources. In Internet-facing deployments, these servers are typically deployed in an edge network. This group needs to be populated on servers running RD Connection Broker. RD Gateway servers and RD Web Access servers used in the deployment need to be in this group.
Inherited user rights:
Access this computer from the network
Add workstations to domain
Bypass traverse checking
Increase a process working set

Read-only Domain Controllers
This group contains all read-only domain controllers in the domain.
Inherited user rights:
Access this computer from the network
Add workstations to domain
Bypass traverse checking
Increase a process working set

Remote Desktop Users
Members of this group are granted the right to log on remotely using RDP.
Inherited user rights:
Access this computer from the network

Add workstations to domain
Bypass traverse checking
Increase a process working set

Remote Management Users
Members of this group can access WMI resources over management protocols (such as WS-Management via the Windows Remote Management service). This applies only to WMI namespaces that grant access to the user.
Inherited user rights:
Access this computer from the network
Add workstations to domain
Bypass traverse checking
Increase a process working set

Replicator
Supports legacy file replication in a domain.
Inherited user rights:
Access this computer from the network
Add workstations to domain
Bypass traverse checking
Increase a process working set

Schema Admins (exists only in forest root domain)
Schema admins are the only users who can make modifications to the Active Directory schema, and only if the schema is write-enabled.
Inherited user rights:
Access this computer from the network
Add workstations to domain
Bypass traverse checking
Increase a process working set

Server Operators
Members of this group can administer domain servers.
Direct user rights:
Allow log on locally
Back up files and directories
Change the system time
Change the time zone
Force shutdown from a remote system
Restore files and directories
Shut down the system

Inherited user rights:
Access this computer from the network
Add workstations to domain
Bypass traverse checking
Increase a process working set

Terminal Server License Servers
Members of this group can update user accounts in Active Directory with information about license issuance, for the purpose of tracking and reporting TS Per User CAL usage

Inherited user rights:
Access this computer from the network
Add workstations to domain
Bypass traverse checking
Increase a process working set

Users

Users have permissions that allow them to read many objects and attributes in Active Directory, although they cannot change most. Users are prevented from making accidental or intentional system-wide changes and can run most applications.

Direct user rights:
Increase a process working set
Inherited user rights:
Access this computer from the network
Add workstations to domain
Bypass traverse checking

Windows Authorization Access Group

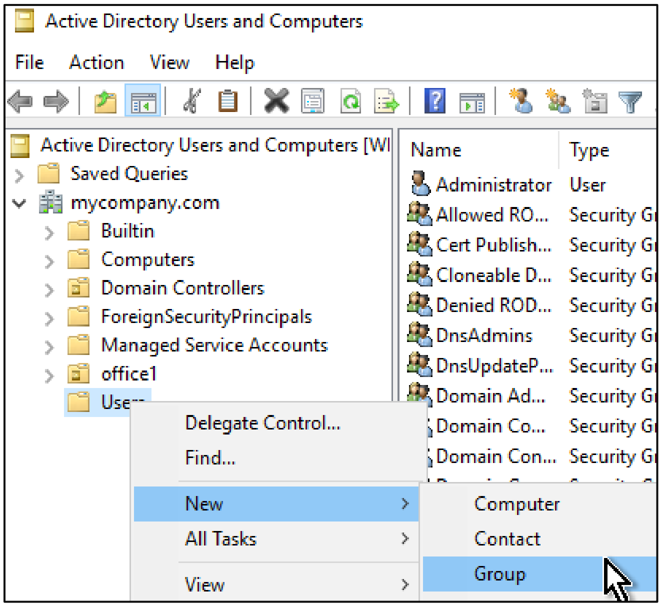
Members of this group have access to the computed tokenGroupsGlobalAndUniversal attribute on User objects
Inherited user rights:
Access this computer from the network
Add workstations to domain
Bypass traverse checking
Increase a process working set

WinRMRemoteWMIUsers

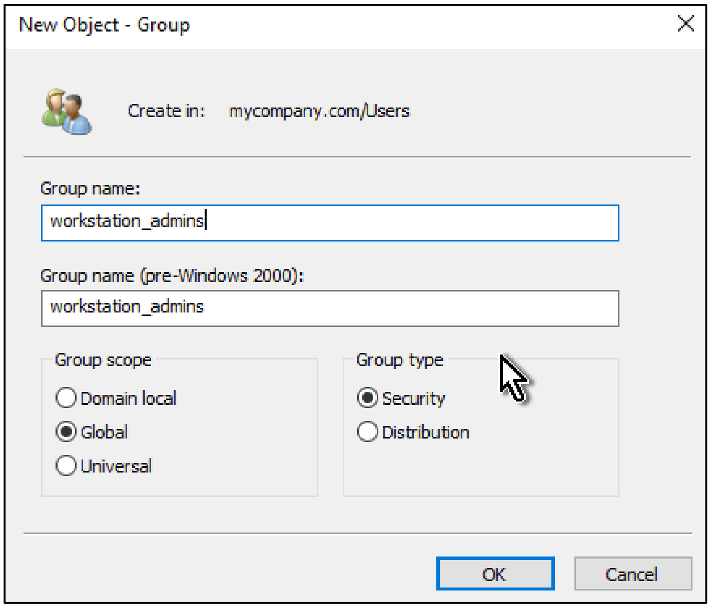
Members of this group can access WMI resources over management protocols (such as WS-Management via the Windows Remote Management service). This applies only to WMI namespaces that grant access to the user.
Inherited user rights:
Access this computer from the network
Add workstations to domain
Bypass traverse checking
Increase a process working set

Creating Groups and adding users

Using the Active Directory Users and Computers Tool



Name	Type
Administrator	User
Allowed RO...	Security Gı
Cert Publish...	Security Gı
Cloneable D...	Security Gı
Denied ROD...	Security Gı
DnsAdmins	Security Gı
DnsUpdateP...	Security Gı
Domain Ad...	Security Gı
Domain Co...	Security Gı
Domain Con...	Security Gı



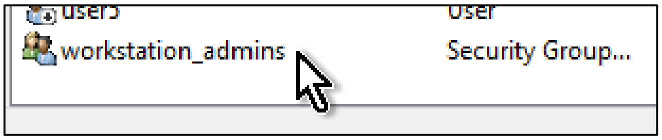
Create in: mycompany.com/Users

Group name:
workstation_admins

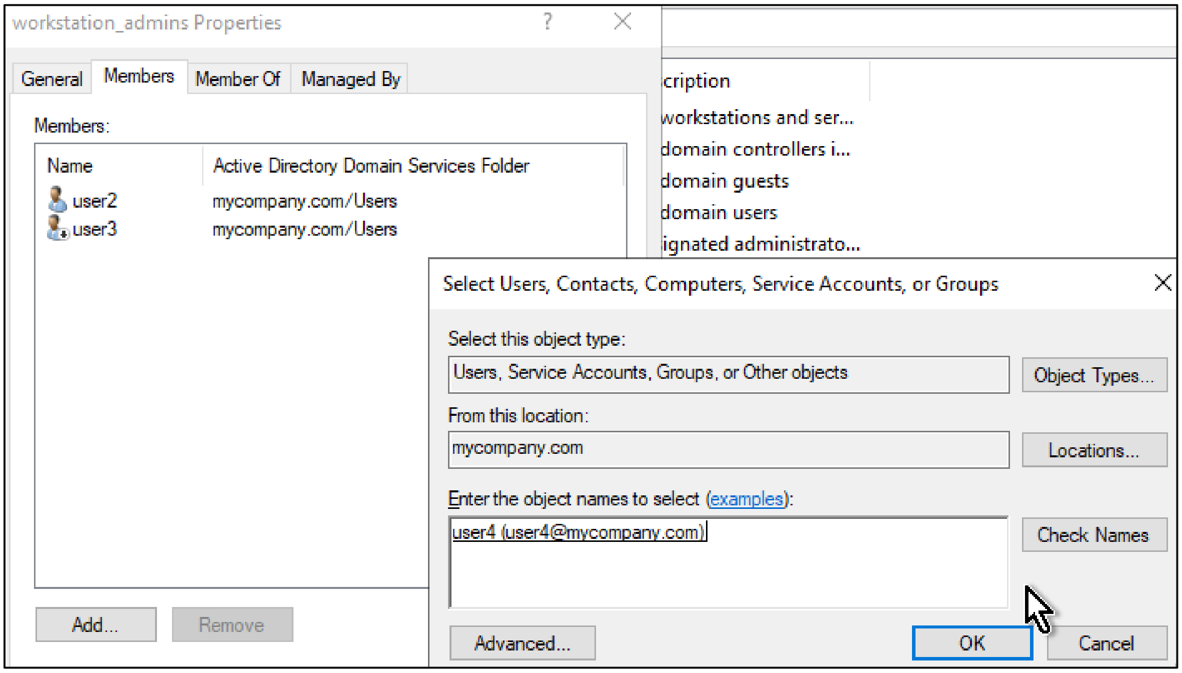
Group name (pre-Windows 2000):
workstation_admins

Group scope
○ Domain local
● Global
○ Universal

Group type
● Security
○ Distribution



user3	User
workstation_admins	Security Group...



Members:

Name	Active Directory Domain Services Folder
user2	mycompany.com/Users
user3	mycompany.com/Users

cription
workstations and ser...
domain controllers i...
domain guests
domain users
ignated administrato...

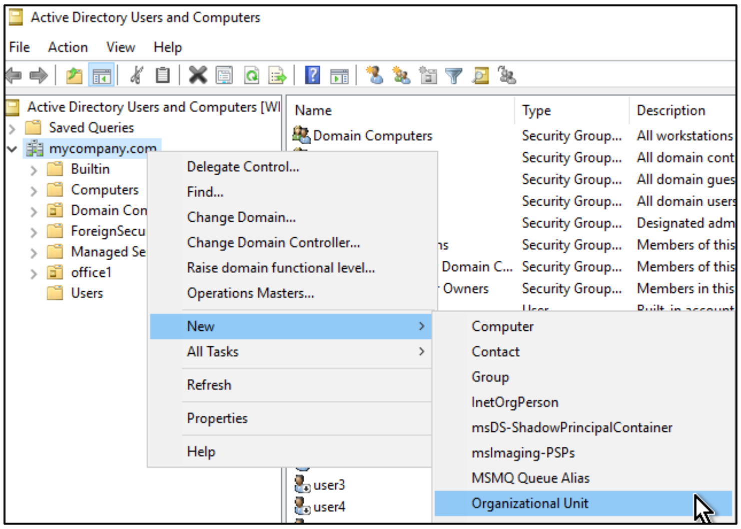
Select this object type:
Users, Service Accounts, Groups, or Other objects

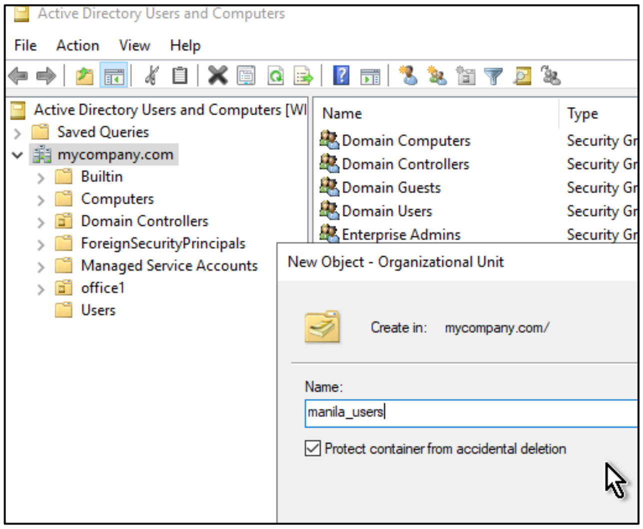
From this location:
mycompany.com

Enter the object names to select (examples):
user4 (user4@mycompany.com)

Creating organizational units

Using the Active Directory Users and Computers Tool





New Object - Organizational Unit

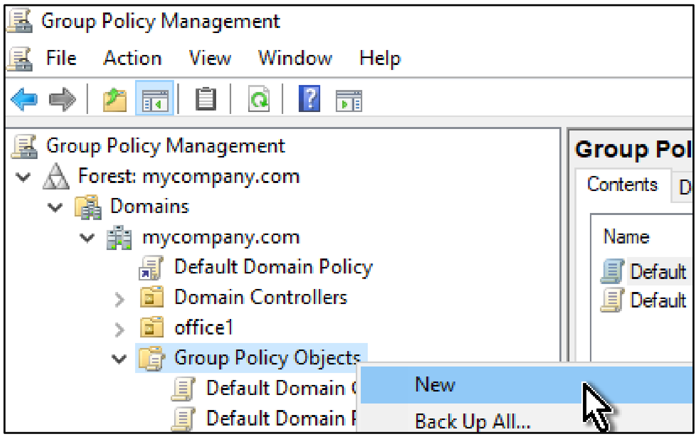
Create in: mycompany.com/

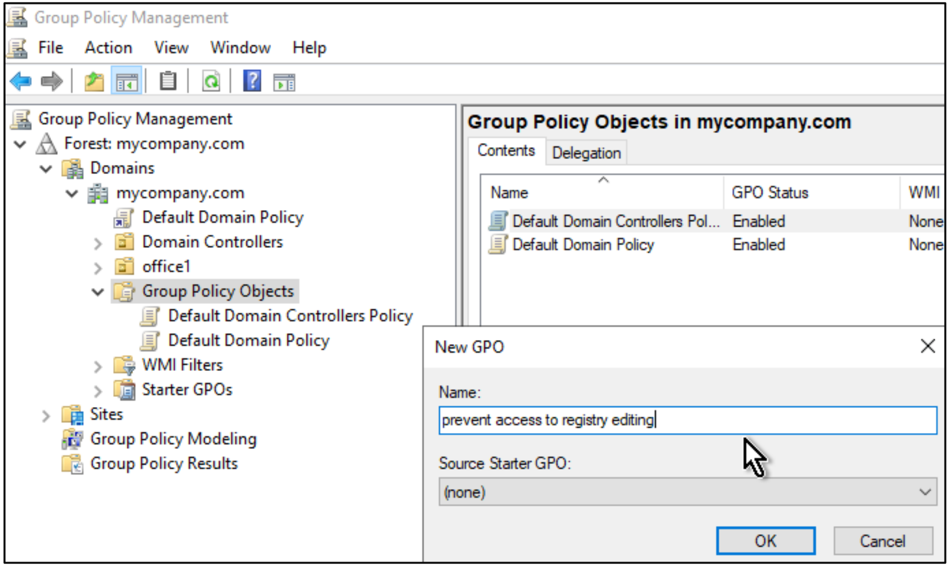
Name: manila_users

☑ Protect container from accidental deletion

Implement Group Policy Management

1. Group policies can be linked to OUs, so plan your OU hierarchy
2. Using the group policy management tool



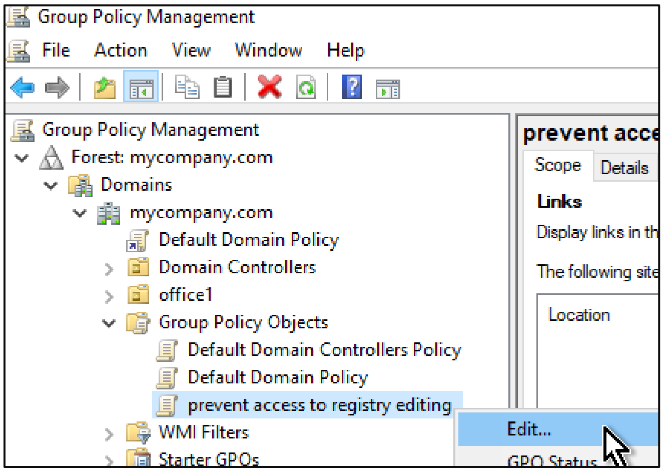


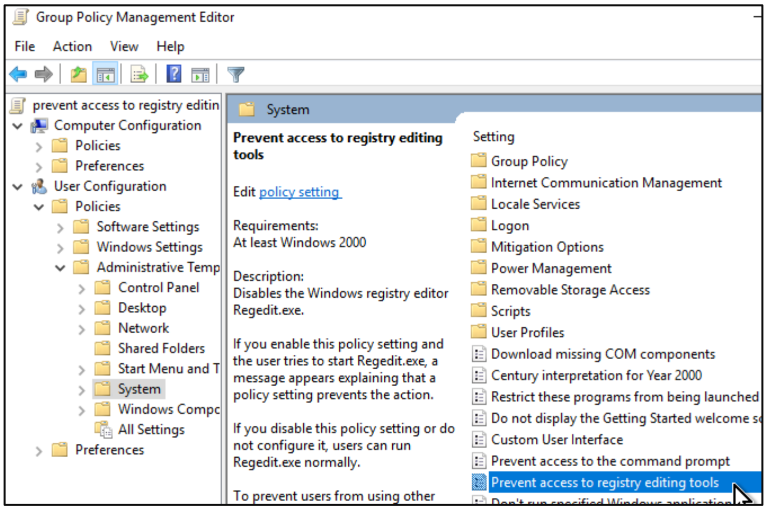
Name	GPO Status	WMI
Default Domain Controllers Pol...	Enabled	None
Default Domain Policy	Enabled	None

New GPO

Name: prevent access to registry editing

Source Starter GPO: (none)





Prevent access to registry editing tools

Edit policy setting

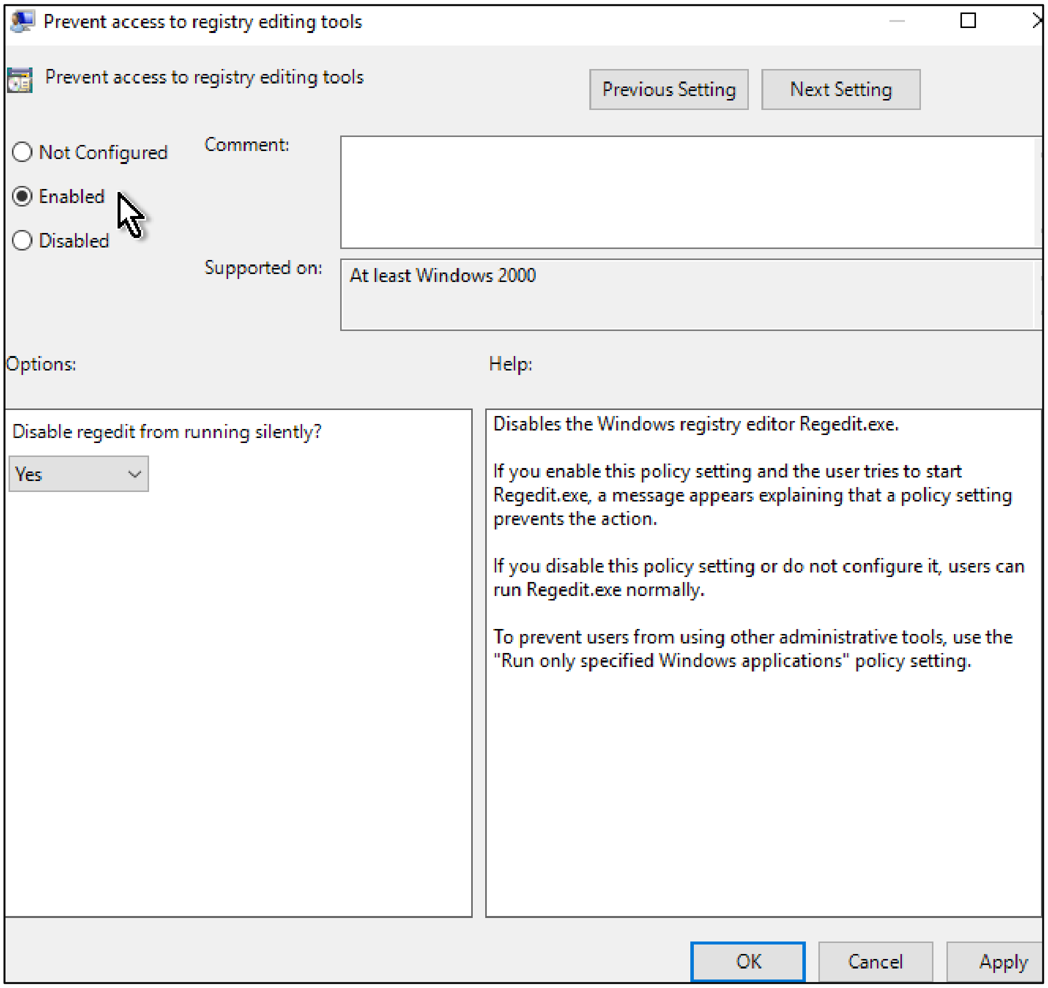
Requirements:
At least Windows 2000

Description:
Disables the Windows registry editor Regedit.exe.

If you enable this policy setting and the user tries to start Regedit.exe, a message appears explaining that a policy setting prevents the action.

If you disable this policy setting or do not configure it, users can run Regedit.exe normally.

To prevent users from using other


Prevent access to registry editing tools
Prevent access to registry editing tools
Previous Setting
Next Setting
Options:
Help:
OK
Cancel
Apply

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows 2000

Disable regedit from running silently? Yes

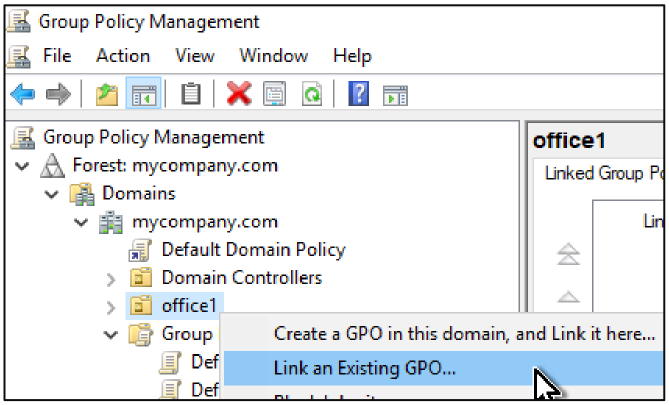
Disables the Windows registry editor Regedit.exe.

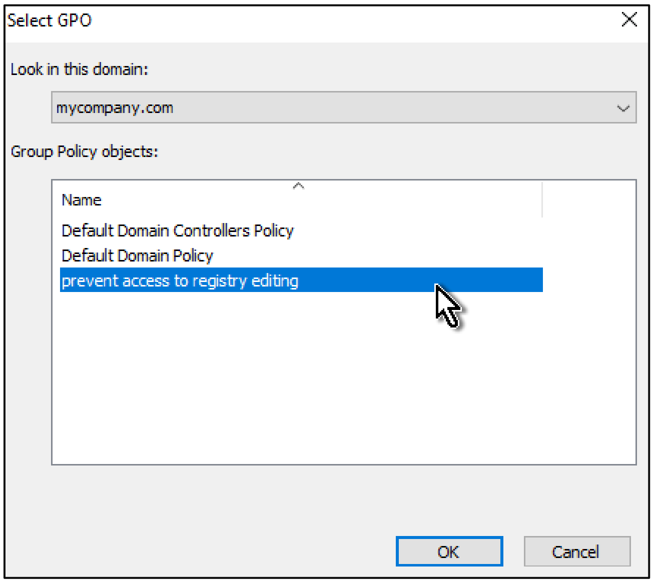
If you enable this policy setting and the user tries to start Regedit.exe, a message appears explaining that a policy setting prevents the action.

If you disable this policy setting or do not configure it, users can run Regedit.exe normally.

To prevent users from using other administrative tools, use the "Run only specified Windows applications" policy setting.

After creating and setting GPO, do not forget to link it to OU




Select GPO

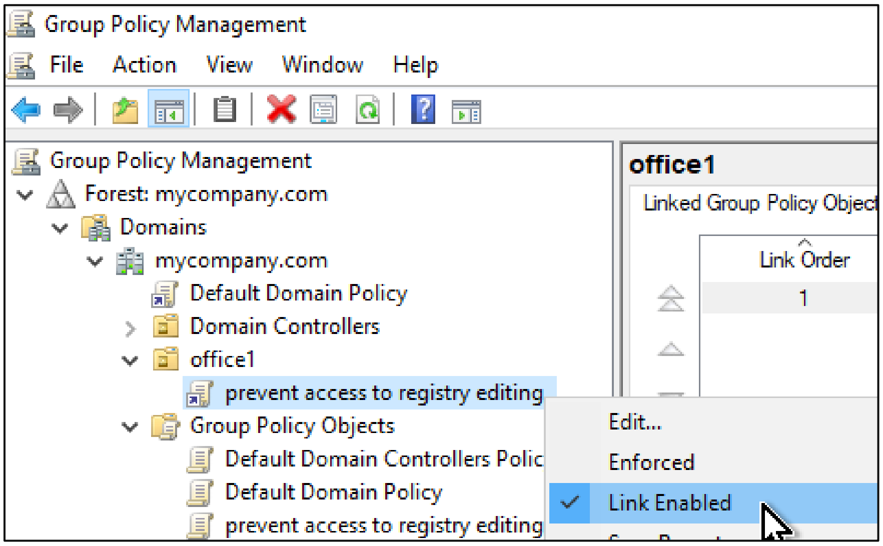
Look in this domain: mycompany.com

Group Policy objects:

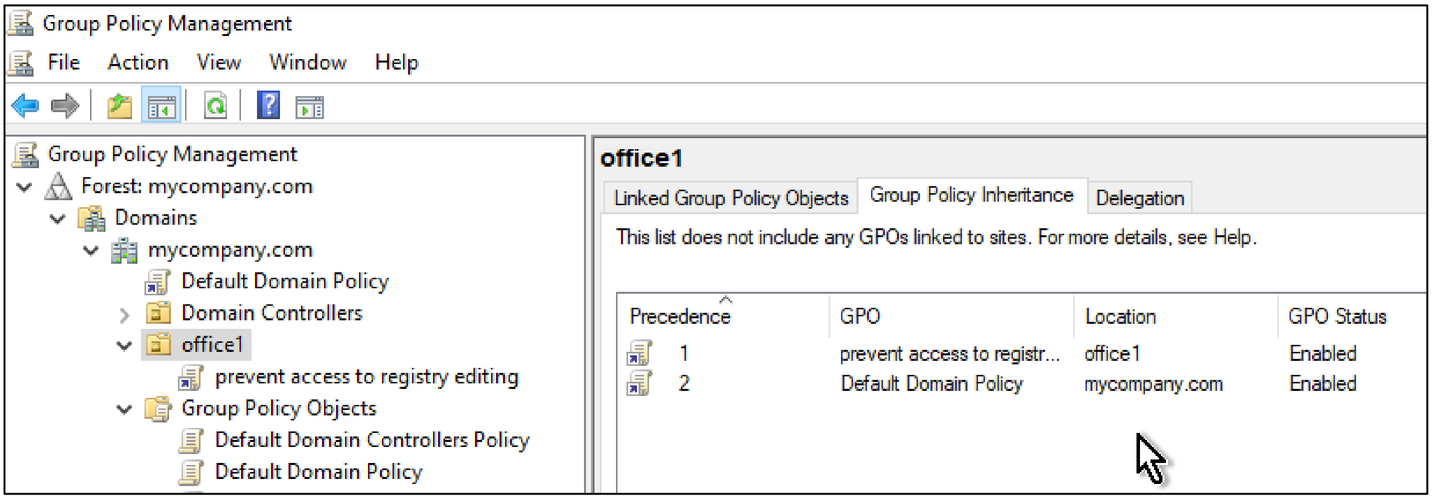
Name
Default Domain Controllers Policy
Default Domain Policy
prevent access to registry editing

Administrate Group Policy Management

- Check for the status and applied policy settings in a GP object (click on the policy then Settings tab)
- Group policies include lots of user logon restrictions for enhanced security
  gp policy→computer conf→windows settings→security settings→local policies→security options→ samples: rename local admin, disable/enable local admin, force logoff on logon hours, and interactive logon policies.
- Enable / disable policies



- Inheritance and precedence (link order)



- Group Policy Management
  - Forest: mycompany.com
    - Domains
      - mycompany.com
        - Default Domain Policy
        - Domain Controllers
        - office1
          - prevent access to registry editing
        - Group Policy Objects
          - Default Domain Controllers Policy
          - Default Domain Policy

office1

This list does not include any GPOs linked to sites. For more details, see Help.

Precedence	GPO	Location	GPO Status
1	prevent access to registr...	office1	Enabled
2	Default Domain Policy	mycompany.com	Enabled

- GPO scope
  - Gpo link (maximum scope)
  - Security filters (specify a user or group to which the GPO should or should not apply
  - Windows management instrumentation (wmi) filters → set specifications or characteristics of system.
- Group policy refresh
  - Auto every startup /logon and every 90-120minutes
  - Cmd→ gpupdate, gpupdate /force, /target:user, /target:computer, /logoff, /boot
- Software deployment using group policy (assign and publish)
- Group policy copy-paste, backup-restore-import, and save report
- Creating a group policy central store (policies will come from a central location instead from the local workstations.
  - Create a folder in \\fqdn\sysvol\fqdn\policies\ named="PolicyDefinitions"
  - Go to %systemroot%\windows\PolicyDefinitions and copy everything to YOUR "PolicyDefinitions folder
  - Verify administrative template source by hovering your pointer on it while setting a group policy.
- Gpotool.exe can be downloaded to troubleshoot group policy issues.
- Using Resultant Set of Policy (RSOP)
  - Enable inbound connections for remote administration for clients (comp.config→policies→admin templates→network→network connections→windows firewall→domain profile folder (window firewall:allow inbound remote administration exception)
  - R.click group policy result→wizard→select pc→view result
  - Cmd→gpresult /v or /z or /s [remote pc name] or /scope [user|computer]

Managing the DNS Role

DNS Server Any computer providing domain name services is a DNS name server. No matter where the server resides in the DNS namespace, it's still a DNS name server. For example, 13 root name servers at the top of the DNS tree are responsible for delegating the TLDs. The root servers provide referrals to name servers for the TLDs, which in turn provide referrals to an authoritative name server for a given domain.

Any DNS server implementation supporting Service Location Resource Records (see RFC 2782) and Dynamic Updates (RFC 2136) is sufficient to provide the name service for any operating system running Windows 2003 software and newer.

DNS Client A DNS client is any machine that issues queries to a DNS server. The client hostname may or may not be registered in a DNS database. Clients issue DNS requests through processes called resolvers. You'll sometimes see the terms client and resolver used synonymously.

Resolver Resolvers are software processes, sometimes implemented in software libraries that handle the actual process of finding the answers to queries for DNS data. The resolver is also built into many larger pieces of software so that external libraries don't have to

be called to make and process DNS queries. Resolvers can be what you'd consider client computers or other DNS servers attempting to resolve an answer on behalf of a client (for example, Internet Explorer).

Query A query is a request for information sent to a DNS server. Three types of queries can be made to a DNS server: recursive, inverse, and iterative. I'll discuss the differences between these query types in the section "DNS Queries," a bit later in the Module.

Understanding the DNS Process

Dynamic DNS and Non-Dynamic DNS

To understand Dynamic DNS and Non-Dynamic DNS, you must go back in time. (Here is where the TV screen always used to get wavy.) Many years ago when many of us worked on Windows NT 3.51 and Windows NT 4.0, almost all Microsoft networks used Windows Internet Name Service (WINS) to do their TCP/IP name resolution. Windows versions 95/98 and NT 4.0 Professional were all built on the idea of using WINS. This worked out well for administrators because WINS was dynamic (which meant that once it was installed, it automatically built its own database). Back then, there was no such thing as Dynamic DNS; administrators had to enter DNS records into the server manually. This is important to know even today. If you have clients still running any of these older operating systems (95/98 or NT 4), these clients cannot use Dynamic DNS.

Now let's move forward in time to the release of Windows Server 2000. Microsoft announced that DNS was going to be the name resolution method of choice. Many administrators (myself included) did not look forward to the switch. Because there was no such thing as Dynamic DNS, most administrators had nightmares about manually entering records. However, luckily for us, when Microsoft released Windows Server 2000, DNS had the ability to operate dynamically. Now when you're setting up Windows Server 2019 DNS, you can choose what type of dynamic update you would like to use, if any. Let's talk about why you would want to choose one over the other.

The Dynamic DNS (DDNS) standard, described in RFC 2136, allows DNS clients to update information in the DNS database files. For example, a Windows Server 2019 DHCP server can automatically tell a DDNS server which IP addresses it has assigned to what machines. Windows 2000, 2003, 2008, XP Pro, Vista, Windows 7, and Windows 8 DHCP clients can do this too. For security reasons, however, it's better to let the DHCP server do it. The result: IP addresses and DNS records stay in sync so that you can use DNS and DHCP together seamlessly. Because DDNS is a proposed Internet standard, you can even use the Windows Server 2019 DDNS-aware parts with Unix/Linux-based DNS servers.

Non-Dynamic DNS (NDDNS) does not automatically populate the DNS database. The client systems do not have the ability to update to DNS. If you decide to use Non-Dynamic DNS, an administrator will need to populate the DNS database manually. Non-Dynamic DNS is a reasonable choice if your organization is small to midsized and you do not

want extra network traffic (clients updating to the DNS server) or if you need to enter the computer's TCP/IP information manually because of strict security measures.

The major downside to entering records into DNS manually occurs when the organization is using the Dynamic Host Configuration Protocol (DHCP). When using DHCP, it is possible for users to end up with different TCP/IP addresses every day. This means an administrator has to update DNS manually each day to keep it accurate.

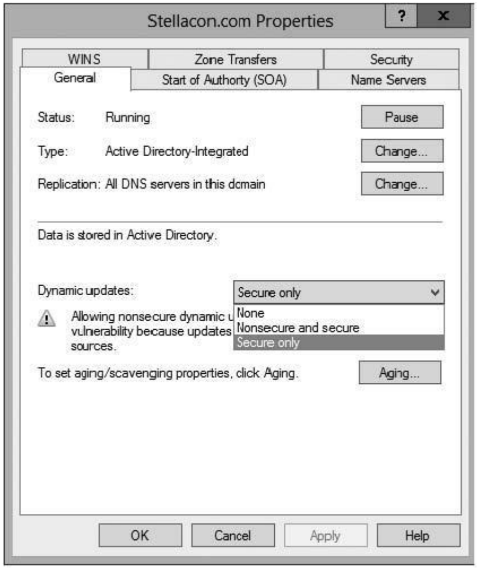
If you choose to allow Dynamic DNS, you need to decide how you want to set it up. When setting up dynamic updates on your DNS server, you have three choices

None This means your DNS server is Non-Dynamic.

Nonsecure and Secure This means that any machine (even if it does not have a domain account) can register with DNS. Using this setting could allow rogue systems to enter records into your DNS server.

Secure Only This means that only machines with accounts in Active Directory can register with DNS. Before DNS registers any account in its database, it checks Active Directory to make sure that account is an authorized domain computer.

FIGURE 2.3 Setting the Dynamic Updates option



Status: Running

Type: Active Directory-Integrated

Replication: All DNS servers in this dcmain

Data is stored in Active Directory.

Dynamic updates: Secure only

⚠ Allowing nonsecure dynamic u vulnerability because updates sources.

To set aging/scavenging properties, click Aging.

Introducing DNS Database Zones

As mentioned earlier in this Module, a DNS zone is a portion of the DNS namespace over which a specific DNS server has authority. Within a given DNS zone, there are resource records (RRs) that define the hosts and other types of information that make up the database for the zone. You can choose from several different zone types. Understanding the characteristics of each will help you choose which is right for your organization.

Understanding Primary Zones

When you're learning about zone types, things can get a bit confusing. But it's really not difficult to understand how they work and why you would want to choose one type of zone over the other. Zones are databases that store records. By choosing one zone type over another, you are basically just choosing how the database works and how it will be stored on the server.

The primary zone is responsible for maintaining all of the records for the DNS zone. It contains the primary copy of the DNS database. All record updates occur on the primary zone. You will want to create and add primary zones whenever you create a new DNS domain.

There are two types of primary zones:

- Primary zone
- Primary zone with Active Directory Integration (Active Directory DNS)

To install DNS as a primary zone, you must first install DNS using the Server Manager MMC. Once DNS is installed and running, you create a new zone and specify it as a primary zone.

Primary zones have advantages and disadvantages. Knowing the characteristics of a primary zone will help you decide when you need the zone and when it fits into your organization.

Local Database

Primary DNS zones get stored locally in a file (with the suffix .dns) on the server. This allows you to store a primary zone on a domain controller or a member server. In addition, by loading DNS onto a member server, you can help a small organization conserve resources. Such an organization may not have the resources to load DNS on an Active Directory domain controller.

Understanding Secondary Zones

In Windows Server 2019 DNS, you have the ability to use secondary DNS zones. Secondary zones are non-editable copies of the DNS database. You use them for load balancing (also referred to as load sharing), which is a way of managing network overloads on a single server. A secondary zone gets its database from a primary zone.

A secondary zone contains a database with all of the same information as the primary zone, and it can be used to resolve DNS requests. Secondary zones have the following advantages:

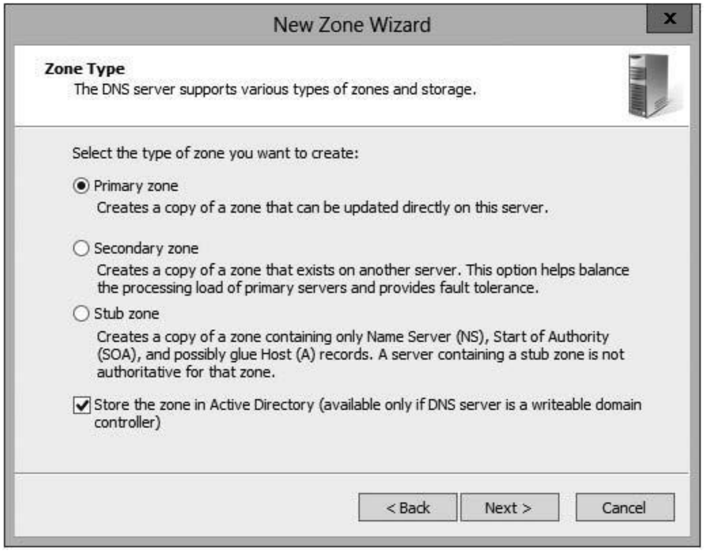
- A secondary zone provides fault tolerance, so if the primary zone server becomes unavailable, name resolution can still occur using the secondary zone server.
- Secondary DNS servers can also increase network performance by offloading some of the traffic that would otherwise go to the primary server.

Secondary servers are often placed within the parts of an organization that have high-speed network access. This prevents DNS queries from having to run across slow wide area network (WAN) connections. For example, if there are two remote offices within the stellacon.com organization, you may want to place a secondary DNS server in each remote office. This way, when clients require name resolution, they will contact the nearest server for this IP address information, thus preventing unnecessary WAN traffic.

Understanding Active Directory Integrated DNS

Windows Server 2000 introduced Active Directory Integrated DNS to the world. This zone type was unique and was a separate choice during setup. In Windows Server 2003, this zone type became an add-on to a primary zone. In Windows Server 2019, it works the same way. After choosing to set up a primary zone, you check the box labeled Store The Zone In Active Directory (see Figure 2.6).

FIGURE 2.6 Setting up an Active Directory Integrated zone



Zone Type

The DNS server supports various types of zones and storage.

Select the type of zone you want to create:

● Primary zone

Creates a copy of a zone that can be updated directly on this server.

○ Secondary zone

Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.

○ Stub zone

Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.

☑ Store the zone in Active Directory (available only if DNS server is a writeable domain controller)

Disadvantages of Active Directory Integrated DNS

The main disadvantage of Active Directory Integrated DNS is that it has to reside on a domain controller because the DNS database is stored in Active Directory. As a result, you cannot load this zone type on a member server, and small organizations might not have the resources to set up a dedicated domain controller.

Advantages of Active Directory Integrated DNS

The advantages of using an Active Directory Integrated DNS zone well outweigh the disadvantage just discussed. The following are some of the major advantages to an Active Directory Integrated zone:

Full Fault Tolerance Think of an Active Directory Integrated zone as a database on your server that stores contact information for all your clients. If you need to retrieve John Smith's phone number, as long as it was entered, you can look it up on the software.

If John Smith's phone number was stored only on your computer and your computer stopped working, no one could access John Smith's phone number. But since John Smith's phone number is stored in a database to which everyone has access, if your computer stops working, other users can still retrieve John Smith's phone number.

An Active Directory Integrated zone works the same way. Since the DNS database is stored in Active Directory, all Active Directory DNS servers can have access to the same data. If one server goes down or you lose a hard drive, all other Active Directory DNS servers can still retrieve DNS records.

No Additional Network Traffic As previously discussed, an Active Directory Integrated zone is stored in Active Directory. Since all records are now stored in Active Directory, when a resolver needs a TCP/IP address for Jsmith, any Active Directory DNS server can access Jsmith's address and respond to the resolver.

When you choose an Active Directory Integrated zone, DNS zone data can be replicated automatically to other DNS servers during the normal Active Directory replication process.

DNS Security An Active Directory Integrated zone has a few security advantages over a primary zone:

■ An Active Directory Integrated zone can use secure dynamic updates.

■ As explained earlier, the Dynamic DNS standard allows secure-only updates or dynamic updates, not both.

■ If you choose secure updates, then only machines with accounts in Active Direc-tory can register with DNS.
Before DNS registers any account in its database, it checks Active Directory to make sure that it is an authorized domain computer.

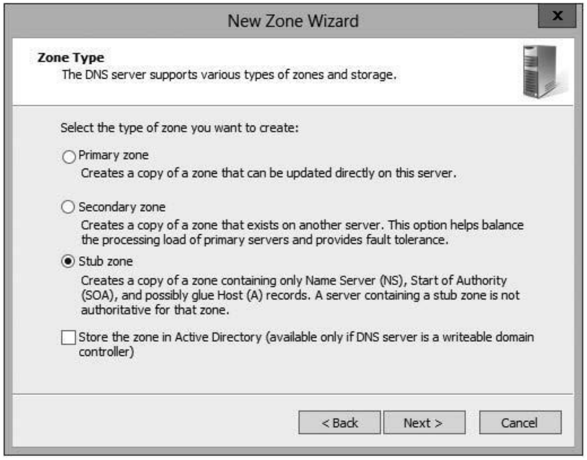
■ An Active Directory Integrated zone stores and replicates its database through Active Directory replication.
Because of this, the data gets encrypted as it is sent from one DNS server to another.

Background Zone Loading Background zone loading (discussed in more detail later in this Module) allows an Active Directory Integrated DNS zone to load in the background. As a result, a DNS server can service client requests while the zone is still loading into memory.

Understanding Stub Zones

Stub zones work a lot like secondary zones—the database is a non-editable copy of a primary zone. The difference is that the stub zone's database contains only the information necessary (three record types) to identify the authoritative DNS servers for a zone (see Figure 2.7). You should not use stub zones to replace secondary zones, nor should you use them for redundancy and load balancing.

FIGURE 2.7 DNS stub zone type



Zone Type
The DNS server supports various types of zones and storage.

Select the type of zone you want to create:

○ Primary zone
Creates a copy of a zone that can be updated directly on this server.

○ Secondary zone
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.

● Stub zone
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.

□ Store the zone in Active Directory (available only if DNS server is a writeable domain controller)

When to Use Stub Zones

Stub zones become particularly useful in a couple of different scenarios. Consider what happens when two large companies merge: example.com and example.net. In most cases, the DNS zone information from both companies must be available to every employee. You could set up a new zone on each side that acts as a secondary for the other side's primary zone, but administrators tend to be very protective of their DNS databases, and they probably wouldn't agree to this plan.

A better solution is to add to each side a stub zone that points to the primary server on the other side. When a client in example.com (which you help administer) makes a request for a name in example.net, the stub zone on the example.com DNS server would send the client to the primary DNS server for example.net without actually resolving the name. At this point, it would be up to example.net's primary server to resolve the name.

An added benefit is that, even if the administrators over at example.net change their configuration, you won't have to do anything because the changes will automatically rep-licate to the stub zone, just as they would for a secondary server.

Stub zones can also be useful when you administer two domains across a slow connec-tion. Let's change the previous example a bit and assume that you have full control over example.com and example.net but that they connect through a 56Kbps line. In this case, you wouldn't necessarily mind using secondary zones because you personally administer the entire network. However, it could get messy to replicate an entire zone file across that slow line. Instead, stub zones would refer clients to the appropriate primary server at the other site.

Setting up Basic File Server

Configuring File Servers

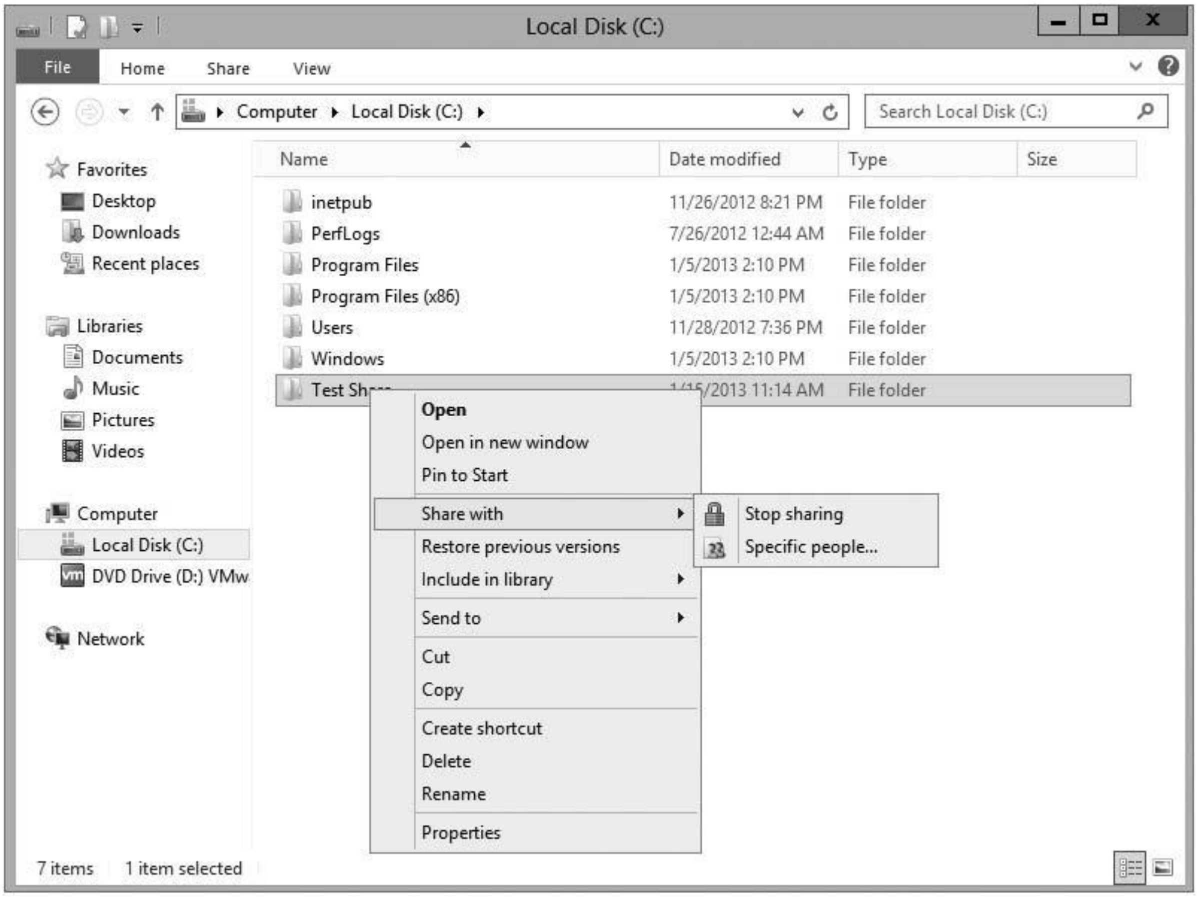
Now that you have an understanding of what a file server does, it's time to discuss how to configure these servers. Setting up a file server properly encompasses many steps. As always, one major concern is security. In the following sections, I will first describe how to share and publish online and offline files and folders. Then I will discuss the two types of security—shared permissions and NTFS security—that an administrator can set when sharing files or folders.

Sharing Folders

A file server is for sharing and storing data. To use one, you need to know how to set up a share, or a shared folder, on your server. A shared folder is exactly what it says; it's a folder that is shared on your network so that users can access the data within that folder. As an administrator, you have the ability to determine which users can access which files within a shared folder.

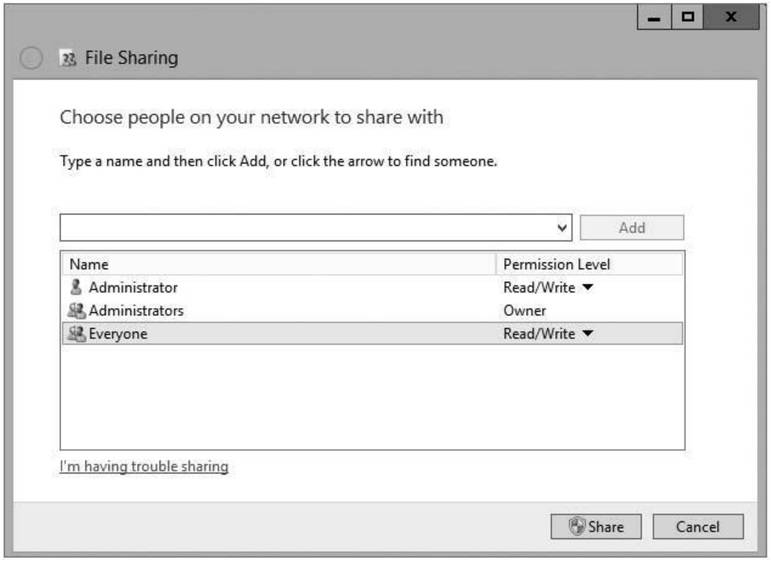
Creating and Publishing a Shared Work Folder

1. Create a new folder in the root directory of your C: partition, and name it Test Share.
2. Right-click the Test Share folder, and choose Share With ➢ Specific People.



Name	Date modified	Type	Size
inetpub	11/26/2012 8:21 PM	File folder	
PerfLogs	7/26/2012 12:44 AM	File folder	
Program Files	1/5/2013 2:10 PM	File folder	
Program Files (x86)	1/5/2013 2:10 PM	File folder	
Users	11/28/2012 7:36 PM	File folder	
Windows	1/5/2013 2:10 PM	File folder	
Test Sh	/2013 11:14 AM	File folder	

3. In the File Sharing dialog box, enter the names of users with whom you want to share this folder. In the upper box, enter Everyone and then click Add. Note that Everyone appears in the lower box. Click in the Permission Level column next to Everyone, and choose Read/Write from the drop-down menu. Then click Share.

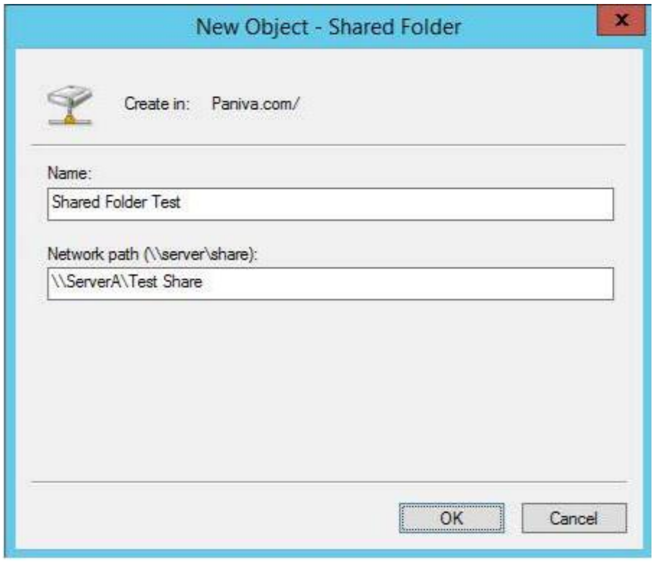


Choose people on your network to share with

Type a name and then click Add, or click the arrow to find someone.

Name	Permission Level
Administrator	Read/Write ▾
Administrators	Owner
Everyone	Read/Write ▾

4. You see a message that your folder has been shared. Click Done.
5. Open the Active Directory Users and Computers tool. Expand the current domain. Select New ➢ Shared Folder.
6. In the New Object – Shared Folder dialog box, type Shared Folder Test for the name of the folder. Then type the UNC path to the share (for example, \\serverA\Test Share). Click OK to create the share.



New Object - Shared Folder

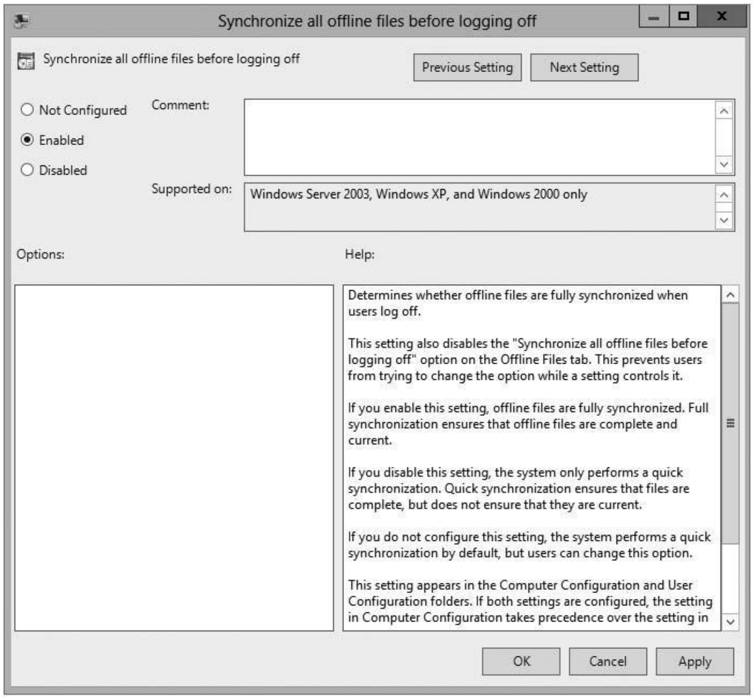
Create in: Paniva.com/

Name:
Shared Folder Test

Network path (\\server\share):
\\ServerA\Test Share

Configuring Offline Folder Options

1. Open the Group Policy Management Console.
2. In the left pane, expand your forest and then your domain. Under your domain name, there should be a default domain policy.
3. Right-click the default domain policy and choose Edit.
4. In the User Configuration section, expand Policies ➢ Administrative Templates ➢ -Network and then click Offline Files.
5. Right-click Synchronize All Offline Files Before Logging Off and choose Edit. The GPO setting dialog box appears. Choose the Enabled option and click OK.



Synchronize all offline files before logging off

Synchronize all offline files before logging off

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: Windows Server 2003, Windows XP, and Windows 2000 only

Options:

Help:

Determines whether offline files are fully synchronized when users log off.

This setting also disables the "Synchronize all offline files before logging off" option on the Offline Files tab. This prevents users from trying to change the option while a setting controls it.

If you enable this setting, offline files are fully synchronized. Full synchronization ensures that offline files are complete and current.

If you disable this setting, the system only performs a quick synchronization. Quick synchronization ensures that files are complete, but does not ensure that they are current.

If you do not configure this setting, the system performs a quick synchronization by default, but users can change this option.

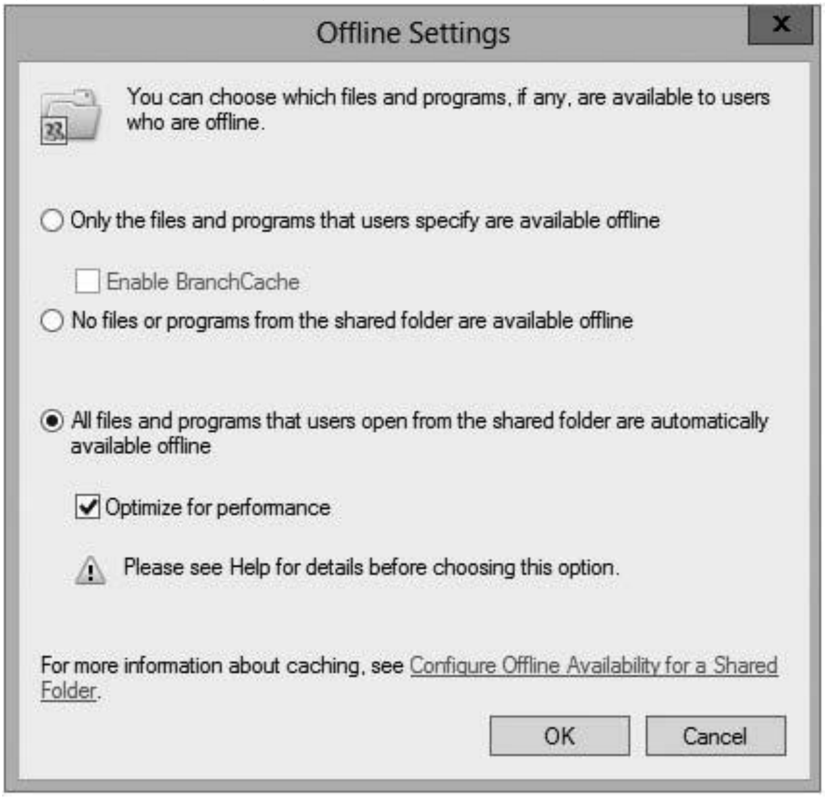
This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in

6. Right-click Synchronize All Offline Files When Logging On and choose Edit. The GPO setting dialog box appears. Choose the Enabled option and click OK.

7. Right-click Synchronize Offline Files Before Suspend and choose Edit. The GPO setting dialog box appears. Choose the Enabled option. In the Action drop-down box, make sure Quick is selected. Click OK.
8. Close the GPMC.

Configuring a Shared Network Folder for Offline Access

1. Right-click the Test Share folder that you created in Exercise 4.1 and choose Properties.
2. Click the Sharing tab and then click the Advanced Sharing button.
3. When the Advanced Sharing dialog box appears, click the Caching button.
4. When the Offline Settings dialog box appears, choose the All Files And Programs That Users Open From The Shares Will Be Automatically Available Offline option. Click OK.



You can choose which files and programs, if any, are available to users who are offline.

○ Only the files and programs that users specify are available offline

□ Enable BranchCache

○ No files or programs from the shared folder are available offline

● All files and programs that users open from the shared folder are automatically available offline

☑ Optimize for performance

⚠ Please see Help for details before choosing this option.

For more information about caching, see Configure Offline Availability for a Shared Folder.

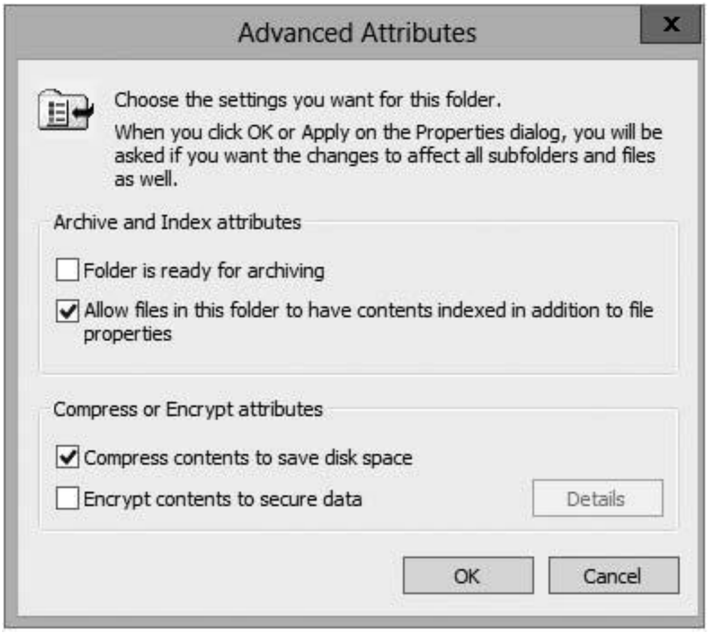
5. Click OK twice more to close the Properties dialog box.

Configuring Permissions

You have gone through the steps necessary to set up a shared folder, publish it to Active Directory, and set it up for offline access. Now you will see how you can protect these files and folders by using permissions.

You can secure folders using permissions in two ways, and you can secure files in one way. You can set up permissions and security through NTFS or through sharing.

Compression Compression helps compact files or folders to allow for more efficient use of hard drive space. For example, a file that usually takes up 20MB of space might use only 13MB after compression. To enable compression, just open the Advanced Attributes dialog box for a folder and check the Compress Contents To Save Disk Space box


Advanced Attributes

Choose the settings you want for this folder.

When you click OK or Apply on the Properties dialog, you will be asked if you want the changes to affect all subfolders and files as well.

Archive and Index attributes

□ Folder is ready for archiving

☑ Allow files in this folder to have contents indexed in addition to file properties

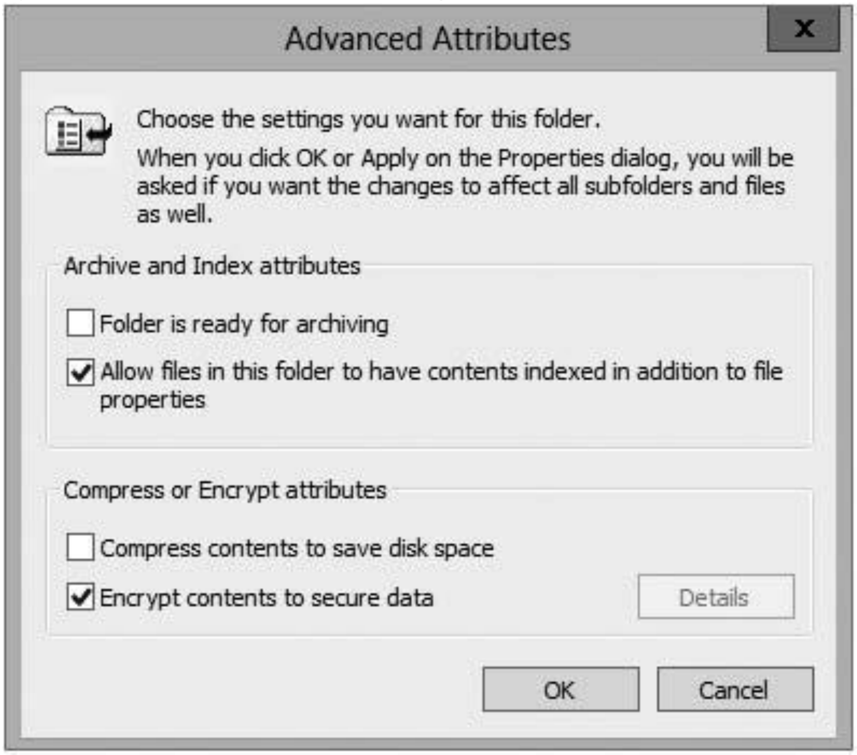
Compress or Encrypt attributes

☑ Compress contents to save disk space

□ Encrypt contents to secure data

Quotas Quotas allow you to limit how much hard drive space users can have on a server. Quotas are discussed in greater detail in the section “Configuring Disk Quotas.”

Encryption Encrypting File System (EFS) allows a user or administrator to secure files or folders by using encryption. Encryption employs the user’s security identification (SID) number to secure the file or folder. To implement encryption, open the Advanced Attributes- dialog box for a folder and check the Encrypt Contents To Secure Data box.


Advanced Attributes

Choose the settings you want for this folder.

When you click OK or Apply on the Properties dialog, you will be asked if you want the changes to affect all subfolders and files as well.

Archive and Index attributes

□ Folder is ready for archiving

☑ Allow files in this folder to have contents indexed in addition to file properties

Compress or Encrypt attributes

□ Compress contents to save disk space

☑ Encrypt contents to secure data

If files are encrypted using EFS and an administrator has to unencrypt the files, there are two ways to do this. First, you can log in using the user’s account (the account that encrypted the files) and unencrypt the files. Second, you can become a recovery agent and manually unencrypt the files.

Security One of the biggest advantages of NTFS is security. Security is one of the most important aspects of an IT administrator's job. An advantage of NTFS security is that the security can be placed on individual files and folders. It does not matter whether you are local to the share (in front of the machine where the data is stored) or remote to the share (coming across the network to access the data); the security is always in place with NTFS.

The default security permission is Users = Read on new folders or shares.

Configuring Shared and NTFS Settings

1. Right-click the Test Share folder you created and choose Properties.
2. Click the Sharing tab and then click the Advanced Sharing button. (You will set the shared permissions first.)
3. Click the Permissions button. Click the Add button. When the Select User page appears, choose a group from Active Directory. (I used the Sales group.) Once you find your group, click OK.
4. The Permissions dialog box appears. With your group highlighted, click the Allow check box next to Full Control and click OK. (All of the other Allow check boxes will -automatically become checked.)
5. On the Advanced Sharing page, click OK. Now click the Security tab. (This allows you to set the NTFS security settings.)
6. Click the Edit button. That takes you to the Permissions page. Now click the Add button. When the Select User page appears, choose a group from Active Directory. (I used the Everyone group.) Once you find your group, choose OK.
7. The Permissions dialog box appears. With your group highlighted, click the Allow check box next to Modify, and click OK. (All of the check boxes below Modify will -automatically become checked.)

8. Click Close.

Configuring Disk Quotas

1. Open Windows Explorer.
2. Right-click the local disk (C:) and choose Properties.
3. Click the Quotas tab.
4. Check the Enable Quota Management check box. Also check the Deny Disk Space To Users Exceeding Quota Limit box.
5. Click the Limit Disk Space To option and enter 1000MB in the box.
6. Enter 750MB in the Set Warning Level To boxes.
7. Click the Apply button. If a warning box appears, click OK. This warning is just informing you that the disk may need to be rescanned for the quota.
8. Now that you have set up an umbrella quota to cover everyone, you'll set up a quota that exceeds the umbrella. Click the Quota Entries button.
9. The Quotas Entries for (C:) window appears. You will see some users already listed. These are users who are already using space on the volume. Click the Quota menu at the top and choose New Quota Entry.
Notice the N/A entry in the Percent Used column. This belongs to the administrator account, which by default has no limit.
10. On the Select User page, choose a user that you want to allow to exceed the quota (for this example, I used the wpanek account). Click OK.
11. This opens the Add New Quota Entry dialog box. Click the Do Not Limit Disk Usage option and click OK.
12. You will notice that the new user has no limit. Close the disk quota tool.

Setting up and Administering Web Services

According to Microsoft Docs, the Web Server (IIS) role in Windows Server 2019 provides a secure, easy-to-manage, modular and extensible platform for reliably hosting websites, services, and applications. The new release of Windows Server 2019 from Microsoft comes with IIS version 10. This guide shows how it is installed and how various activities such as the creation of websites, Virtual directories, and others are tackled. We shall begin by installing IIS.

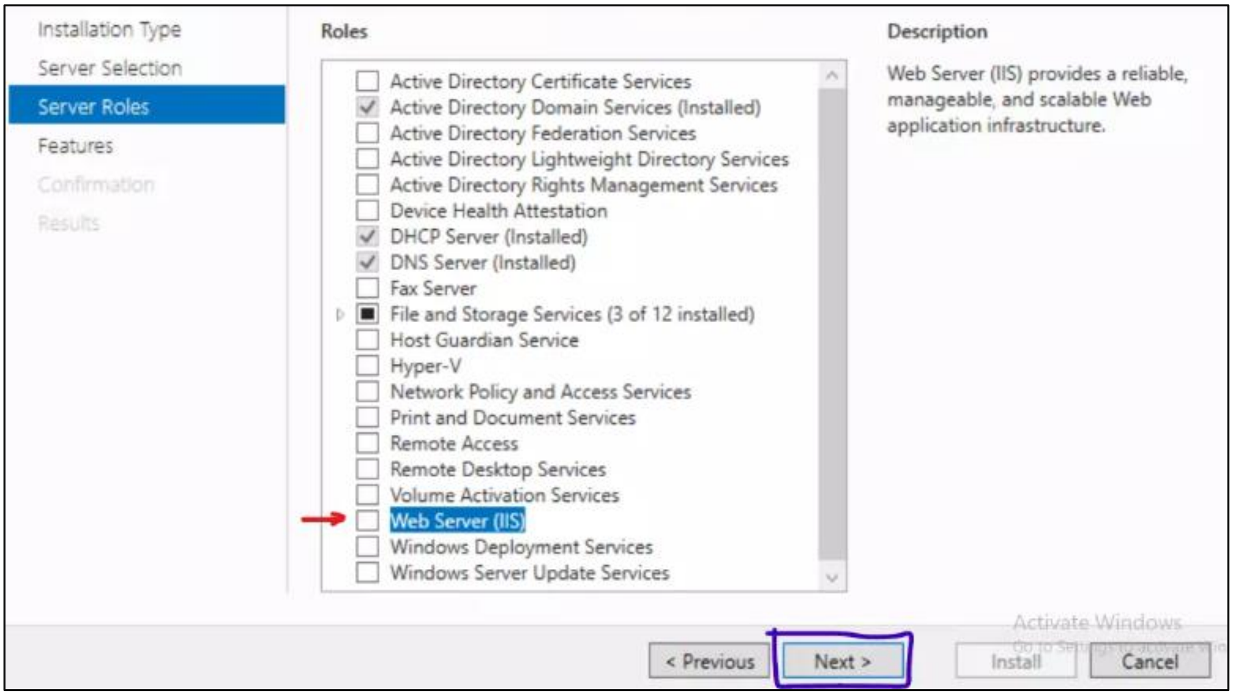
Step 1: Start Server Manager
As with all Windows Server roles, we have to go to the Server Manager to begin the installation. Hit your "Windows" key and search for Server Manager if it is not already opened. Once open, click on "Add Roles and Features"

Step 2: Click Next on Wizard
On the first page of the "Add Roles and Features Wizard", click "Next"

Step 3: Select Installation Type
In the "Select Installation type page", select "Role-based or feature-based-installation" and click "Next"

Step 4: Choose Destination Server
Select the server you will install NFS on and click "Next"

Step 5: Select Roles to install
In this "Select server roles" part check the "WebServer (IIS)" box then a pop-up window will come up.



Roles

- ☐ Active Directory Certificate Services
- ☑ Active Directory Domain Services (Installed)
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Device Health Attestation
- ☑ DHCP Server (Installed)
- ☑ DNS Server (Installed)
- ☐ Fax Server
- ■ File and Storage Services (3 of 12 installed)
- ☐ Host Guardian Service
- ☐ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services
- ☐ Volume Activation Services
- ☐ Web Server (IIS)
- ☐ Windows Deployment Services
- ☐ Windows Server Update Services

Description

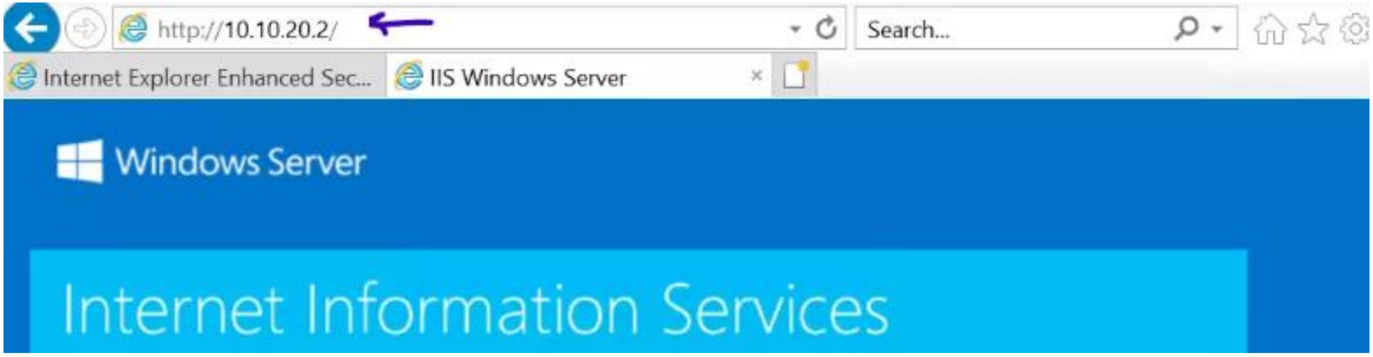
Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

Step 6: Add IIS Features
In the pop-up window, just click on "Add Features" then hit "Next".

Step 7: Confirm Selections
On the "Confirm installation selections" page simply click on "Install" and afford it some time to finish after which you just click "Close".

Step 8: Prove the Web Server is running

Open your browser either within the server or on a computer that can access your IIS Server network and input its IP Address on the browser's search as shown below. If it loads, then we are good to go.



http://10.10.20.2/

Search...
Internet Explorer Enhanced Sec...
IIS Windows Server
Windows Server
Internet Information Services

Setting up and Administering FTP Services

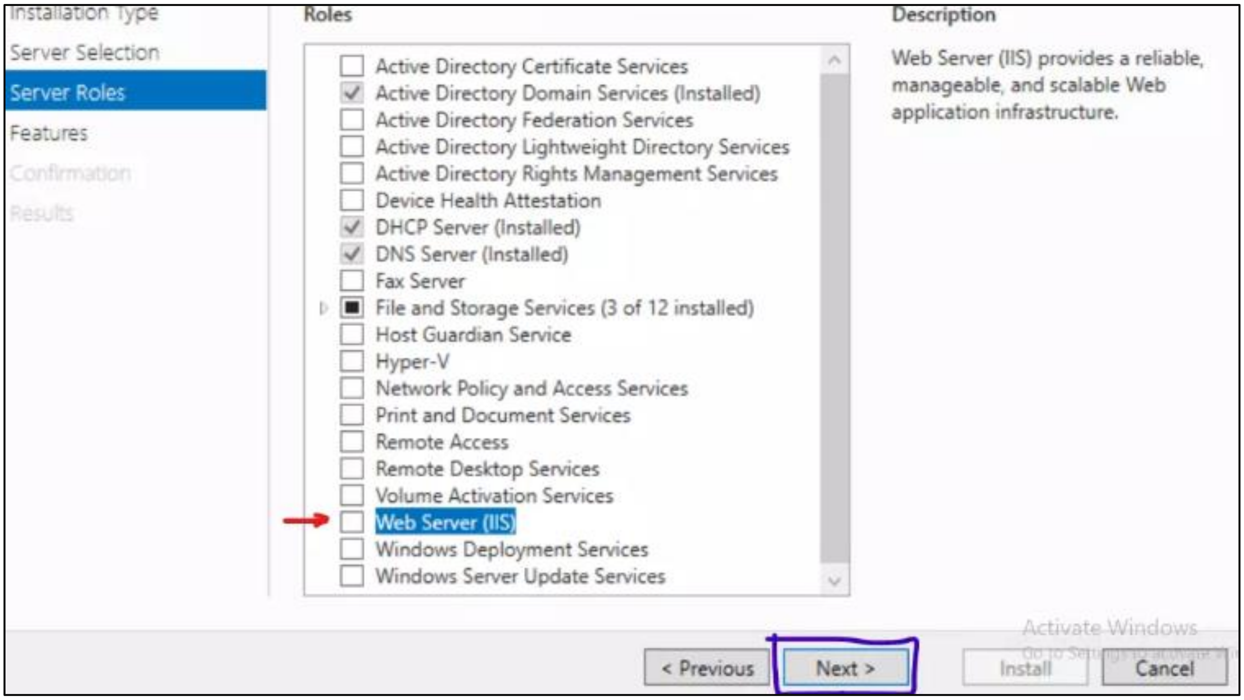
Step 1: Start Server Manager
As with all Windows Server roles, we have to go to the Server Manager to begin the installation. Hit your "Windows" key and search for "Server Manager" if it is not already opened. Once open, click on "Add Roles and Features"

Step 2: Click Next on Wizard
On the first page of the "Add Roles and Features Wizard", click "Next"

Step 3: Select Installation Type
In the "Select Installation type page", select "Role-based or feature-based-installation" and click "Next"

Step 4: Choose Destination Server
Select the server you will install NFS on and click "Next"

Step 5: Select Roles to install
Select "Web Server (IIS)" checkbox and click on "Add Features" in the pop-up that will come up as shown below. Click "Next" after that is done.



Roles

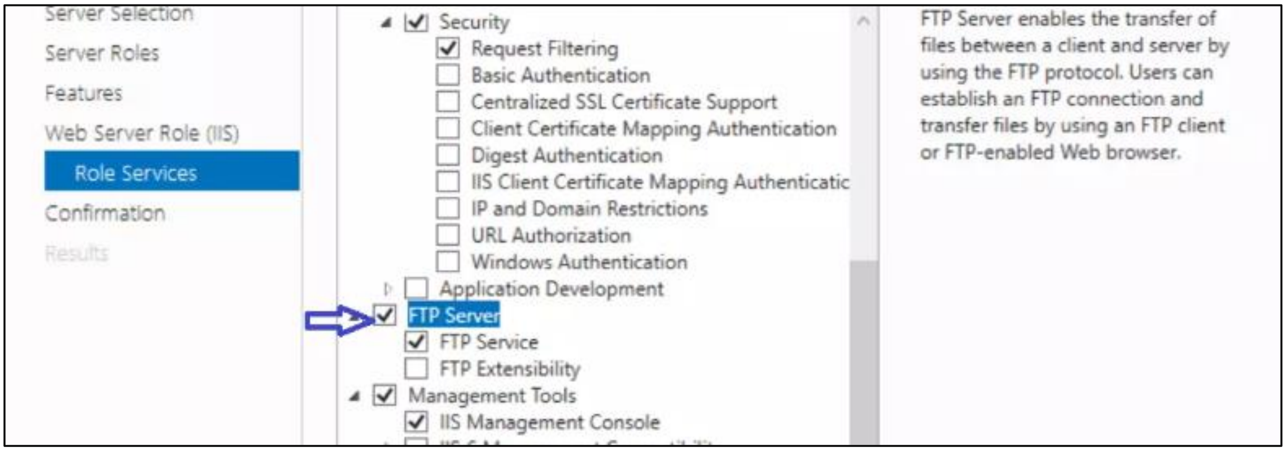
- ☐ Active Directory Certificate Services
- ☑ Active Directory Domain Services (Installed)
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Device Health Attestation
- ☑ DHCP Server (Installed)
- ☑ DNS Server (Installed)
- ☐ Fax Server
- ■ File and Storage Services (3 of 12 installed)
- ☐ Host Guardian Service
- ☐ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services
- ☐ Volume Activation Services
- ☐ Web Server (IIS)
- ☐ Windows Deployment Services
- ☐ Windows Server Update Services

Description

Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

Step 6: Select Features
In the “Select Features” stage simply click on “Next” and click on “Next” again in the “Web Server Role (IIS)” stage as well.

Step 7: Select role services
This is the step we have been waiting for. Among the many checkboxes, select “File Server ” one and hit “Next“. After that, happily click on “Install” and wait for your server to finish up installing.

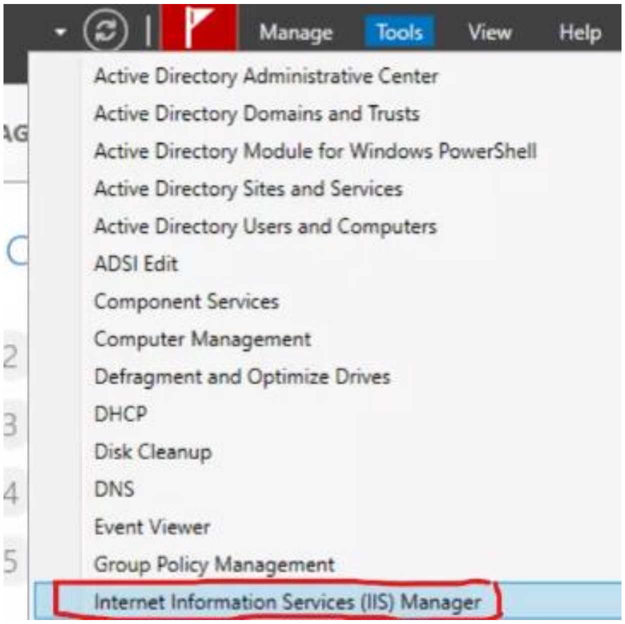


- ☑ Security
  - ☑ Request Filtering
  - ☐ Basic Authentication
  - ☐ Centralized SSL Certificate Support
  - ☐ Client Certificate Mapping Authentication
  - ☐ Digest Authentication
  - ☐ IIS Client Certificate Mapping Authenticatic
  - ☐ IP and Domain Restrictions
  - ☐ URL Authorization
  - ☐ Windows Authentication
- ☐ Application Development
- ☑ FTP Server
  - ☑ FTP Service
  - ☐ FTP Extensibility
- ☑ Management Tools
  - ☑ IIS Management Console

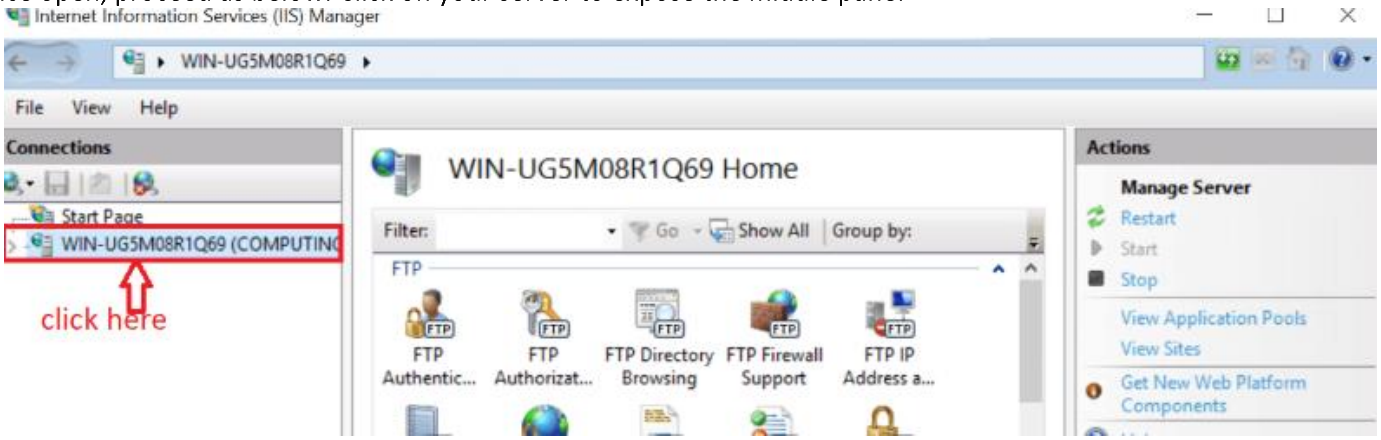
FTP Server enables the transfer of files between a client and server by using the FTP protocol. Users can establish an FTP connection and transfer files by using an FTP client or FTP-enabled Web browser.

Step 8: Configure your FTP in passive mode
Let us now configure our FTP Server in Passive Mode

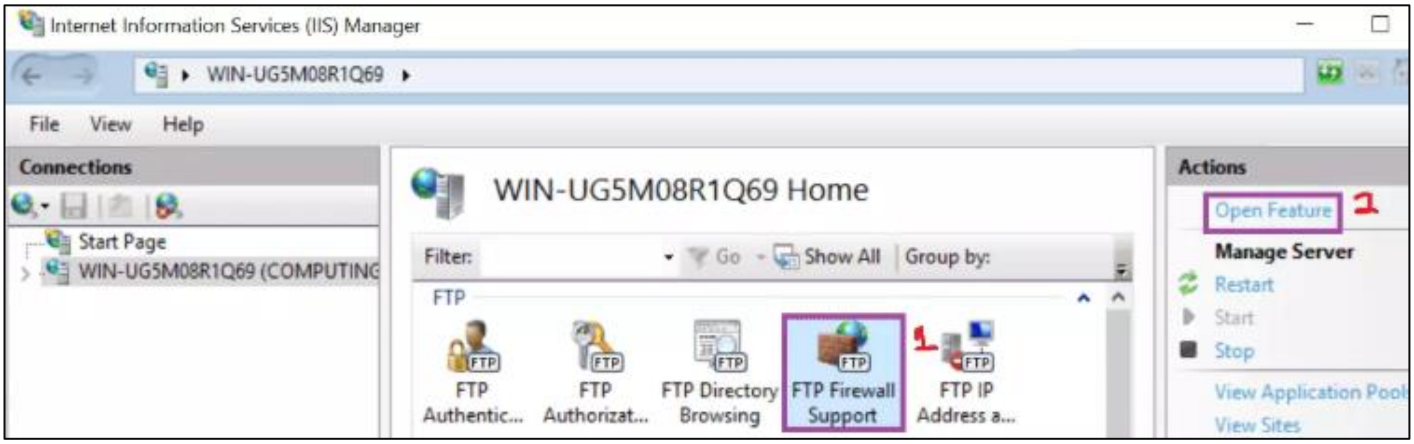
Open Server Manager >Tools > Internet Information Services (IIS) Manager


Manage
Tools
View
Help
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
DHCP
Disk Cleanup
DNS
Event Viewer
Group Policy Management
Internet Information Services (IIS) Manager

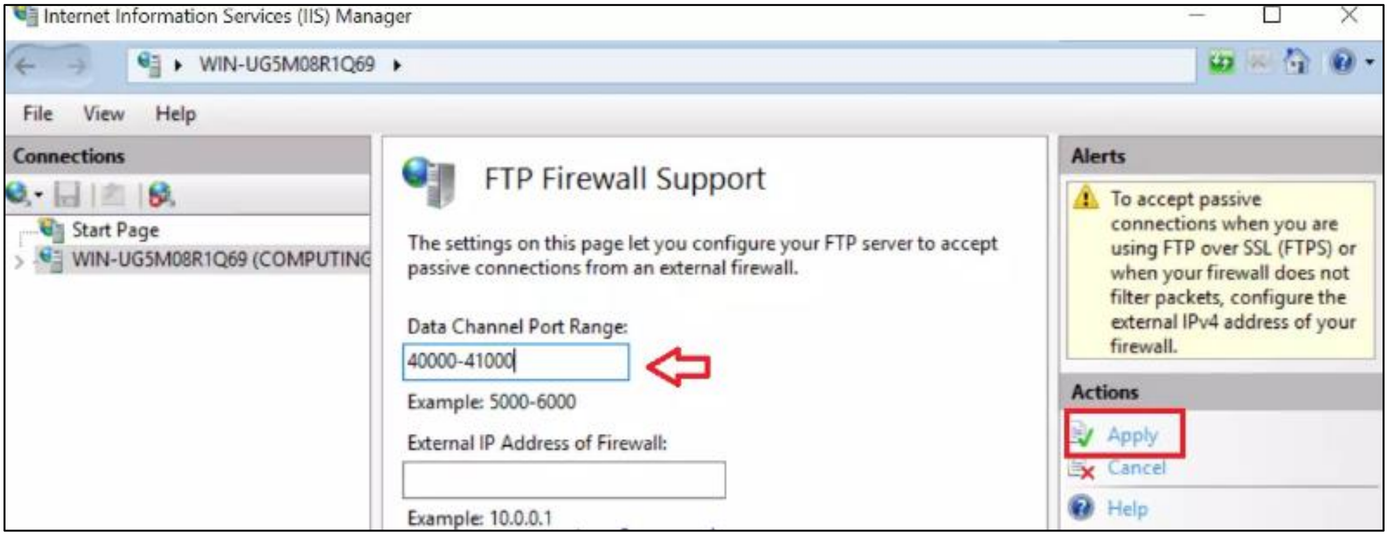
Once open, proceed as below. Click on your server to expose the middle pane.



Step 9: Open Feature
Select “FTP Firewall Support” and click on “Open Feature” on the right pane as illustrated. Alternatively, you can just double-click on “FTP Firewall Support“. That will open a small pop-up. Proceed to step 11.



Step 10: FTP Firewall Support
Input the port range for passive mode in this pop-up as shown below then click “Apply” on the right pane.



FTP Firewall Support

The settings on this page let you configure your FTP server to accept passive connections from an external firewall.

Data Channel Port Range: 40000-41000

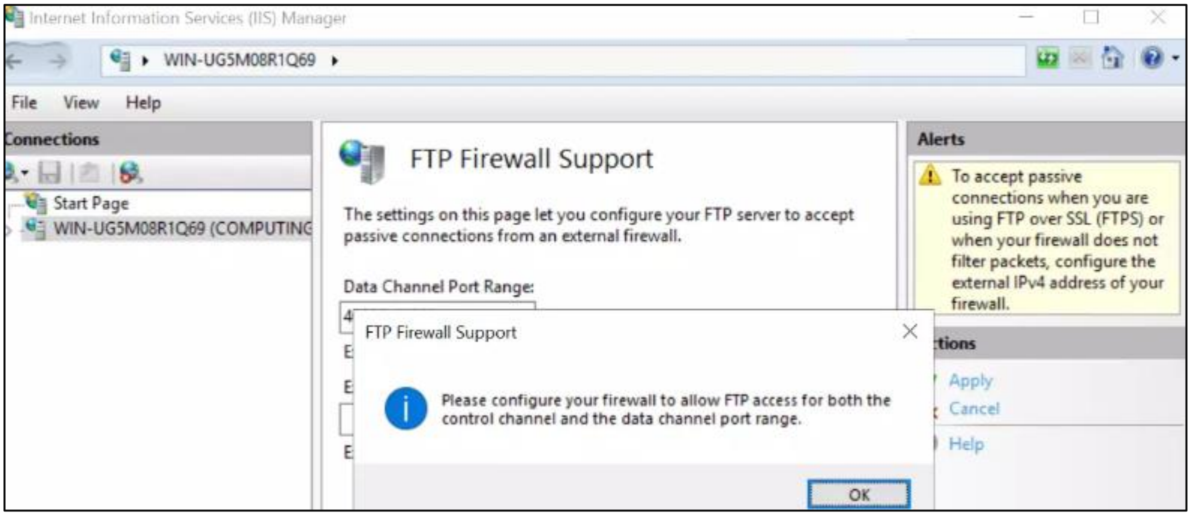
Example: 5000-6000

External IP Address of Firewall:

Example: 10.0.0.1

To accept passive connections when you are using FTP over SSL (FTPS) or when your firewall does not filter packets, configure the external IPv4 address of your firewall.

The pop-up below will appear making you aware that you need to allow the port range we configured in the firewall. Click “OK“. After that, restart, FTP Server to make the changes applied.



FTP Firewall Support

The settings on this page let you configure your FTP server to accept passive connections from an external firewall.

Data Channel Port Range:

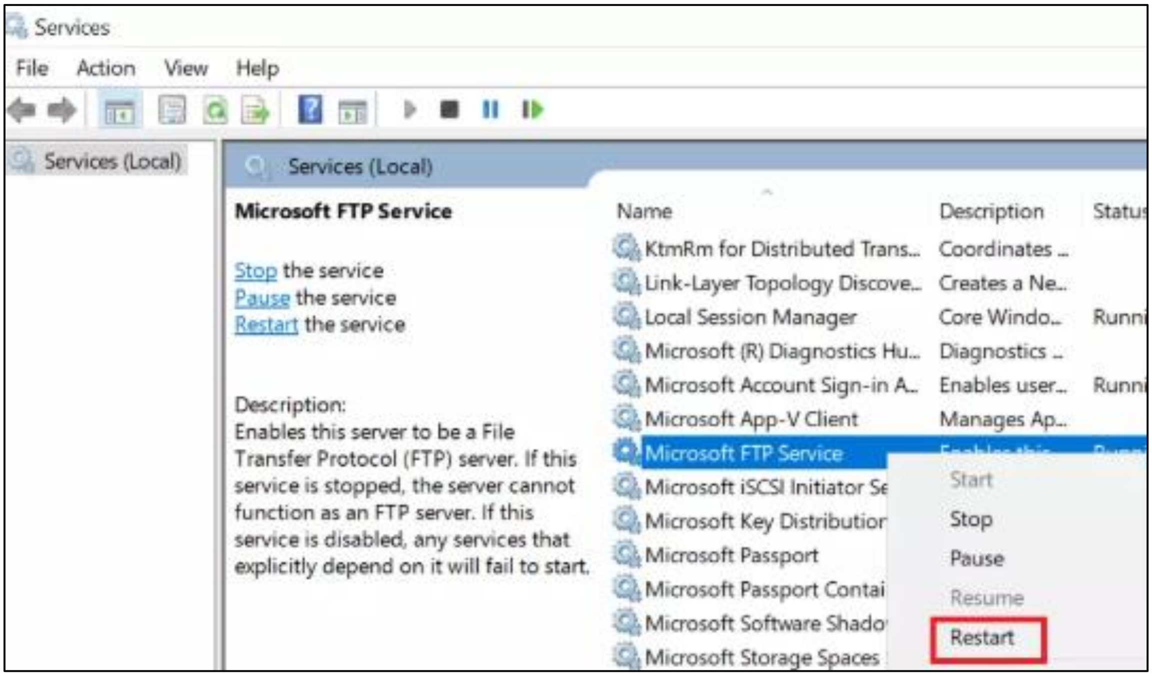
To accept passive connections when you are using FTP over SSL (FTPS) or when your firewall does not filter packets, configure the external IPv4 address of your firewall.

FTP Firewall Support

Please configure your firewall to allow FTP access for both the control channel and the data channel port range.

Step 11: Restart FTP Server

Open Services App, look for “Microsoft FTP Server“, right-click on it and select restart.



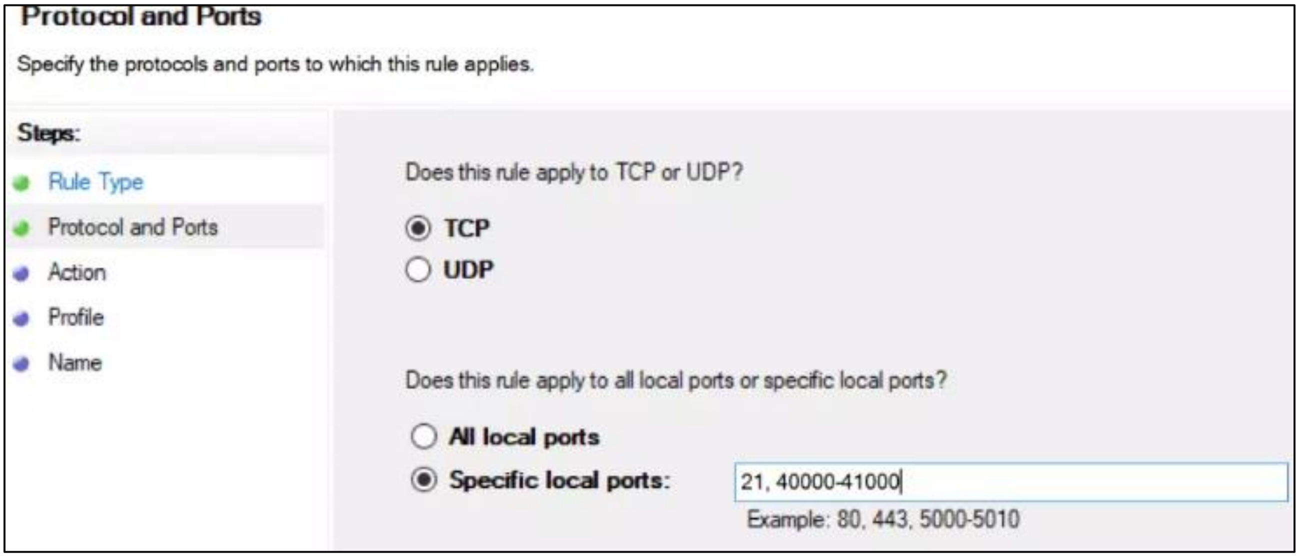
Microsoft FTP Service

Stop the service
Pause the service
Restart the service

Description:
Enables this server to be a File Transfer Protocol (FTP) server. If this service is stopped, the server cannot function as an FTP server. If this service is disabled, any services that explicitly depend on it will fail to start.

Name	Description	Status
KtmRm for Distributed Trans...	Coordinates ...	
Link-Layer Topology Discove...	Creates a Ne...	
Local Session Manager	Core Windo...	Runni
Microsoft (R) Diagnostics Hu...	Diagnostics ...	
Microsoft Account Sign-in A...	Enables user...	Runni
Microsoft App-V Client	Manages Ap...	
Microsoft FTP Service	Enables this...	Runni
Microsoft iSCSI Initiator Se		
Microsoft Key Distributior		
Microsoft Passport		
Microsoft Passport Contai		
Microsoft Software Shado		
Microsoft Storage Spaces		

Step 12: Add the ports in Firewall
Use How To open a port in Windows Server Firewall to add the ports in your Firewall. Also, include port 21. It should look like below:



Protocol and Ports

Specify the protocols and ports to which this rule applies.

Does this rule apply to TCP or UDP?

● TCP
○ UDP

Does this rule apply to all local ports or specific local ports?

○ All local ports
● Specific local ports: 21, 40000-41000

Example: 80, 443, 5000-5010

Setting up DHCP Services

TCP/IP is the priority protocol for Windows Server 2019. There are two ways to have clients and servers get TCP/IP addresses:

- You can manually assign the addresses.
- The addresses can be assigned automatically.

Manually assigning addresses is a fairly simple process. An administrator goes to each of the machines on the network and assigns TCP/IP addresses. The problem with this method arises when the network becomes midsized or larger. Think of an administrator trying to individually assign 4,000 TCP/IP addresses, subnet masks, default gateways, and all other configuration options needed to run the network.

DHCP’s job is to centralize the process of IP address and option assignment. You can configure a DHCP server with a range of addresses (called a pool) and other configuration information and let it assign all of the IP parameters—addresses, default gateways, DNS server addresses, and so on.

Introducing the DORA Process

An easy way to remember how DHCP works is to learn the acronym DORA. DORA stands for Discover, Offer, Request, and Acknowledge. In brief, here is DHCP’s DORA process:
1. Discover: When IP networking starts up on a DHCP-enabled client, a special message called a DHCPDISCOVER is broadcast within the local physical subnet.
2. Offer: Any DHCP server that hears the request checks its internal database and replies with a message called a DHCPOFFER, which contains an available IP address.

The contents of this message depend on how the DHCP server is configured—there are numerous options aside from an IP address that you can specify to pass to the client on a Windows Server DHCP server.

3. Request: The client receives one or more DHCPOFFERs (depending on how many DHCP servers exist on the local subnet), chooses an address from one of the offers, and sends a DHCPREQUEST message to the server to signal acceptance of the DHCPOF-FER.

This message might also request additional configuration parameters.

Other DHCP servers that sent offers take the request message as an acknowledgment that the client didn’t accept their offer.

4. Acknowledge: When the DHCP server receives the DHCPREQUEST, it marks the IP address as being in use (that is, usually, though it’s not required). Then it sends a DHC-PACK to the client.

The acknowledgment message might contain requested configuration parameters.

If the server is unable to accept the DHCPREQUEST for any reason, it sends a DHCPNAK message. If a client receives a DHCPNAK, it begins the configuration pro-cess over again.

5. When the client accepts the IP offer, the address is assigned to the client for a specified period of time, called a lease. After receiving the DHCPACK message, the client performs a final check on the parameters (sometimes it sends an ARP request for the offered IP address) and makes note of the duration of the lease. The client is now configured. If the client detects that the address is already in use, it sends a DHCPDECLINE.

If the DHCP server has given out all of the IP addresses in its pool, it won’t make an offer. If no other servers make an offer, the client’s IP network initialization will fail, and the client will use Automatic Private IP Addressing (APIPA).

DHCP Lease Renewal

No matter how long the lease period, the client sends a new lease request message directly to the DHCP server when the lease period is half over (give or take some randomness required by RFC 2131). This period goes by the name T1 (not to be confused with the T1 type of network connection). If the server hears the request message and there's no reason to reject it, it sends a DHCPACK to the client. This resets the lease period.

If the DHCP server isn't available, the client realizes that the lease can't be renewed. The client continues to use the address, and once 87.5 percent of the lease period has elapsed (again, give or take some randomness), the client sends out another renewal request.

This interval is known as T2. At that point, any DHCP server that hears the renewal can respond to this DHCP request message (which is a request for a lease renewal) with a DHCPACK and renew the lease. If at any time during this process the client gets a negative DHCPNACK message, it must stop using its IP address immediately and start the leasing process over from the beginning by requesting a new lease.

When a client initializes its IP networking, it always attempts to renew its old address. If the client has time left on the lease, it continues to use the lease until its end. If the client is unable to get a new lease by that time, all IP functions stop until a new, valid address can be obtained.

DHCP Lease Release

Although leases can be renewed repeatedly, at some point they might run out. Furthermore, the lease process is "at will." That is, the client or server can cancel the lease before it ends. In addition, if the client doesn't succeed in renewing the lease before it expires, the client loses its lease and reverts to APIPA. This release process is important for reclaiming extinct IP addresses used by systems that have moved or switched to a non-DHCP address.

Advantages and Disadvantages of DHCP

DHCP was designed from the start to simplify network management. It has some significant advantages, but it also has some drawbacks.

Advantages of DHCP

The following are advantages of DHCP:

- Configuration of large and even midsized networks is much simpler. If a DNS server address or some other change is necessary to the client, the administrator doesn't have to touch each device in the network physically to reconfigure it with the new settings.
- Once you enter the IP configuration information in one place—the server—it's automatically propagated to clients, eliminating the risk that a user will misconfigure some parameters and require you to fix them.
- IP addresses are conserved because DHCP assigns them only when requested.
- IP configuration becomes almost completely automatic. In most cases, you can plug in a new system (or move one) and then watch as it receives a configuration from the server. For example, when you install new network changes, such as a gateway or DNS server, the client configuration is done at only one location—the DHCP server.
- It allows a preboot execution environment (PXE) client to get a TCP/IP address from DHCP. PXE clients (also called Microsoft Windows Deployment Services [WDS] clients) can get an IP address without needing to have an operating system installed. This allows WDS clients to connect to a WDS server through the TCP/IP protocol and download an operating system remotely.

Disadvantages of DHCP

Unfortunately, there are a few drawbacks with DHCP:

■ DHCP can become a single point of failure for your network. If you have only one DHCP server and it’s not available, clients can’t request or renew leases.
■ If the DHCP server contains incorrect information, the misinformation will automati-cally be delivered to all of your DHCP clients.
■ If you want to use DHCP on a multisegment network, you must put either a DHCP server or a relay agent on each segment, or you must ensure that your router can for-ward Bootstrap Protocol (BOOTP) broadcasts.

Ipconfig Lease Options

ipconfig /renew Instructs the DHCP client to request a lease renewal. If the client already has a lease, it requests a renewal from the server that issued the current lease. This is equivalent to what happens when the client reaches the half-life of its lease. Alternatively, if the client doesn’t currently have a lease, it is equivalent to what happens when you boot a DHCP client for the first time. It initiates the DHCP mating dance, listens for lease offers, and chooses one it likes.

ipconfig /release Forces the client to give up its lease immediately by sending the server a DHCP release notification. The server updates its status information and marks the client’s old IP address as “available,” leaving the client with no address bound to its network interface. When you use this command, most of the time it will be immediately followed by ipconfig/renew. The combination releases the existing lease and gets a new one, probably with a different address. (It’s also a handy way to force your client to get a new set of settings from the server before the lease expiration time.)

ipconfig /setclassidclassID Sets a new class ID for the client. You will see how to configure class options later in the section “Setting Scope Options for IPv4.” For now, you should know that the only way to add a client machine to a class is to use this command. Note that you need to renew the client lease for the class assignment to take effect.

If you have multiple network adapters in a single machine, you can provide the name of the adapter (or adapters) upon which you want the command to work, including an asterisk (*) as a wildcard. For example, one of my servers has two network cards: an Intel EtherExpress (ELNK1) and a generic 100Mbps card. If you want to renew DHCP settings for both adapters, you can type ipconfig /renew *. If you just want to renew the Intel EtherExpress card, you can type ipconfig /renew ELNK1.

Understanding Scope Details

By now you should have a good grasp of what a lease is and how it works. To learn how to configure your servers to hand out those leases, however, you need to have a complete understanding of some additional topics: scopes, superscopes, exclusions, reservations, address pool, and relay agents.

Scope

Let’s start with the concept of a scope, which is a contiguous range of addresses. There’s usually one scope per physical subnet, and a scope can cover a Class A, Class B, or Class C network address or a TCP/IP v6 address. DHCP uses scopes as the basis for managing and assigning IP addressing information.

Each scope has a set of parameters, or scope options, that you can configure. Scope options control what data is delivered to DHCP clients when they’re completing the DHCP negotiation process with a particular server. For example, the DNS server name, default gateway, and default network time server are all separate options that can be assigned.

These settings are called option types. You can use any of the types provided with Windows Server 2019, or you can specify your own.

Superscope

A superscope enables the DHCP server to provide addresses from more than one scope to clients on the same physical subnet. This is helpful when clients within the same subnet have more than one IP network and thus need IPs from more than one address pool. Microsoft's DHCP snap-in allows you to manage IP address assignment in the superscope, though you must still configure other scope options individually for each child scope.

Exclusions and Reservations

The scope defines what IP addresses could potentially be assigned, but you can influence the assignment process in two additional ways by specifying exclusions and reservations:

Exclusions These are IP addresses within the range that you never want automatically assigned. These excluded addresses are off-limits to DHCP. You'll typically use exclusions to tag any addresses that you never want the DHCP server to assign at all. You might use exclusions to set aside addresses that you want to assign permanently to servers that play a vital role in your organization.

Reservations These are IP addresses within the range for which you want a permanent DHCP lease. They essentially reserve a particular IP address for a particular device. The device still goes through the DHCP process (that is, its lease expires and it asks for a new one), but it always obtains the same addressing information from the DHCP server.

Address Pool

The range of IP addresses that the DHCP server can assign is called its address pool. For example, let's say you set up a new DHCP scope covering the 192.168.1 subnet. That gives you 255 IP addresses in the pool. After adding an exclusion from 192.168.1.240 to 192.168.1.254, you're left with 241 (255 – 14) IP addresses in the pool. That means (in theory, at least) that you can service 241 unique clients at a time before you run out of IP addresses.

DHCP Relay Agent

By design, DHCP is intended to work only with clients and servers on a single IP network to communicate. But RFC 1542 sets out how BOOTP (on which DHCP is based) should work in circumstances in which the client and server are on different IP networks. If no DHCP server is available on the client's network, you can use a DHCP relay agent to forward DHCP broadcasts from the client's network to the DHCP server. The relay agent acts like a radio repeater, listening for DHCP client requests and retransmitting them through the router to the server.

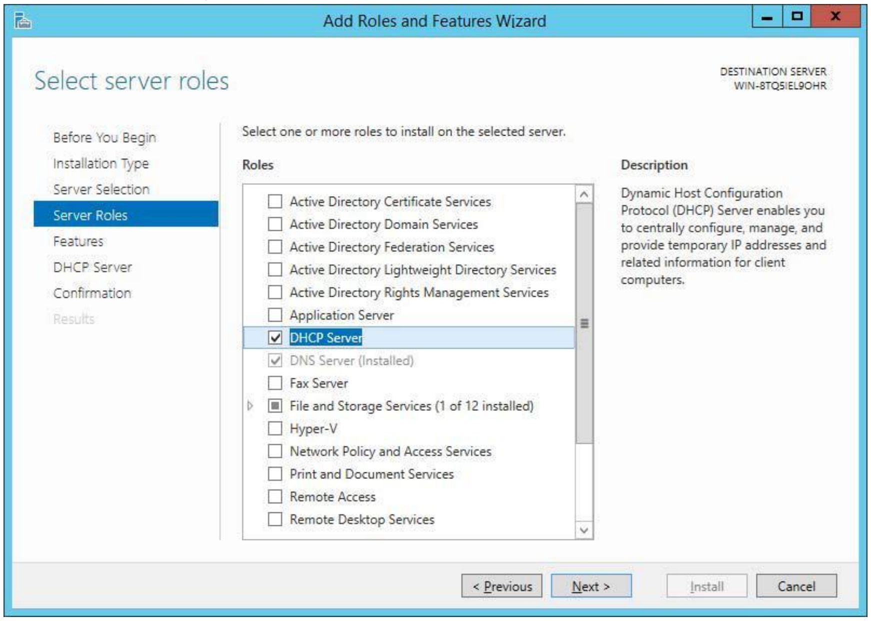
Installing and Authorizing DHCP

Installing DHCP is easy using the Windows Server 2012/2019 installation mechanism. Unlike some other services discussed in this book, the installation process installs just the service and its associated snap-in, starting it when the installation is complete. At that point, it's not delivering any DHCP service, but you don't have to reboot.

Installing the DHCP Service

1. Choose Server Manager by clicking the Server Manager icon on the taskbar.
2. Click Add Roles And Features.
3. Choose role-based or feature-based installation and click Next.

4. Choose your server and click Next.
5. Choose DHCP and click Next.
6. At the Features screen, click Next.
7. Click Next at the DHCP screen.
8. At the DHCP confirmation screen, click the Install button.



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
WIN-8TQ5IEL9OHR

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- DHCP Server
- Confirmation
- Results

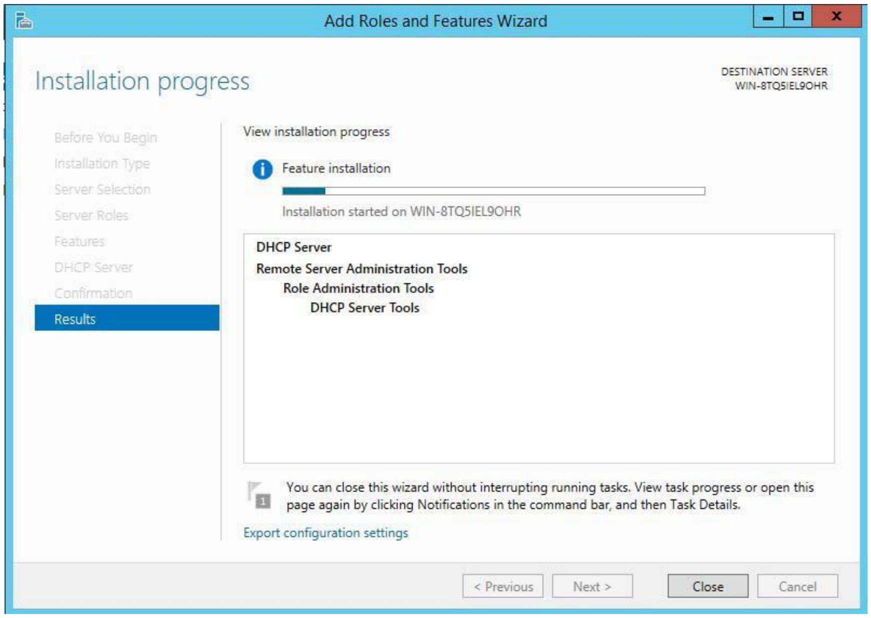
Select one or more roles to install on the selected server.

Roles

- ☐ Active Directory Certificate Services
- ☐ Active Directory Domain Services
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☑ DHCP Server
- ☑ DNS Server (Installed)
- ☐ Fax Server
- ▣ File and Storage Services (1 of 12 installed)
- ☐ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services

Description

Dynamic Host Configuration Protocol (DHCP) Server enables you to centrally configure, manage, and provide temporary IP addresses and related information for client computers.



Add Roles and Features Wizard

Installation progress

DESTINATION SERVER
WIN-8TQ5IEL9OHR

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- DHCP Server
- Confirmation
- Results

View installation progress

Feature installation

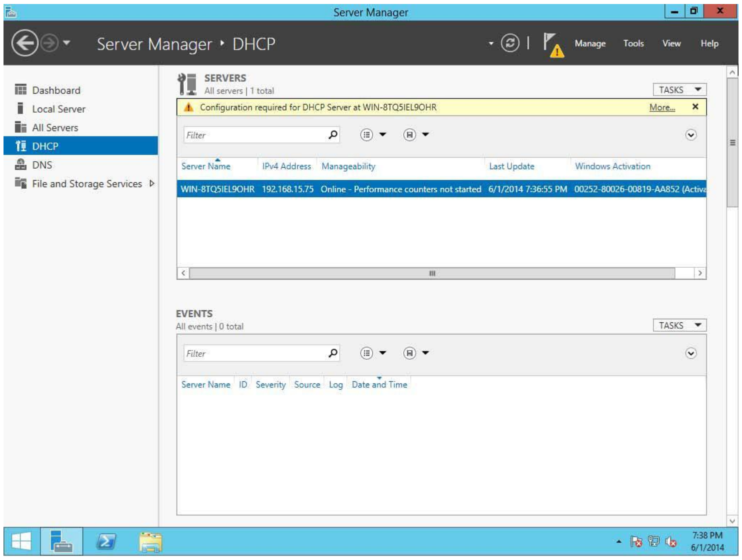
Installation started on WIN-8TQ5IEL9OHR

DHCP Server
Remote Server Administration Tools
    Role Administration Tools
        DHCP Server 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

9. When the installation is complete, click the Close button.
10. On the left side, click the DHCP link.
11. Click the More link next to Configuration Required For DHCP Server.
12. Under Action, click Complete DHCP Configuration.



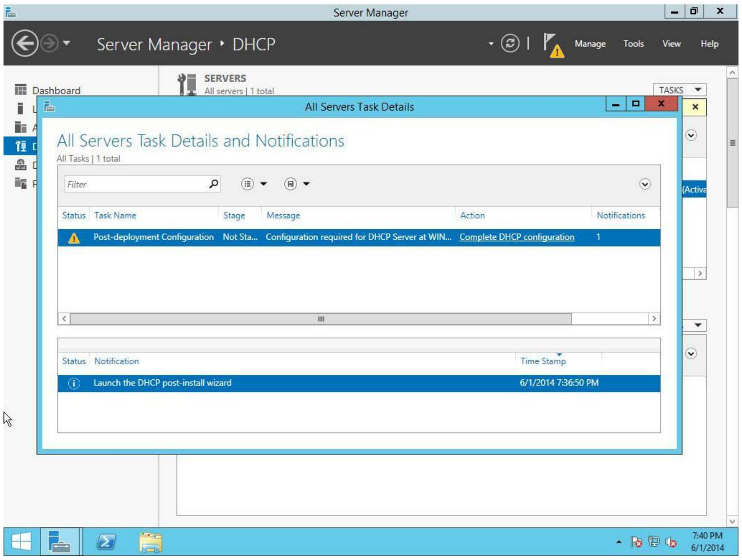
SERVERS
All servers | 1 total

Configuration required for DHCP Server at WIN-8TQ5IEL9OHR More...

Server Name	IPv4 Address	Manageability	Last Update	Windows Activation
WIN-8TQ5IEL9OHR	192.168.15.75	Online - Performance counters not started	6/1/2014 7:36:55 PM	00252-80026-00819-AA852 (Activa

EVENTS
All events | 0 total

Server Name	ID	Severity	Source	Log	Date and Time

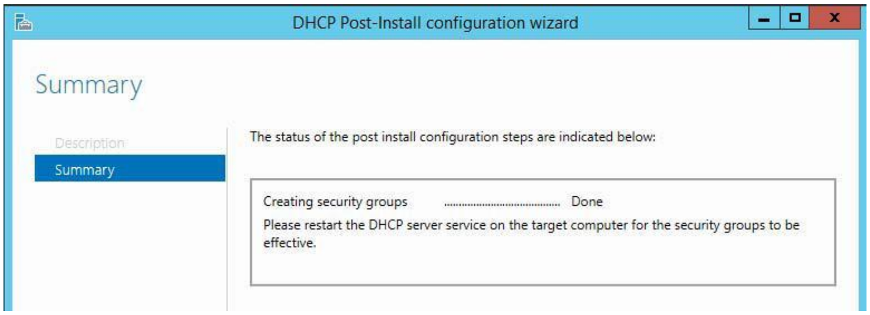


All Servers Task Details and Notifications
All Tasks | 1 total

Status	Task Name	Stage	Message	Action	Notifications
⚠	Post-deployment Configuration	Not Sta...	Configuration required for DHCP Server at WIN...	Complete DHCP configuration	1

Status	Notification	Time Stamp
ⓘ	Launch the DHCP post-install wizard	6/1/2014 7:36:50 PM

13. At the DHCP Description page, click Commit.
14. Click Close at the Summary screen.



The status of the post install configuration steps are indicated below:

Creating security groups .... Done
Please restart the DHCP server service on the target computer for the security groups to be effective.

15. Close Server Manager.

Introducing the DHCP Snap-In

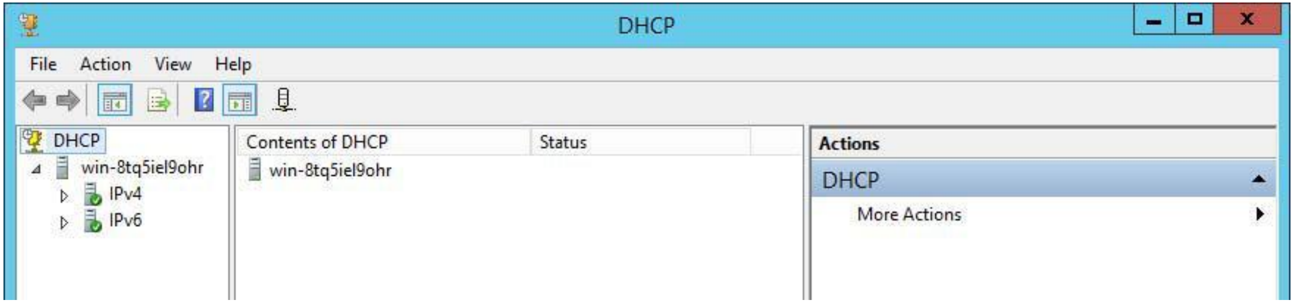
When you install the DHCP server, the DHCP snap-in is also installed. You can open it by selecting Administrative Tools ➢ DHCP. Figure 2.17 shows the snap-in.

As you can see, the snap-in follows the standard MMC model. The left pane displays IPv4 and IPv6 sections and which servers are available; you can connect to servers other than the one to which you're already connected. A Server Options folder contains options that are specific to a particular DHCP server. Each server contains subordinate items grouped into folders. Each scope has a folder named after the scope's IP address range. Within each scope, four subordinate views show you interesting things about the scope, such as the following:

■ The Address Pool view shows what the address pool looks like.

■ The Address Leases view shows one entry for each current lease. Each lease shows the computer name to which the lease was issued, the corresponding IP address, and the current lease expiration time.

F I GU R E 2 .17 DHCP snap-in



■ The Reservations view shows the IP addresses that are reserved and which devices hold them.

■ The Scope Options view lists the set of options you've defined for this scope.

Authorizing DHCP for Active Directory

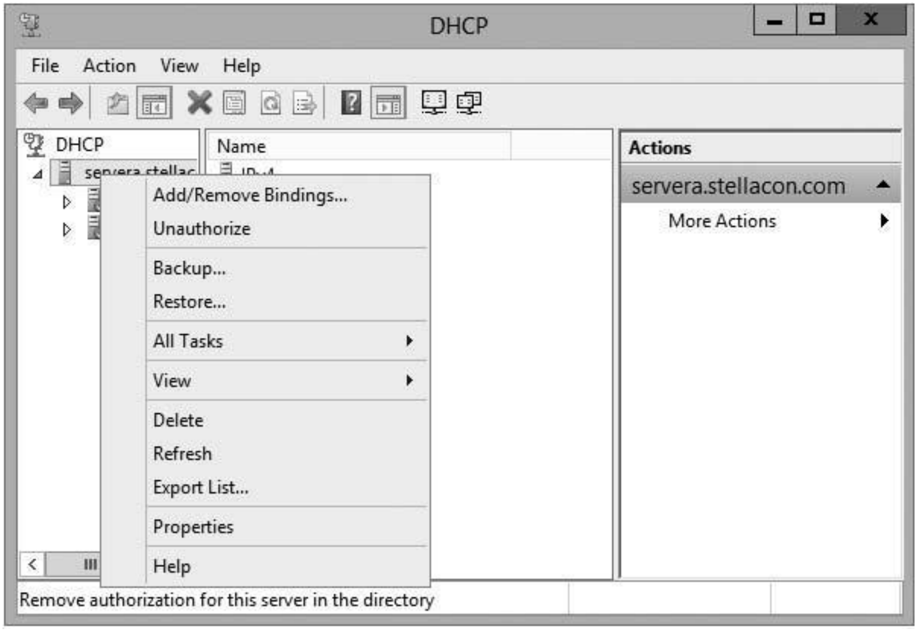
Authorization creates an Active Directory object representing the new server. It helps keep unauthorized servers off your network. Unauthorized servers can cause two kinds of problems. They may hand out bogus leases, or they may fraudulently deny renewal requests from legitimate clients.

When you install a DHCP server using Windows Server 2012/2019 and Active Directory is present on your network, the server won't be allowed to provide DHCP services to clients until it has been authorized. If you install DHCP on a member server in an Active Directory domain or on a stand-alone server, you'll have to authorize the server manually. When you authorize a server, you're adding its IP address to the Active Directory object that contains the IP addresses of all authorized DHCP servers.

At start time, each DHCP server queries the directory, looking for its IP address on the "authorized" list. If it can't find the list or if it can't find its IP address on the list, the DHCP service fails to start. Instead, it adds a message to the event log, indicating that it couldn't service client requests because the server wasn't authorized.

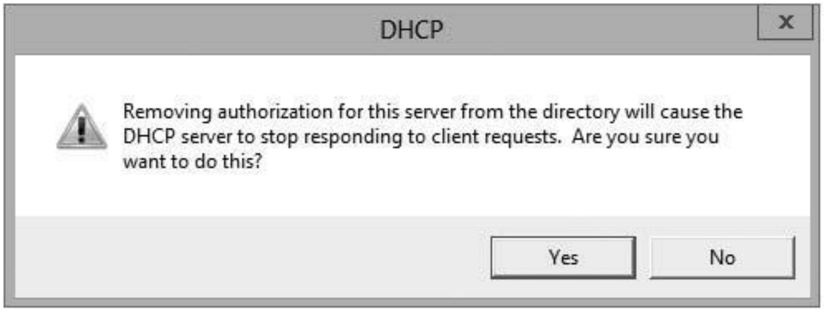
Unauthorizing a DHCP Server

1. From Administrative Tools, choose DHCP to open the DHCP snap-in.
2. Right-click the server you want to unauthorize and choose the Unauthorize command.



Remove authorization for this server in the directory

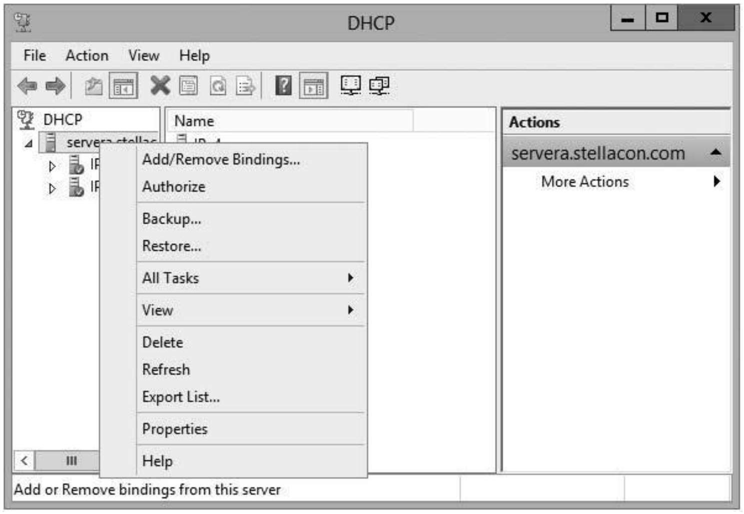
3. Click Yes on the dialog box asking if you are sure you want to complete this action.



Removing authorization for this server from the directory will cause the DHCP server to stop responding to client requests. Are you sure you want to do this?

Authorizing a DHCP Server

1. From Administrative Tools, choose DHCP to open the DHCP snap-in.
2. Right-click the server you want to authorize and choose the Authorize command.



Add or Remove bindings from this server

3. Wait a short time (30 to 45 seconds) to allow the authorization to take place.

4. Right-click the server again. Verify that the Unauthorize command appears in the pop-up menu. This indicates that the server is now authorized.

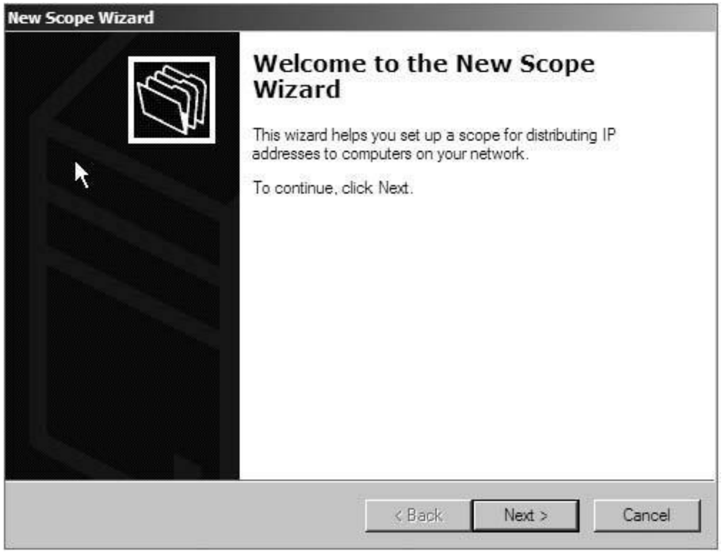
Creating a New Scope in IPv4

Like many other things in Windows Server 2019, a wizard drives the process of creating a new scope. You will most likely create a scope while installing DHCP, but you may need to create more than one. The overall process is simple, as long as you know beforehand what the wizard is going to ask. If you think about what defines a scope, you'll be well prepared. You need to know the following:

■ The IP address range for the scope you want to create.
■ Which IP addresses, if any, you want to exclude from the address pool.
■ Which IP addresses, if any, you want to reserve.
■ Values for the DHCP options you want to set, if any. This item isn't strictly neces-sary for creating a scope. However, to create a useful scope, you'll need to have some options to specify for the clients.

To create a scope, under the server name, right-click the IPv4 option in the DHCP snap-in, and use the Action ➢ New Scope command. This starts the New Scope Wizard (see Figure 2.18). You will look at each page of the wizard in the following sections.

FIGURE 2.18 Welcome page of the New Scope Wizard



New Scope Wizard

Welcome to the New Scope Wizard

This wizard helps you set up a scope for distributing IP addresses to computers on your network.

To continue, click Next.

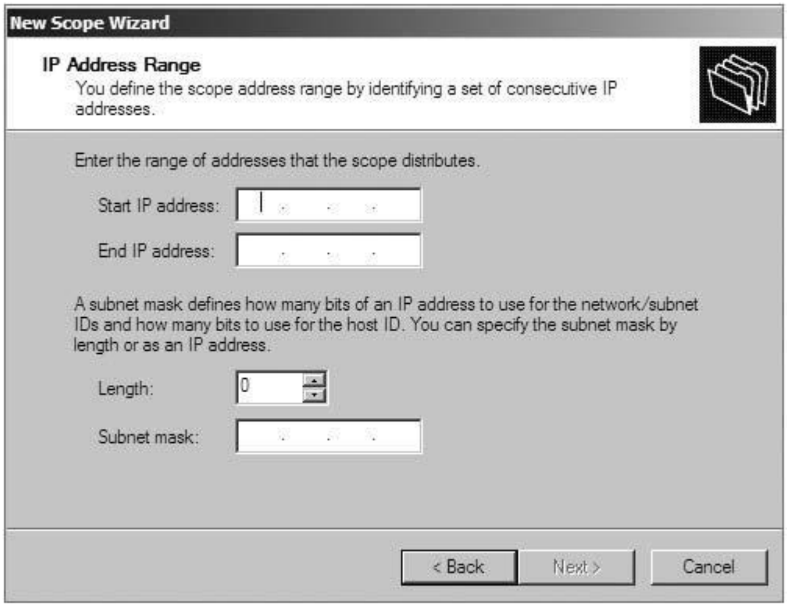
Setting the Screen Name

The Scope Name page allows you to enter a name and description for your scope. These will be displayed by the DHCP snap-in.

Defining the IP Address Range

The IP Address Range page (see Figure 2.19) is where you enter the start and end IP addresses for your range. The wizard does minimal checking on the addresses you enter, and it automatically calculates the appropriate subnet mask for the range. You can modify the subnet mask if you know what you're doing.

F I GU R E 2 .19 IP Address Range page of the New Scope Wizard



New Scope Wizard

IP Address Range

You define the scope address range by identifying a set of consecutive IP addresses.

Enter the range of addresses that the scope distributes.

Start IP address:

End IP address:

A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address.

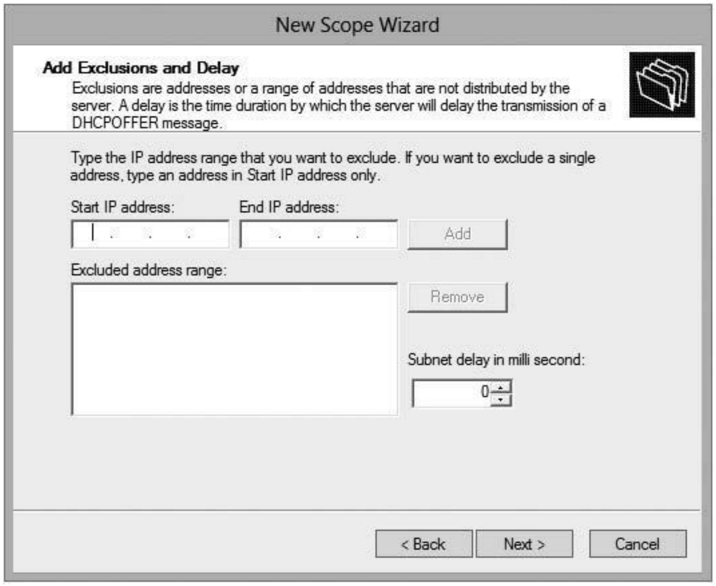
Length: 0

Subnet mask:

Adding Exclusions and Delay

The Add Exclusions And Delay page (see Figure 2.20) allows you to create exclusion ranges. Exclusions are TCP/IP numbers that are in the pool, but they do not get issued to clients. To exclude one address, put it in the Start IP Address field. To exclude a range, also fill in the End IP Address field. The delay setting is a time duration by which the server will delay the transmission of a DHCPOFFER message.

F I GU R E 2 . 20 Add Exclusions And Delay page of the New Scope Wizard



New Scope Wizard

Add Exclusions and Delay

Exclusions are addresses or a range of addresses that are not distributed by the server. A delay is the time duration by which the server will delay the transmission of a DHCPOFFER message.

Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address:

End IP address:

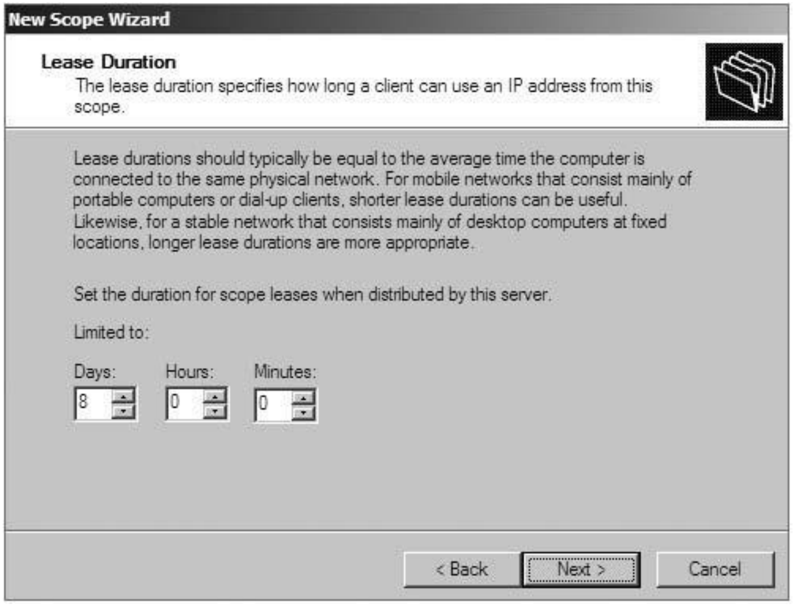
Excluded address range:

Subnet delay in milli second: 0

Setting a Lease Duration

The Lease Duration page (see Figure 2.21) allows you to set how long a device gets to use an assigned IP address before it has to renew its lease. The default lease duration is eight days. You may find that a shorter or longer duration makes sense for your network. If your network is highly dynamic, with lots of arrivals, departures, and moving computers, set a shorter lease duration; if it's less active, make it longer.

FIGURE 2.21 Lease Duration page of the New Scope Wizard



New Scope Wizard

Lease Duration

The lease duration specifies how long a client can use an IP address from this scope.

Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

Set the duration for scope leases when distributed by this server.

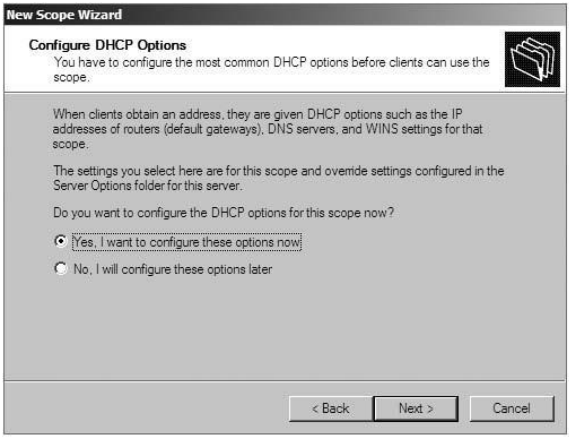
Limited to:

Days: 8 Hours: 0 Minutes: 0

Configuring Basic DHCP Options

The Configure DHCP Options page (see Figure 2.22) allows you to choose whether you want to set up basic DHCP options such as default gateway and DNS settings. The options are described in the following sections. If you choose not to configure options, you can always do so later. However, you should not activate the scope until you've configured the options you want assigned.

FIGURE 2.22 Configure DHCP Options page of the New Scope Wizard



New Scope Wizard

Configure DHCP Options

You have to configure the most common DHCP options before clients can use the scope.

When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.

The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

Do you want to configure the DHCP options for this scope now?

● Yes, I want to configure these options now

○ No, I will configure these options later

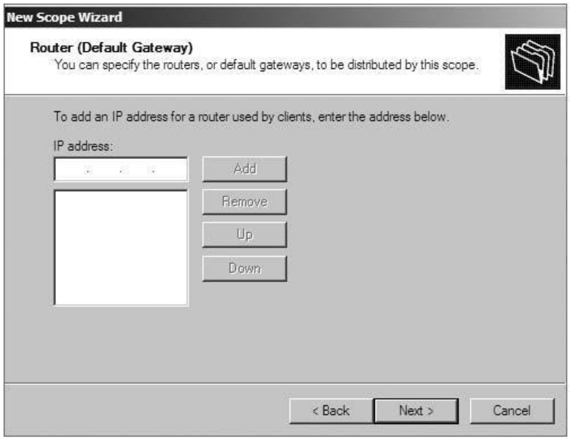
Configuring a Router

The first option configuration page is the Router (Default Gateway) page (see Figure 2.23), in which you enter the IP addresses of one or more routers (more commonly referred to as default gateways) that you want to use for outbound traffic. After entering the IP addresses of the routers, use the Up and Down buttons to order the addresses. Clients will use the routers in the order specified when attempting to send outgoing packets.

Providing DNS Settings

On the Domain Name And DNS Servers page (see Figure 2.24), you specify the set of DNS servers and the parent domain you want passed down to DHCP clients. Normally, you'll want to specify at least one DNS server by filling in its DNS name or IP address. You can also specify the domain suffix that you want clients to use as the base domain for all connections that aren't fully qualified. For example, if your clients are used to navigating based on server name alone rather than the fully qualified domain name (FQDN) of server.willpanek.com, then you'll want to place your domain here.

FIGURE 2.23 Router (Default Gateway) page of the New Scope Wizard



New Scope Wizard

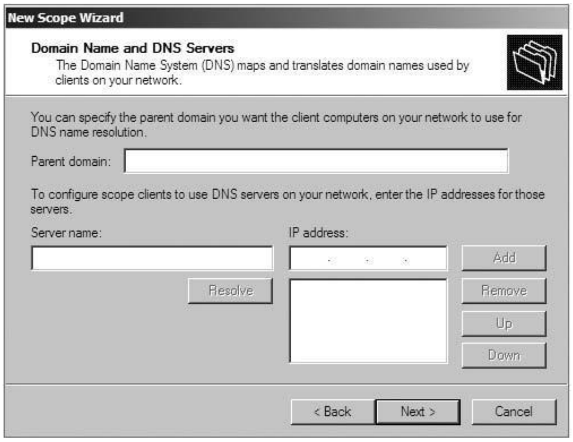
Router (Default Gateway)

You can specify the routers, or default gateways, to be distributed by this scope.

To add an IP address for a router used by clients, enter the address below.

IP address:

FIGURE 2.24 Domain Name And DNS Servers page of the New Scope Wizard



New Scope Wizard

Domain Name and DNS Servers

The Domain Name System (DNS) maps and translates domain names used by clients on your network.

You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain:

To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

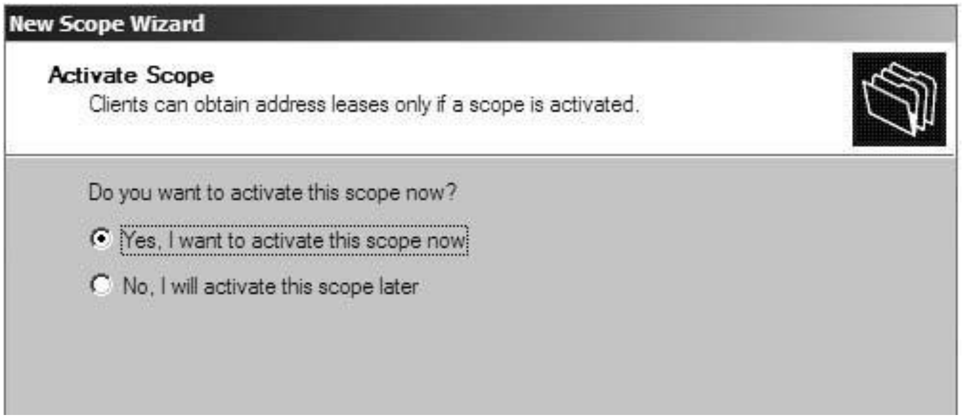
Server name:

IP address:

Activating the Scope

The Activate Scope page (see Figure 2.26) gives you the option to activate the scope immediately after creating it. By default, the wizard assumes that you want the scope activated unless you select the No, I Will Activate This Scope Later radio button, in which case the scope will remain dormant until you activate it manually.

FIGURE 2.26 Activate Scope page of the New Scope Wizard


New Scope Wizard

Activate Scope
Clients can obtain address leases only if a scope is activated.

Do you want to activate this scope now?

● Yes, I want to activate this scope now

○ No, I will activate this scope later

Creating a New Scope
1. Open the DHCP snap-in by selecting Administrative Tools ➢ DHCP.
2. Right-click the IPv4 folder and choose New Scope. The New Scope Wizard appears.
3. Click the Next button on the welcome page.
4. Enter a name and a description for your new scope and click the Next button.
5. On the IP Address Range page, enter 192.168.0.2 as the start IP address for the scope and 192.168.0.250 as the end IP address. Leave the subnet mask controls alone (though when creating a scope on a production network, you might need to change them). Click the Next button.
6. On the Add Exclusions And Delay page, click Next without adding any excluded addresses or delays.
7. On the Lease Duration page, set the lease duration to 3 days and click the Next button.
8. On the Configure DHCP Options page, click the Next button to indicate you want to con-figure default options for this scope.
9. On the Router (Default Gateway) page, enter 192.168.0.1 for the router IP address and then click the Add button. Once the address is added, click the Next button.
10. On the Domain Name And DNS Servers page, enter the IP address of a DNS server on your network in the IP Address field (for example, you might enter 192.168.0.251) and click the Add button. Click the Next button.
11. On the WINS Servers page, click the Next button to leave the WINS options unset.
12. On the Activate Scope page, if your network is currently using the 192.168.0.x range, select Yes, I Want To Activate This Scope Now. Click the Next button.
13. When the wizard's summary page appears, click the Finish button to create the scope.

Creating a New Scope in IPv6

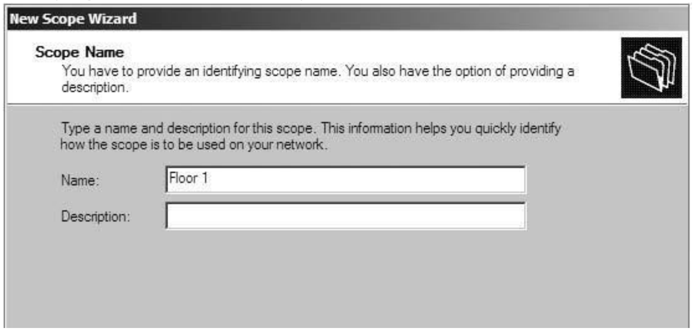
Now that you have seen how to create a new scope in IPv4, I'll go through the steps to create a new scope in IPv6.

To create a scope, right-click the IPv6 option in the DHCP snap-in under the server name and select the Action ➢ New Scope command. This starts the New Scope Wizard. Just as with creating a scope in IPv4, the welcome page of the wizard tells you that you've launched the New Scope Wizard. You will look at each page of the wizard in the following sections.

Setting the Screen Name

The Scope Name page (see Figure 2.27) allows you to enter a name and description for your scope. These will be displayed by the DHCP snap-in.

F I GU R E 2 . 27 IPv6 Scope Name page of the New Scope Wizard



Scope Name

You have to provide an identifying scope name. You also have the option of providing a description.

Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

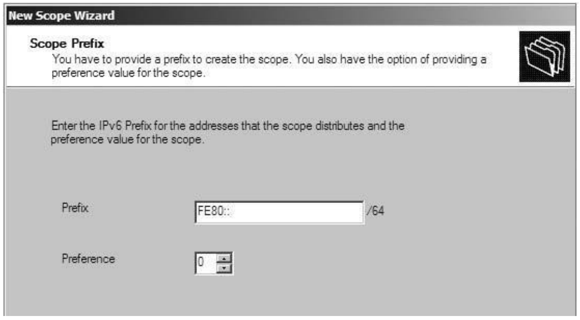
Name: Floor 1

Description:

Scope Prefix

The Scope Prefix page (see Figure 2.28) gets you started creating the IPv6 scope. IPv6 has three types of addresses, which can be categorized by type and scope.

F I GU R E 2 . 28 Scope Prefix page of the New Scope Wizard



Scope Prefix

You have to provide a prefix to create the scope. You also have the option of providing a preference value for the scope.

Enter the IPv6 Prefix for the addresses that the scope distributes and the preference value for the scope.

Prefix FE80:: /64

Preference 0

Unicast Addresses One-to-one. A packet from one host is delivered to another host. The following are some examples of IPv6 unicast:

- The unicast prefix for site-local addresses is FEC0::/48.
- The unicast prefix for link-local addresses is FE80::/64.

The 6to4 address allows communication between two hosts running both IPv4 and IPv6. The way to calculate the 6to4 address is by combining the global prefix 2002::/16 with the 32 bits of a public IPv4 address of the host. This gives you a 48-bit prefix. 6to4 is described in RFC 3056.

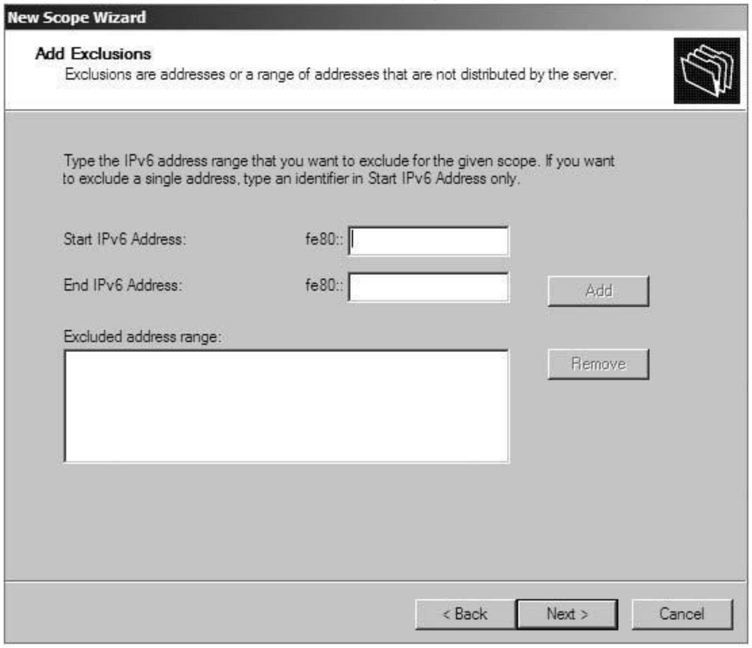
Multicast addresses One-to-many. A packet from one host is delivered to multiple hosts (but not everyone). The prefix for multicast addresses is FF00::/8.

Anycast addresses A packet from one host is delivered to the nearest of multiple hosts (in terms of routing distance).

Adding Exclusions

As with the IPv4 New Scope Wizard, the Add Exclusions page (see Figure 2.29) allows you to create exclusion ranges. Exclusions are TCP/IP numbers that are in the pool but do not get issued to clients. To exclude one address, put it in the Start IPv6 Address field. To exclude a range, also fill in the End IPv6 Address field.

FIGURE 2.29 Add Exclusions page of the New Scope Wizard



New Scope Wizard

Add Exclusions

Exclusions are addresses or a range of addresses that are not distributed by the server.

Type the IPv6 address range that you want to exclude for the given scope. If you want to exclude a single address, type an identifier in Start IPv6 Address only.

Start IPv6 Address: fe80::

End IPv6 Address: fe80::

Excluded address range:

Setting a Lease Duration

The Scope Lease page (see Figure 2.30) allows you to set how long a device gets to use an assigned IP address before it has to renew its lease. You can set two different lease durations. The section labeled Non Temporary Address (IANA) is the lease time for your more permanent hosts (such as printers and server towers). The one labeled Temporary Address (IATA) is for hosts that might disconnect at any time, such as laptops.

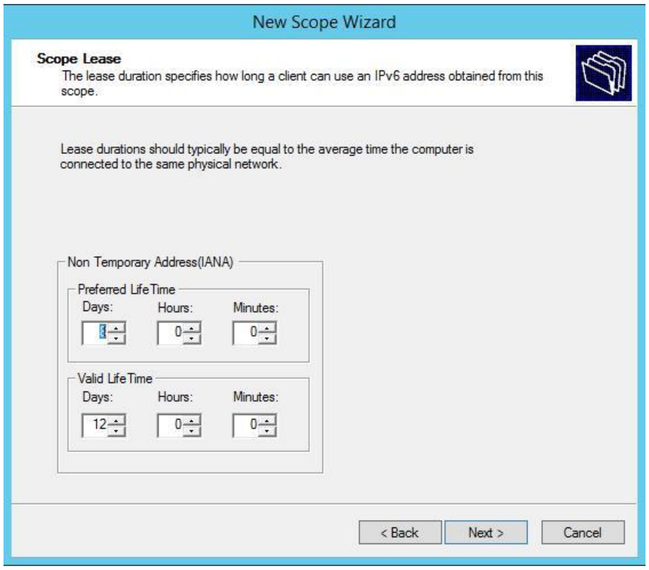
Activating the Scope

The Completing The New Scope Wizard page (see Figure 2.31) gives you the option to activate the scope immediately after creating it. By default, the wizard will assume you want the scope activated. If you want to wait to activate the scope, choose No in the Activate Scope Now box.

Changing Scope Properties (IPv4 and IPv6)

Each scope has a set of properties associated with it. Except for the set of options assigned by the scope, you can find these properties on the General tab of the scope's Properties

FIGURE 2.30 Scope Lease page of the New Scope Wizard



Scope Lease

The lease duration specifies how long a client can use an IPv6 address obtained from this scope.

Lease durations should typically be equal to the average time the computer is connected to the same physical network.

Non Temporary Address(IANA)

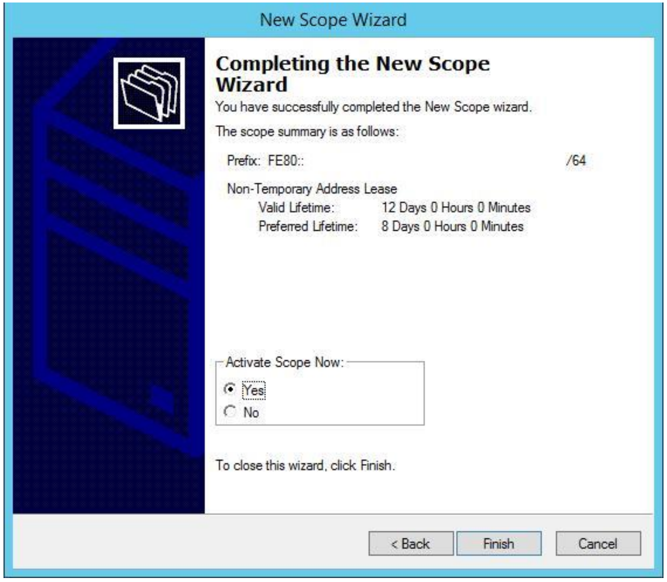
Preferred Life Time

Days: 8 Hours: 0 Minutes: 0

Valid Life Time

Days: 12 Hours: 0 Minutes: 0

F I GU R E 2 . 31 Completing The New Scope Wizard page of the New Scope Wizard



Completing the New Scope Wizard

You have successfully completed the New Scope wizard.

The scope summary is as follows:

Prefix: FE80:: /64

Non-Temporary Address Lease

Valid Lifetime: 12 Days 0 Hours 0 Minutes

Preferred Lifetime: 8 Days 0 Hours 0 Minutes

Activate Scope Now:

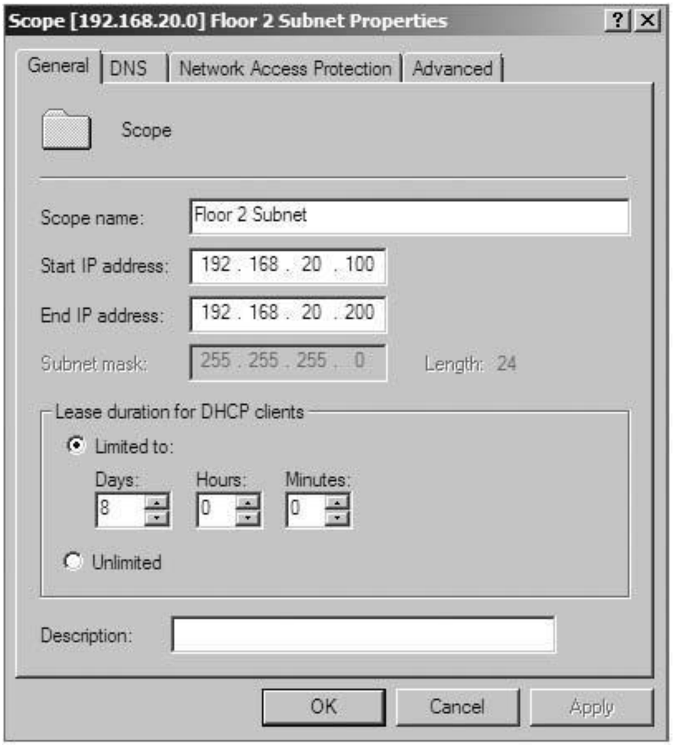
● Yes

○ No

To close this wizard, click Finish.

dialog box (see Figure 2.32). Some of these properties, such as the scope name and description, are self-explanatory. Others require a little more explanation.

F I GU R E 2 . 3 2 General tab of the scope’s Properties dialog box for an IPv4 scope



Scope [192.168.20.0] Floor 2 Subnet Properties

General | DNS | Network Access Protection | Advanced

Scope

Scope name: Floor 2 Subnet

Start IP address: 192 . 168 . 20 . 100

End IP address: 192 . 168 . 20 . 200

Subnet mask: 255 . 255 . 255 . 0 Length: 24

Lease duration for DHCP clients

● Limited to:

Days: 8 Hours: 0 Minutes: 0

○ Unlimited

Description:

- The Start IP Address and End IP Address fields allow you to set the range of the scope.
- For IPv4 scopes, the settings in the section Lease Duration For DHCP Clients control how long leases in this scope are valid.

The IPv6 scope dialog box includes a Lease tab where you set the lease properties.

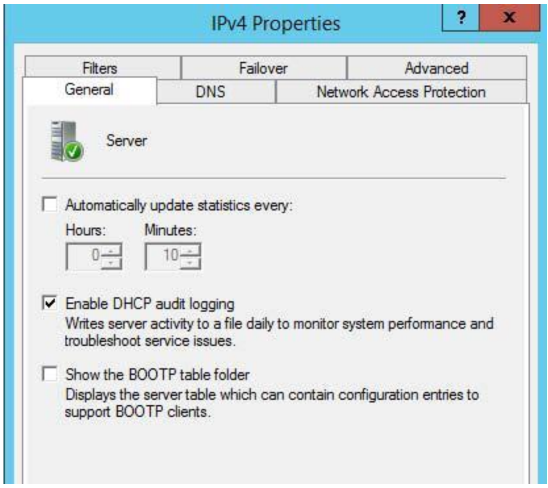
Changing Server Properties

Just as each scope has its own set of properties, so too does the server itself. You access the server properties by right-clicking the IPv4 or IPv6 object within the DHCP management console and selecting Properties.

IPv4 Server Properties

Figure 2.33 shows the IPv4 Properties dialog box.

FIGURE 2.33 General tab of the IPv4 Properties dialog box for the server



IPv4 Properties

Filters | Failover | Advanced

General | DNS | Network Access Protection

Server

□ Automatically update statistics every:

Hours: 0 Minutes: 10

☑ Enable DHCP audit logging

Writes server activity to a file daily to monitor system performance and troubleshoot service issues.

□ Show the BOOTP table folder

Displays the server table which can contain configuration entries to support BOOTP clients.

Setup remote access service / terminal services

Set up rds remote app

1. Server manager→add roles and features
   →remote desktop services installation→quick start
   →session-based
   →select RDS server
   →deploy
   restart

2. server manager→remote desktop services→quicksessioncollection
   →remoteapp programs, click tasks→publish remoteapp programs→select remoteapp program to publish
   →publish

3. on client browser→https://<fqdn>/rdweb

4. if unsecure (because no ssl cert), just proceed even if you see warning in work resources, enter domain username and password you can now select published remoteapp program and connect to use it.