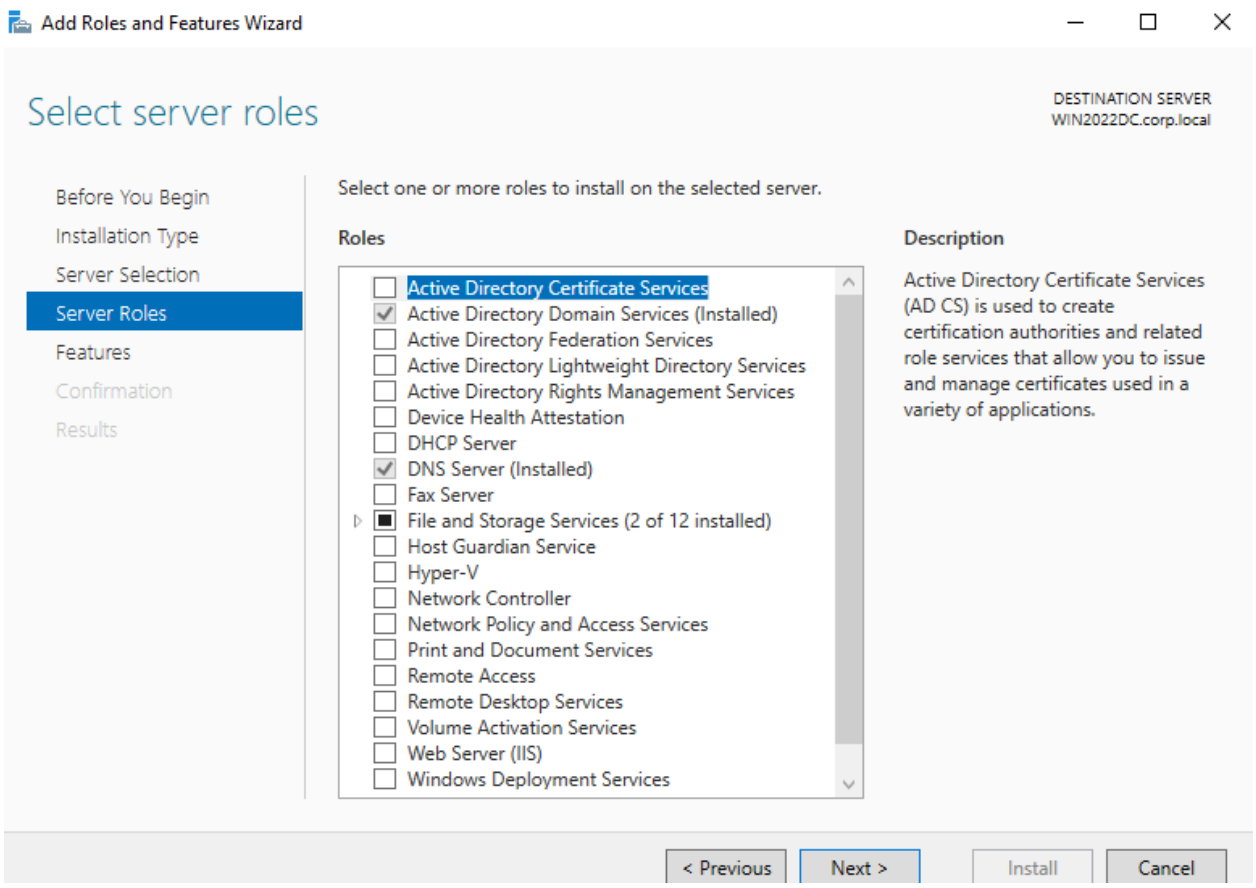
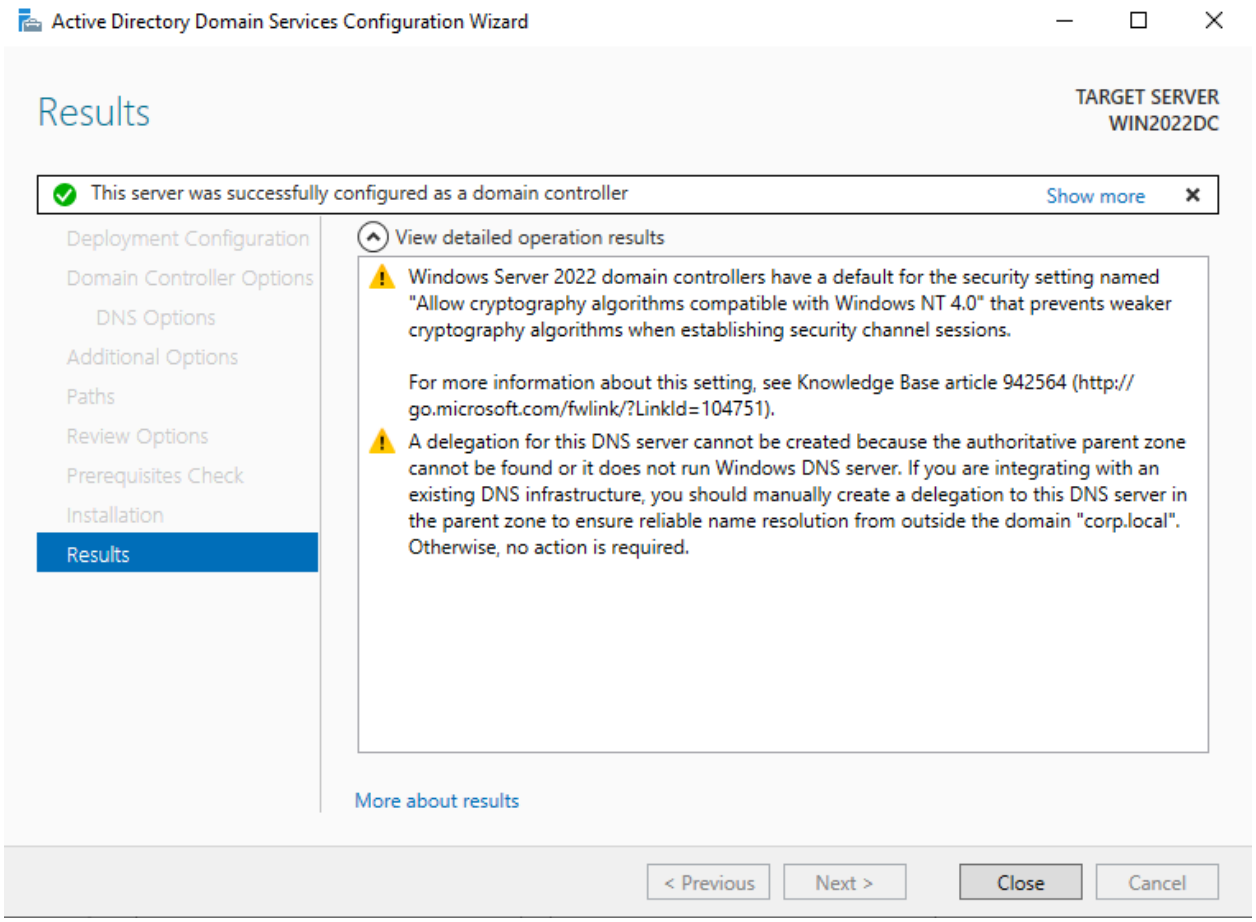
Enterprise-Windows-Server-2022-IT-Infrastructure-Lab Workflow

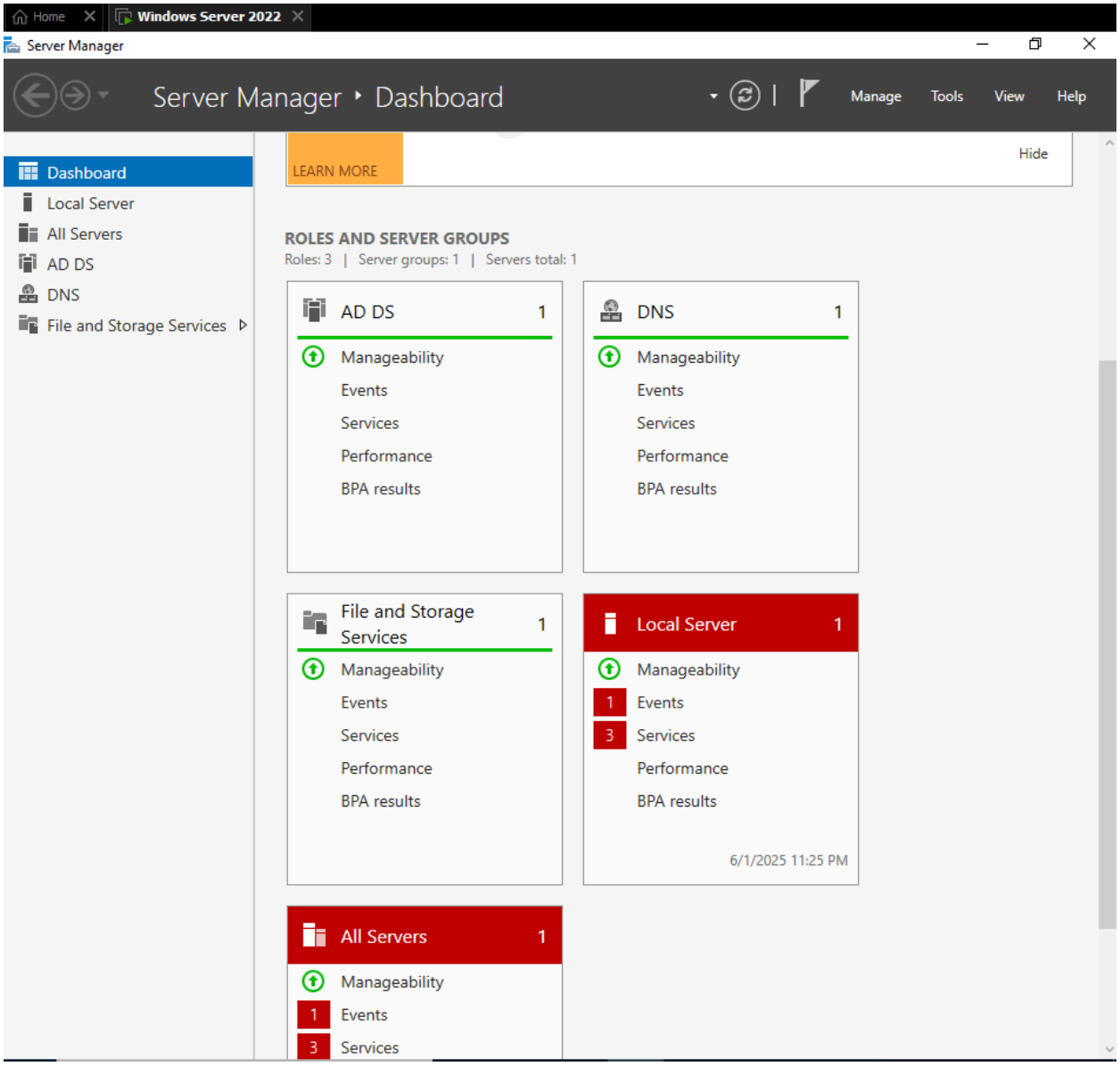
Author: Brennan Tong

Install Active Directory DS and DNS:



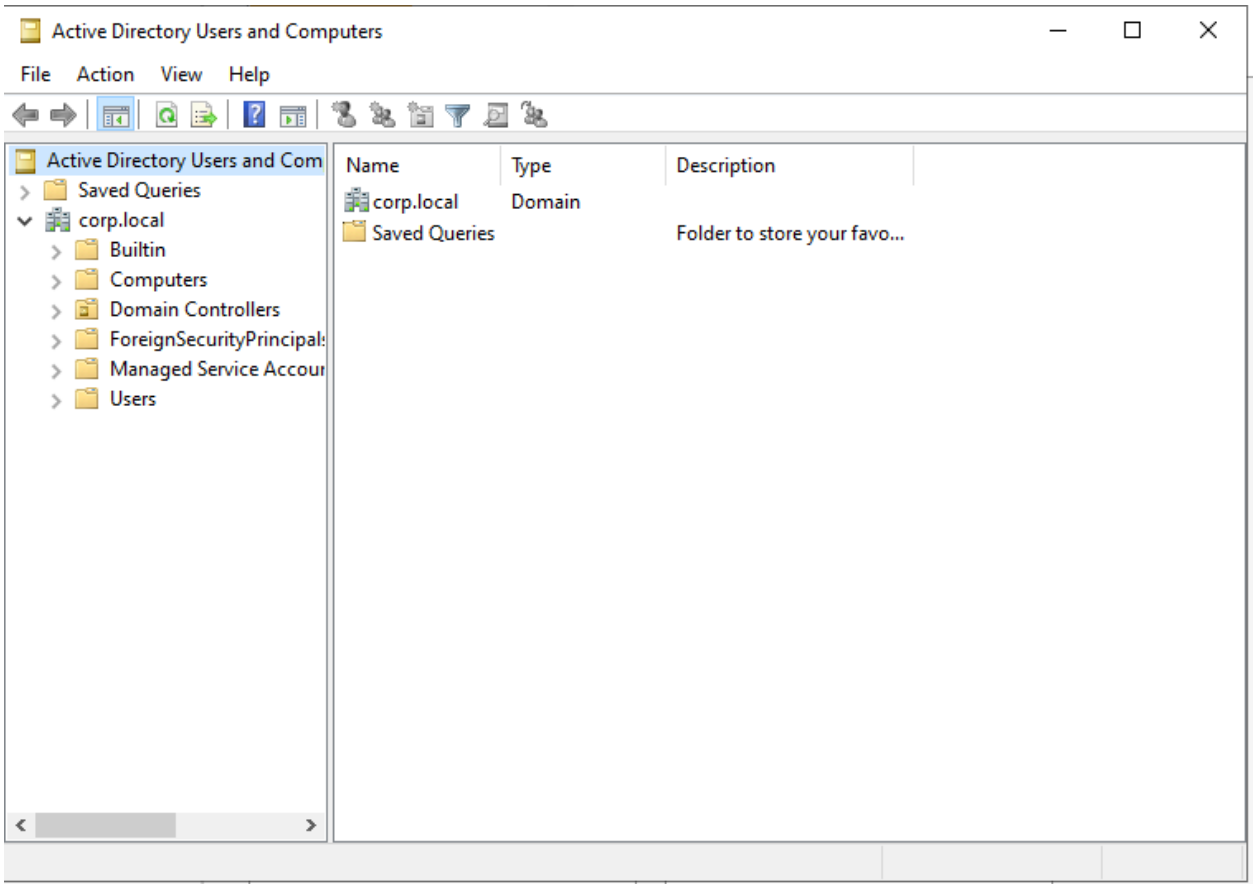

Active Directory Domain Services Configuration Wizard
Results
TARGET SERVER
WIN2022DC
This server was successfully configured as a domain controller
Show more
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
View detailed operation results
Windows Server 2022 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.
For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).
A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "corp.local". Otherwise, no action is required.
More about results
< Previous
Next >
Close
Cancel

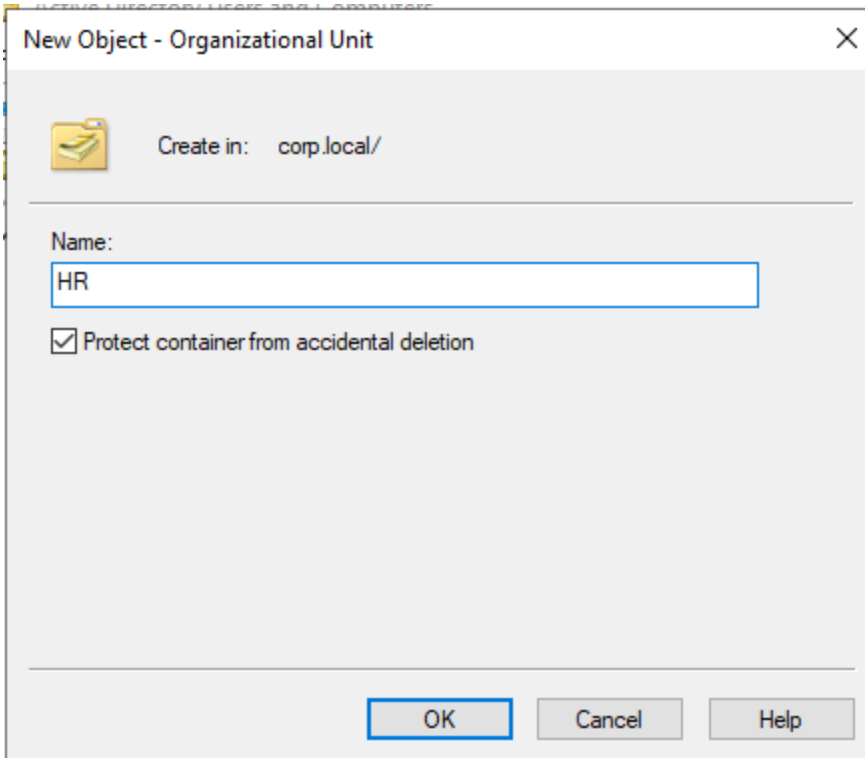
AD DS and DNS installed:

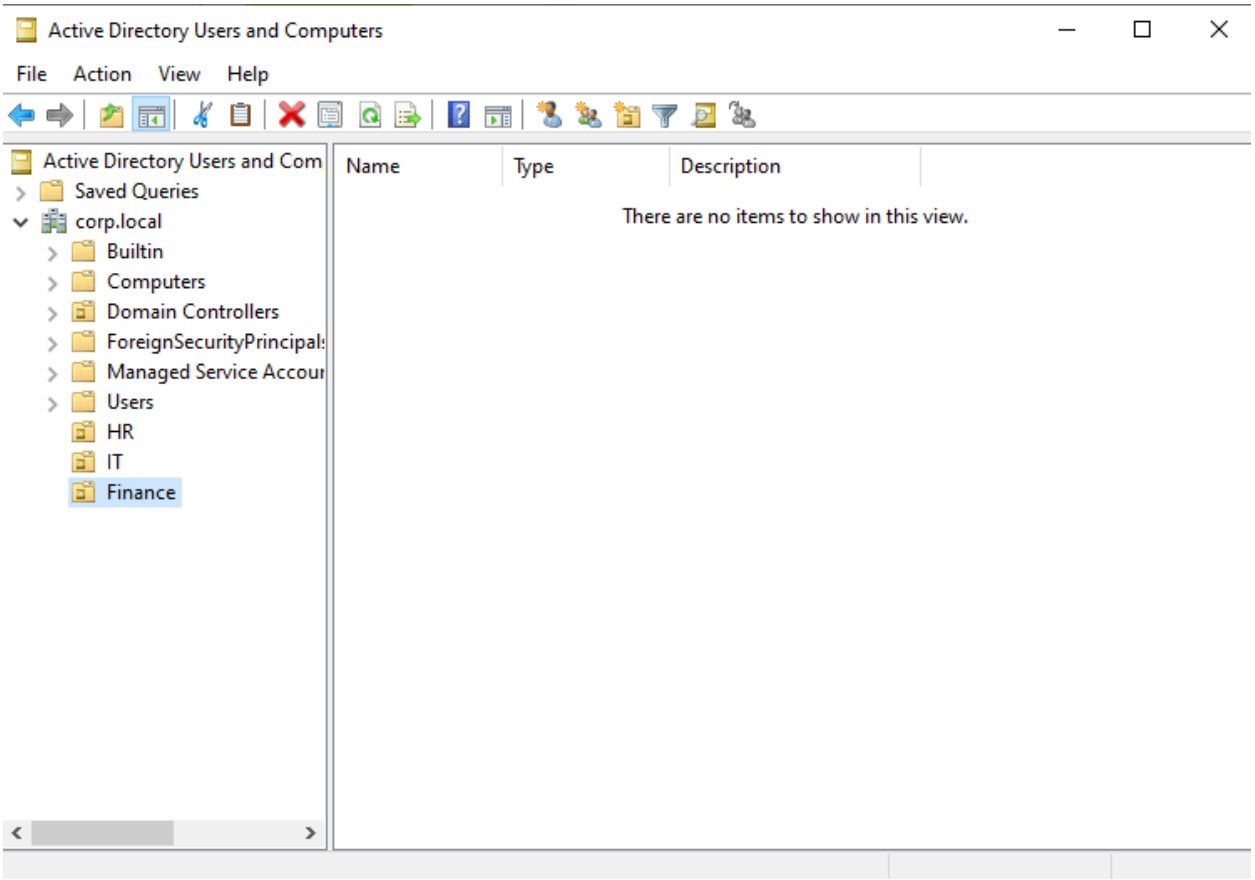


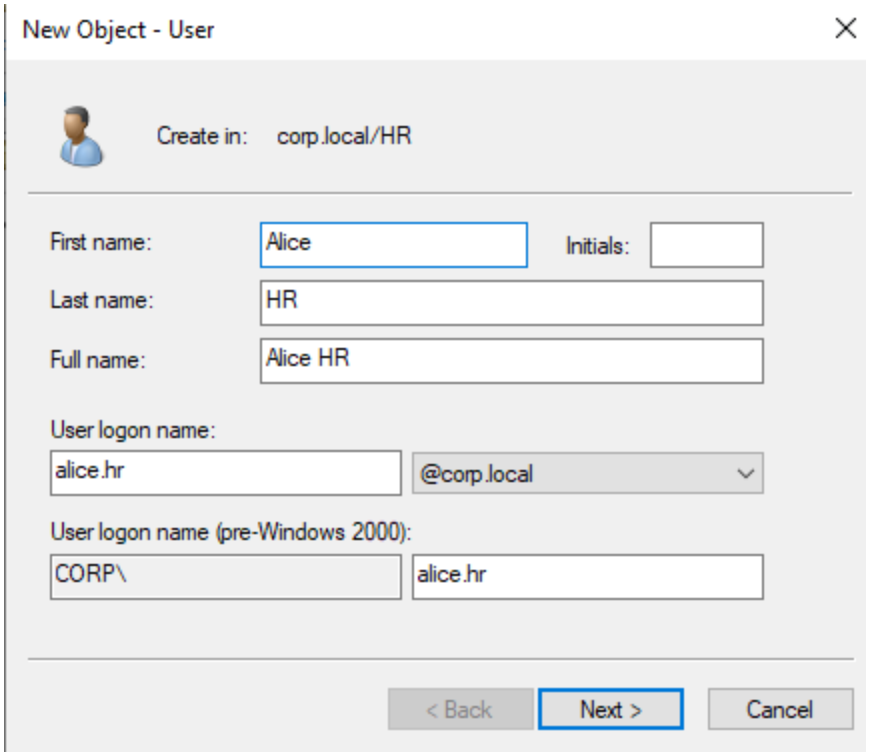
Open Active Directory Users and Computers (ADUC)

Create Users and Groups, HR, IT, Finance

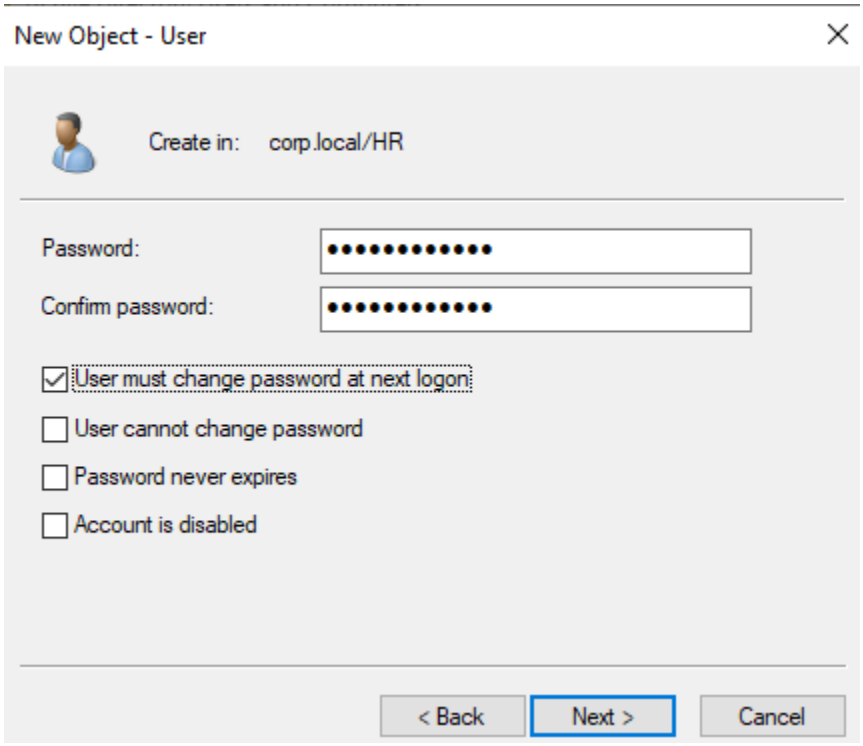


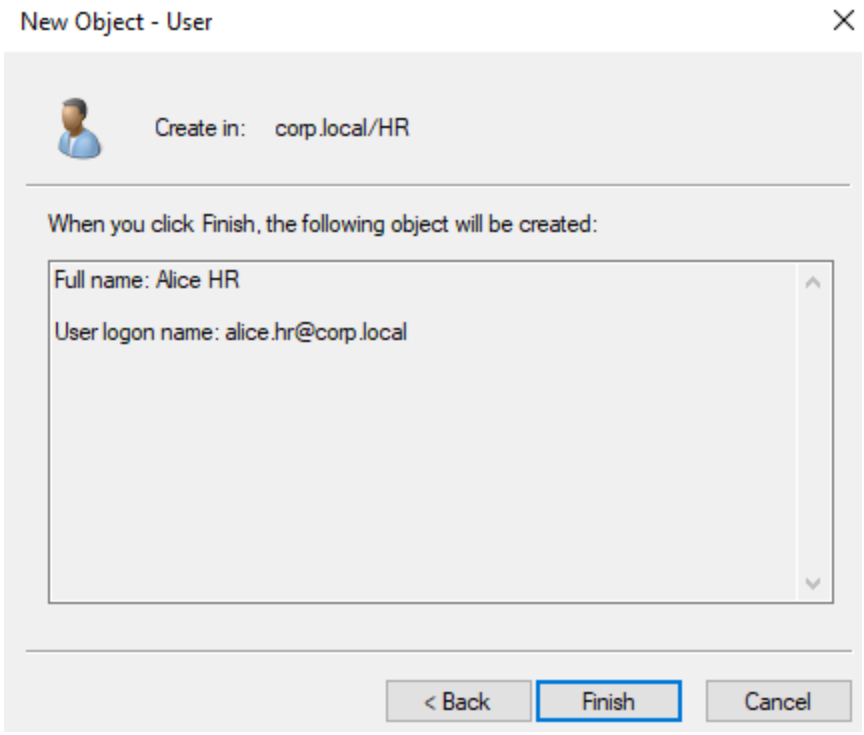

New Object - Organizational Unit
Create in: corp.local/
Name:
HR
Protect container from accidental deletion
OK
Cancel
Help

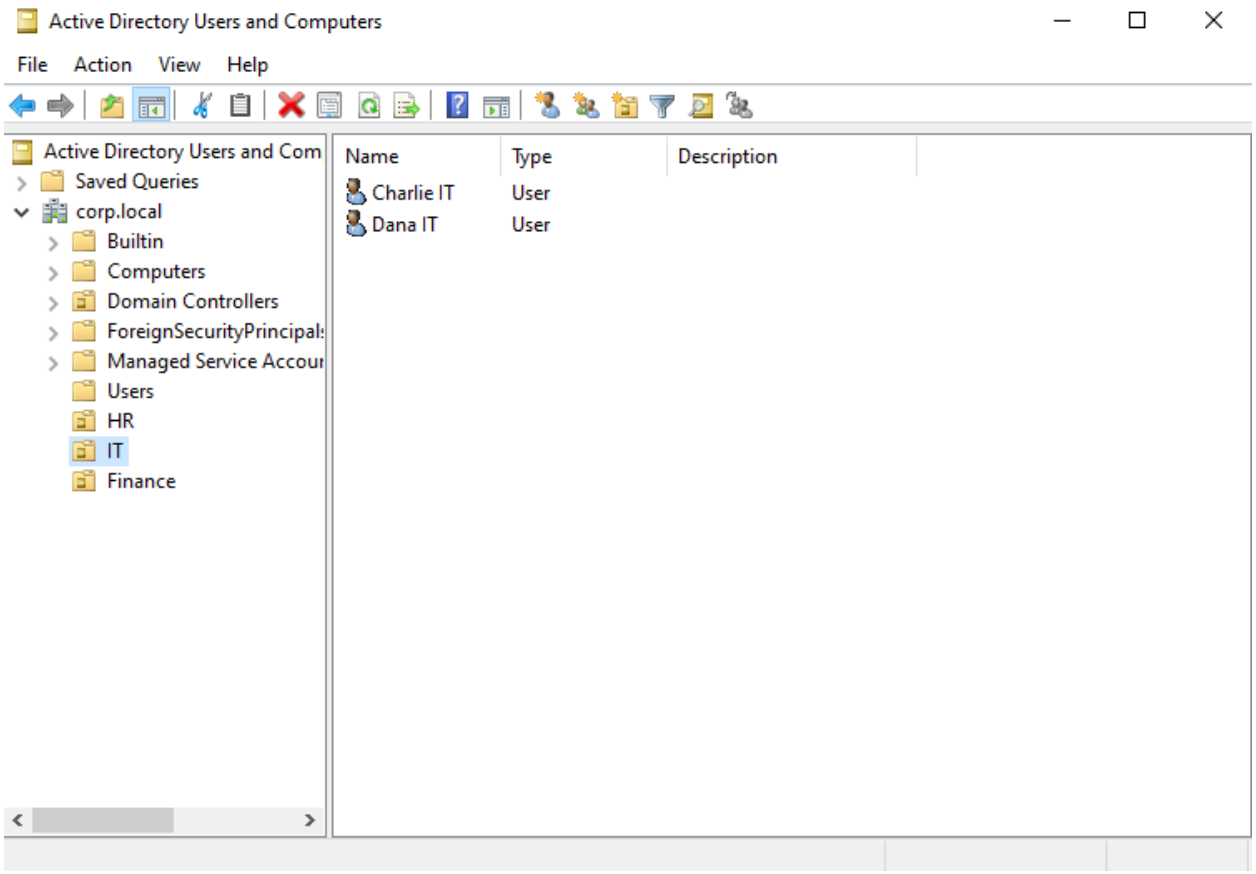

Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
corp.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal
Managed Service Accou
Users
HR
IT
Finance
Name
Type
Description
There are no items to show in this view.

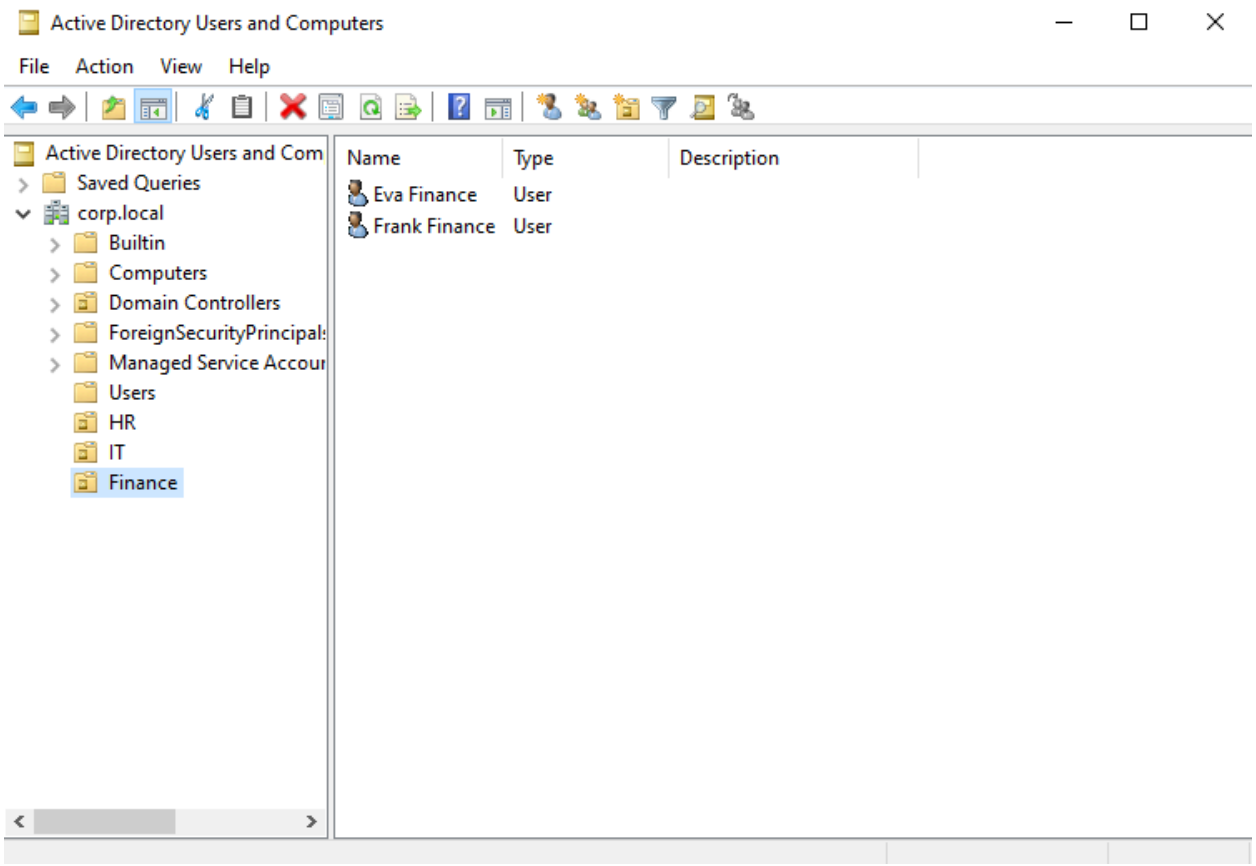


Password123!

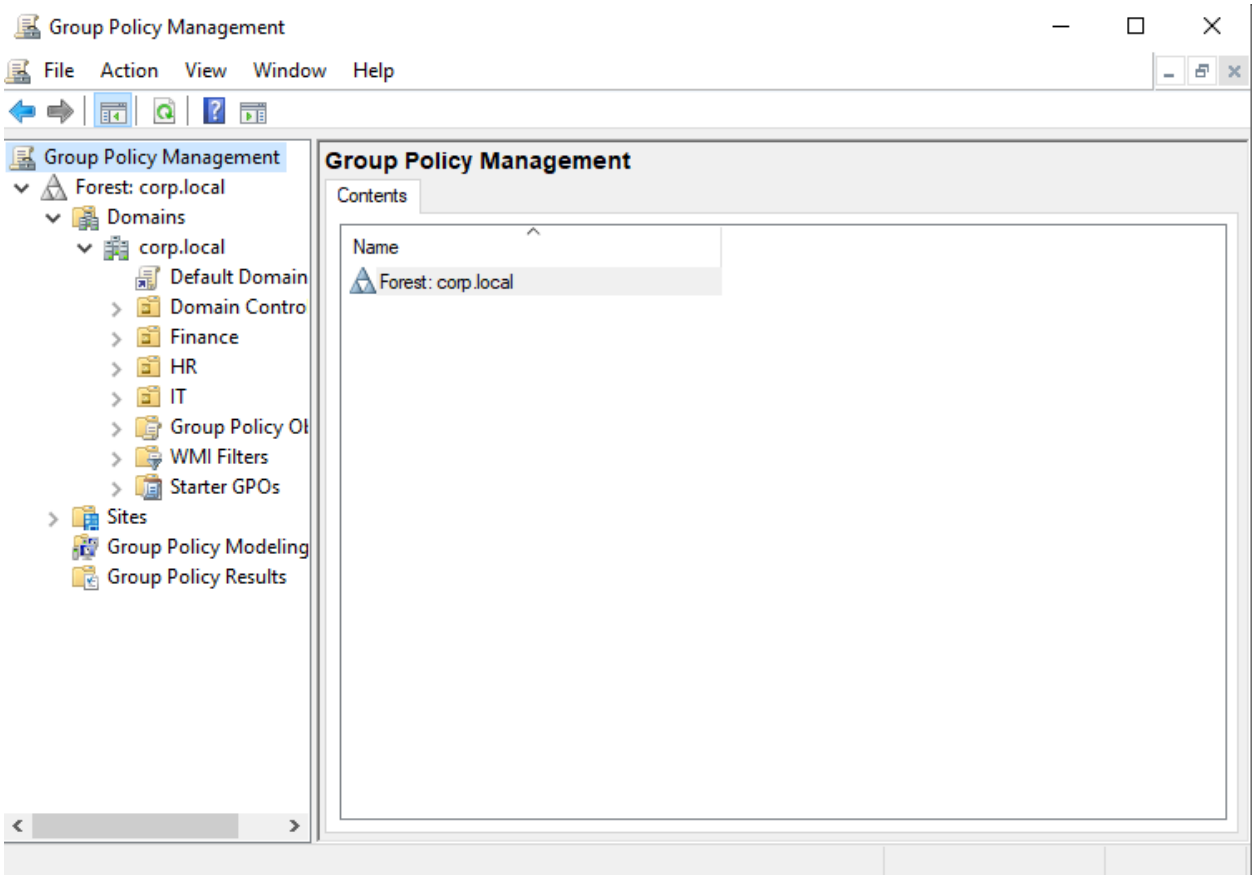


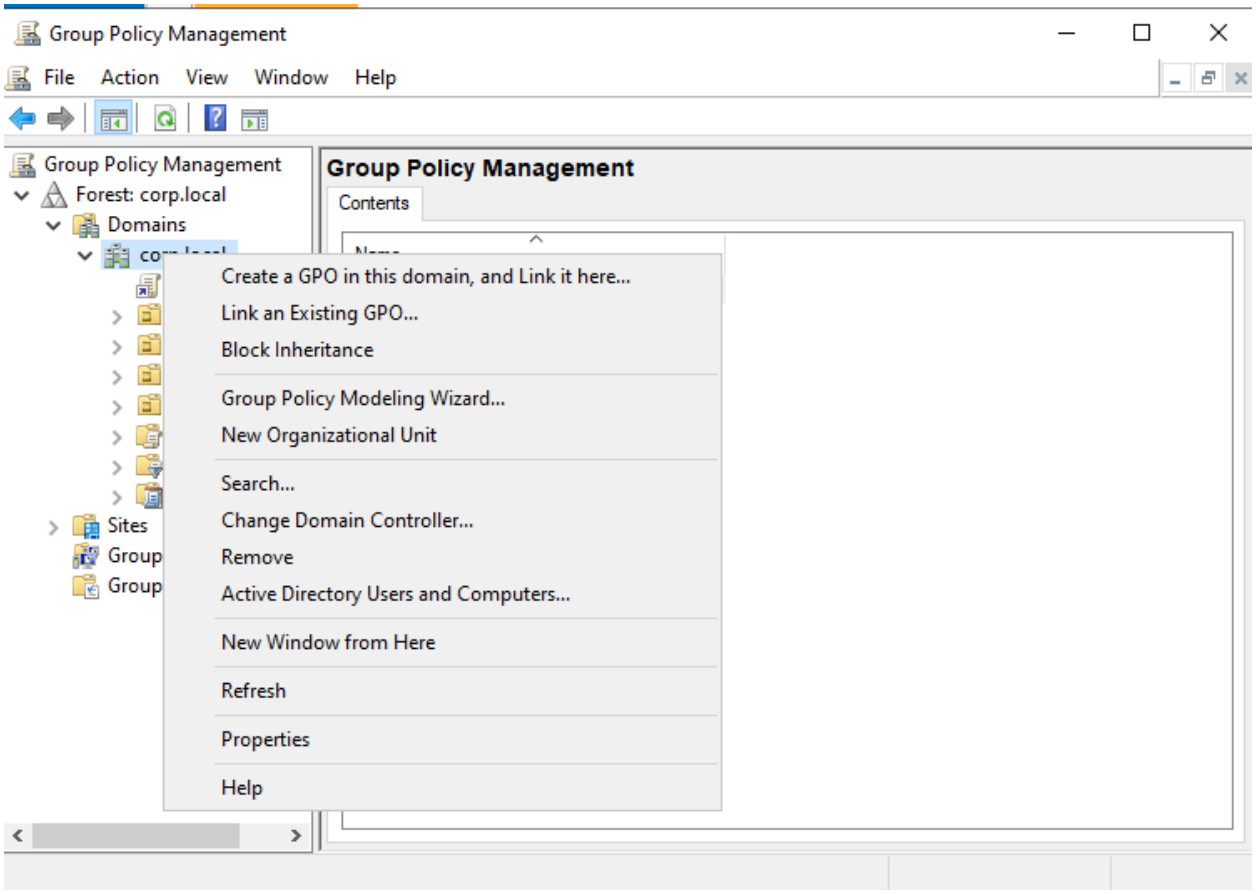

New Object - User
Create in: corp.local/HR
When you click Finish, the following object will be created:
Full name: Alice HR
User logon name: alice.hr@corp.local
< Back
Finish
Cancel

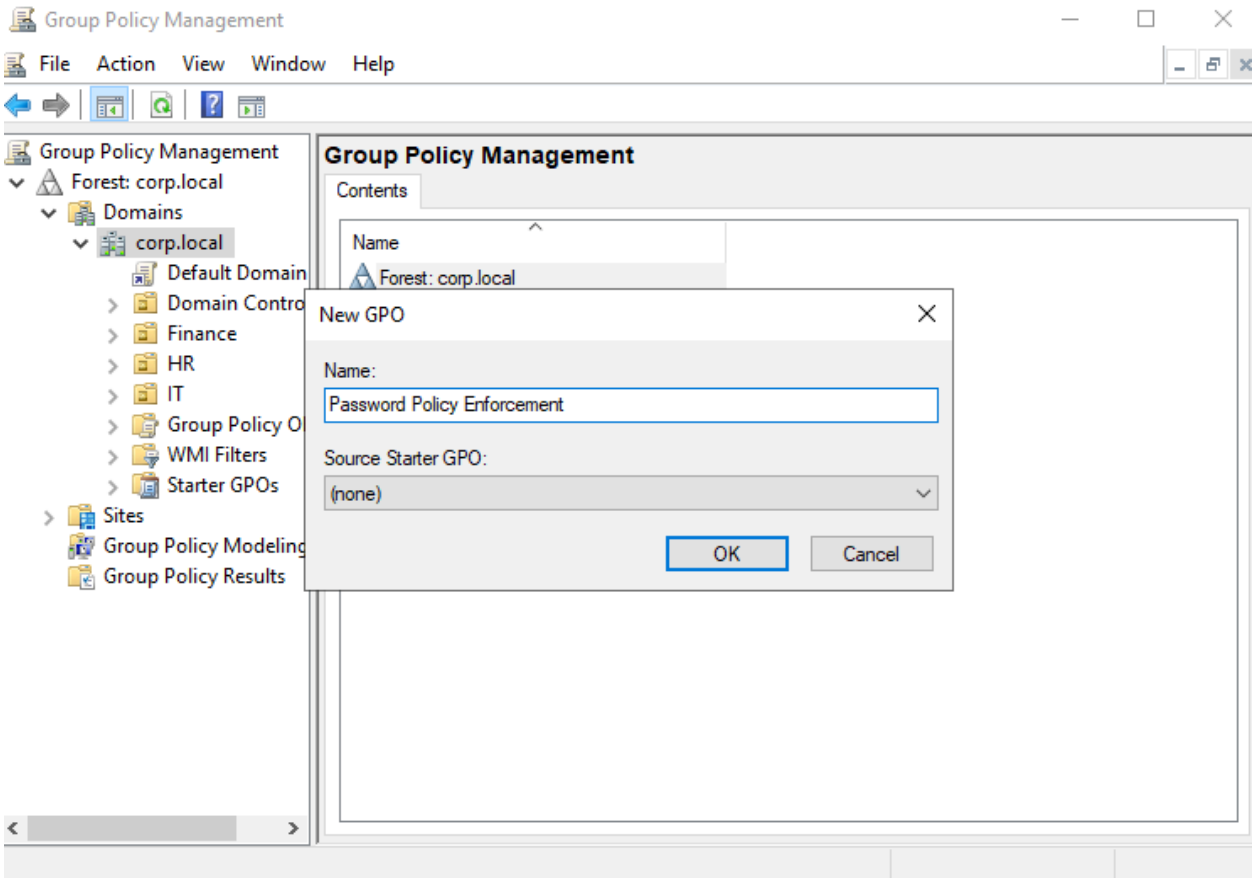

Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Com
Saved Queries
corp.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accour
Users
HR
IT
Finance
Name
Type
Description
Charlie IT
User
Dana IT
User

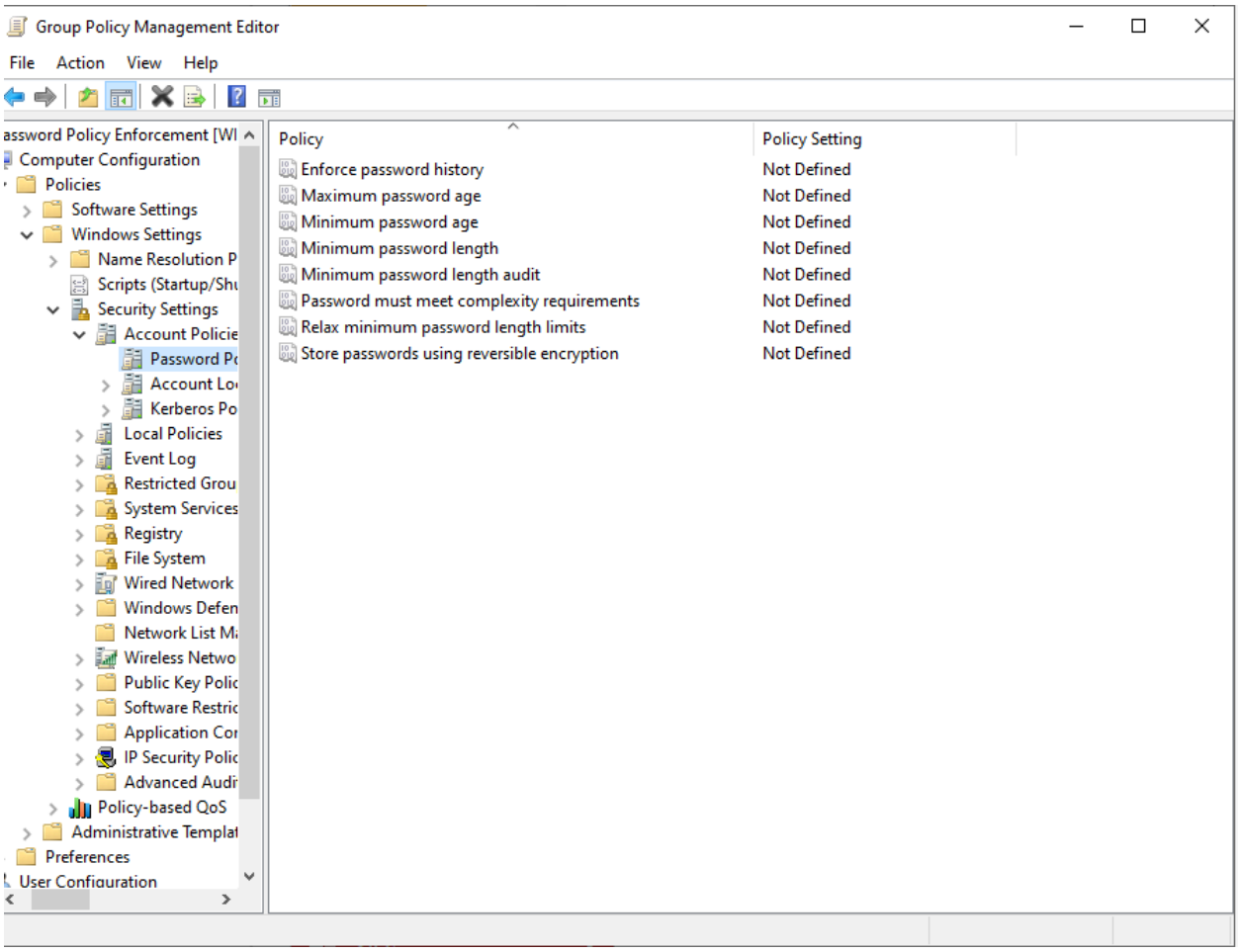

Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Com
Saved Queries
corp.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accour
Users
HR
IT
Finance
Name
Type
Description
Eva Finance
User
Frank Finance
User

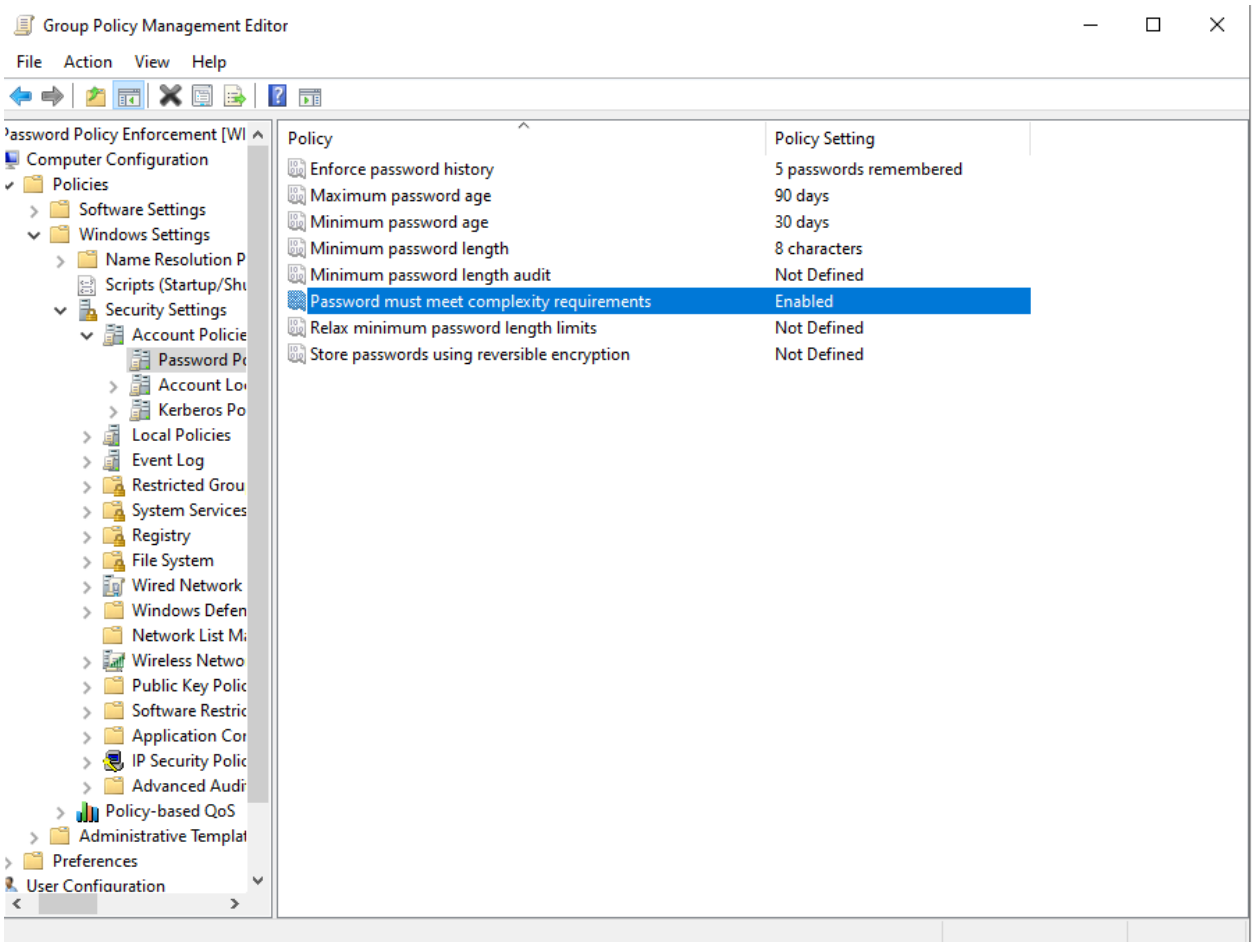
Create Group Policies: Password Policy, Disable USB Storage, Audit Logon Events

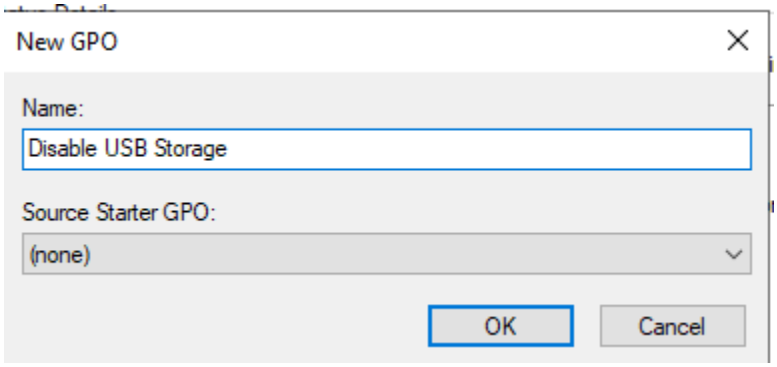


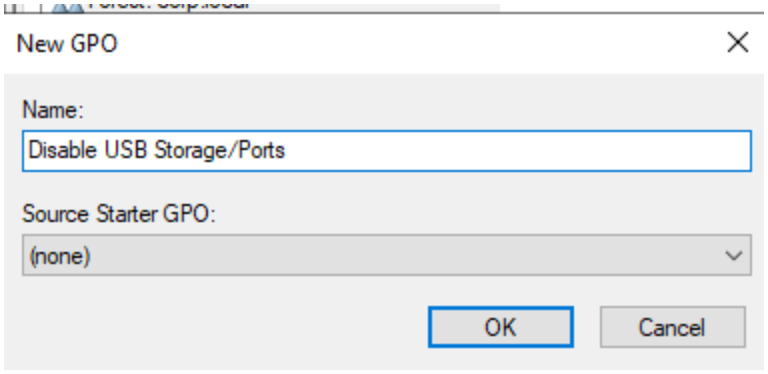

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: corp.local
Domains
Sites
Group
Group
Group Policy Management
Contents
Create a GPO in this domain, and Link it here...
Link an Existing GPO...
Block Inheritance
Group Policy Modeling Wizard...
New Organizational Unit
Search...
Change Domain Controller...
Remove
Active Directory Users and Computers...
New Window from Here
Refresh
Properties
Help

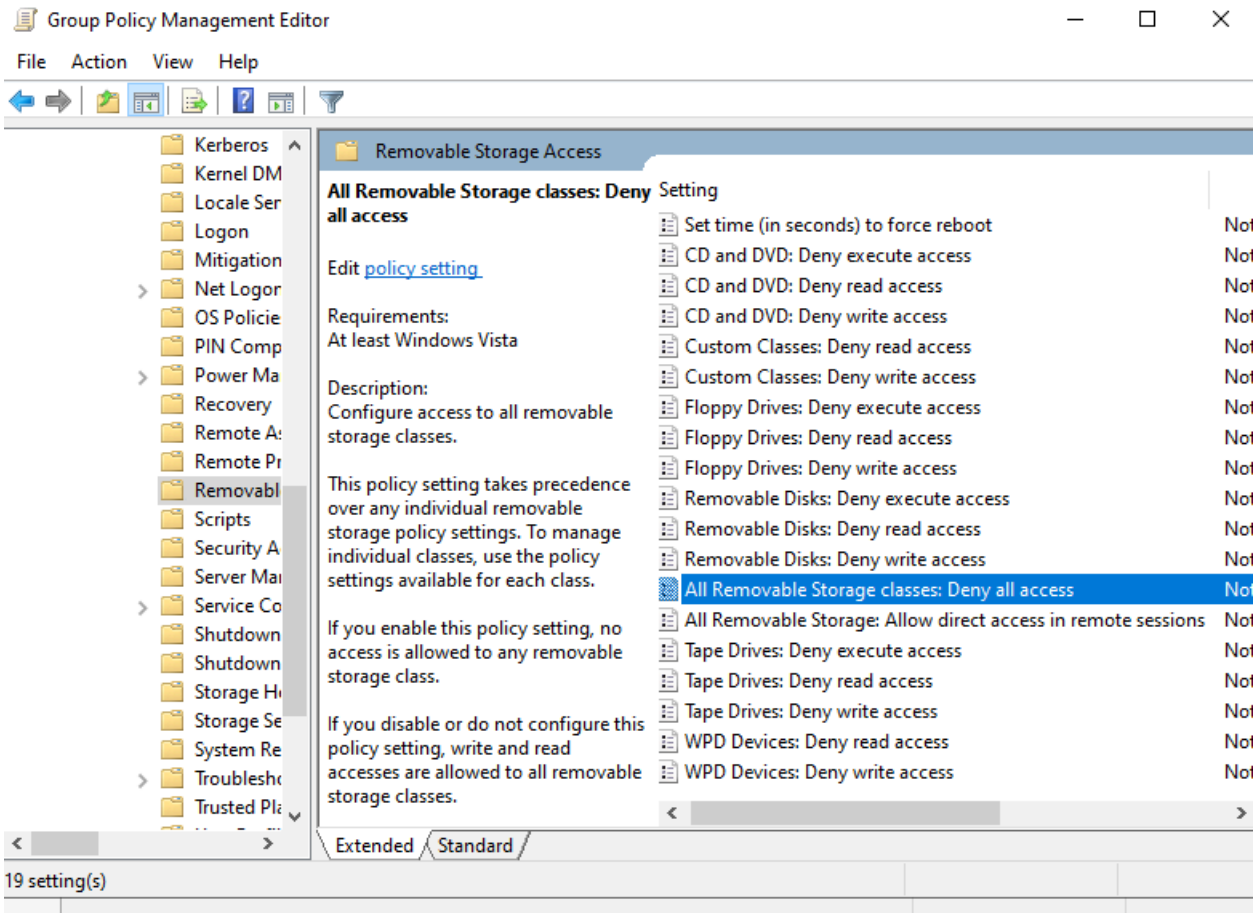

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: corp.local
Domains
corp.local
Default Domain
Domain Contro
Finance
HR
IT
Group Policy O
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Group Policy Management
Contents
Name
Forest: corp.local
New GPO
Name:
Password Policy Enforcement
Source Starter GPO:
(none)
OK
Cancel

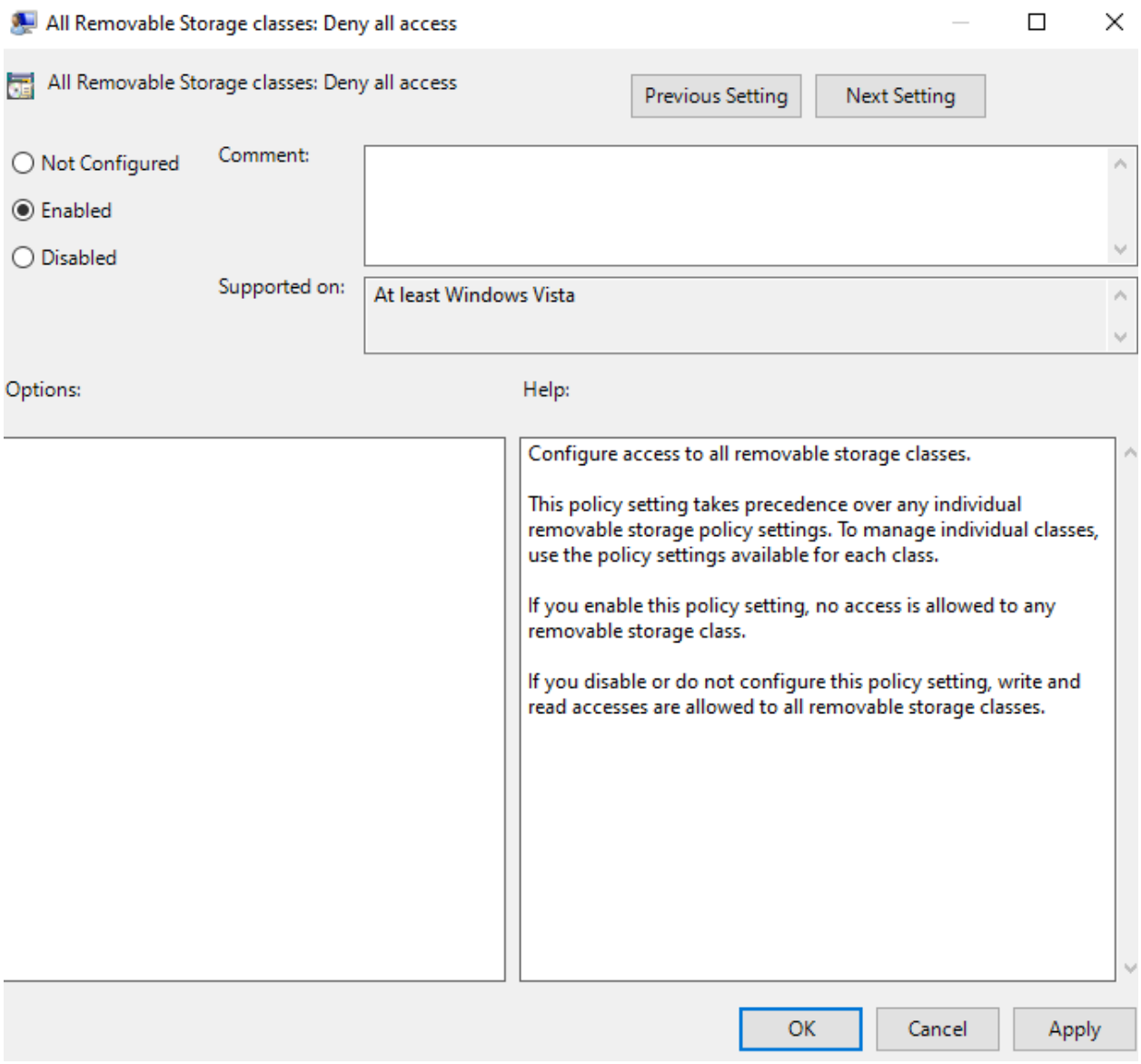

Group Policy Management Editor
File Action View Help
assword Policy Enforcement [WI
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution P
Scripts (Startup/Shu
Security Settings
Account Policie
Password Po
Account Lo
Kerberos Po
Local Policies
Event Log
Restricted Grou
System Services
Registry
File System
Wired Network
Windows Defen
Network List Ma
Wireless Netwo
Public Key Polic
Software Restric
Application Cor
IP Security Polic
Advanced Audi
Policy-based QoS
Administrative Templat
Preferences
User Configuration
Policy
Policy Setting
Enforce password history
Not Defined
Maximum password age
Not Defined
Minimum password age
Not Defined
Minimum password length
Not Defined
Minimum password length audit
Not Defined
Password must meet complexity requirements
Not Defined
Relax minimum password length limits
Not Defined
Store passwords using reversible encryption
Not Defined

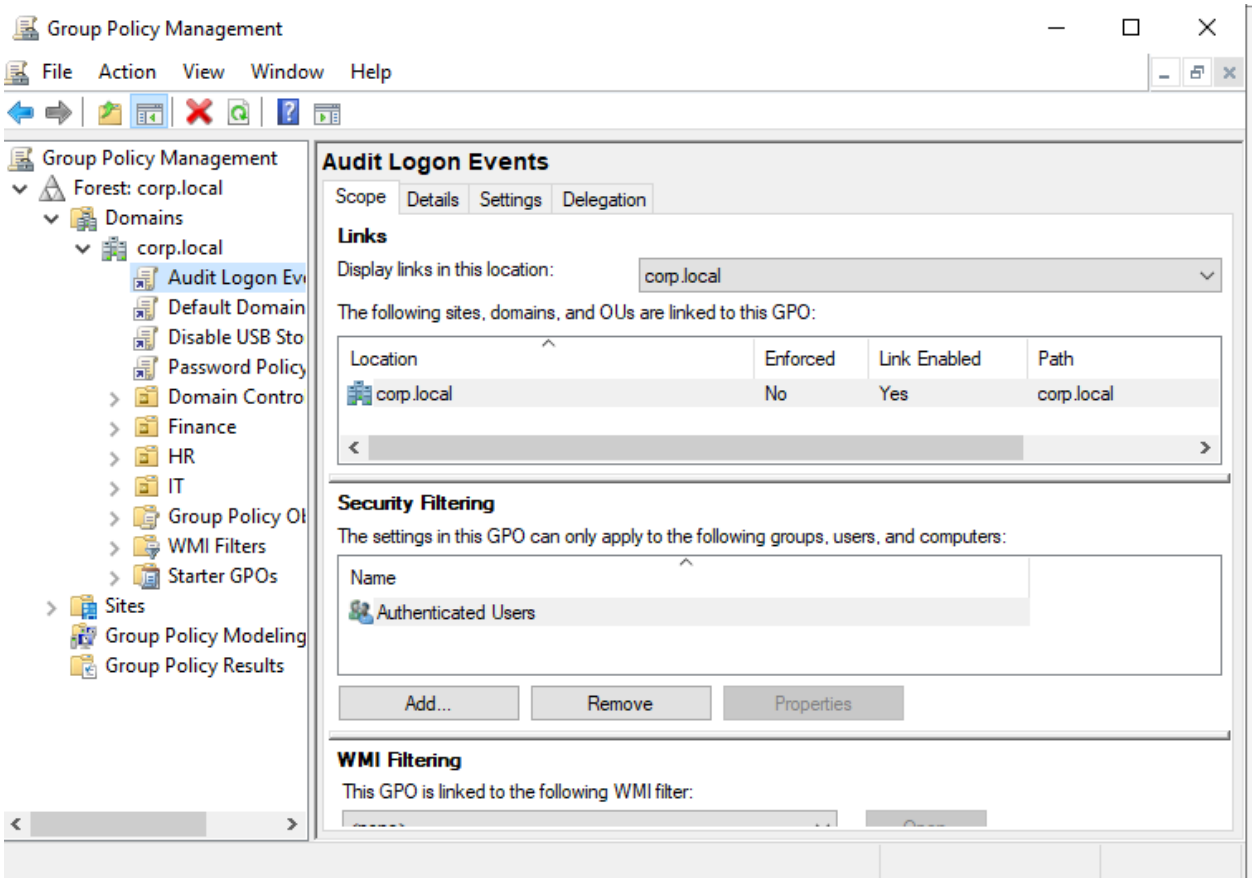

Group Policy Management Editor
File Action View Help
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution P
Scripts (Startup/Shu
Security Settings
Account Policie
Password Po
Account Lo
Kerberos Po
Local Policies
Event Log
Restricted Grou
System Services
Registry
File System
Wired Network
Windows Defen
Network List Ma
Wireless Netwo
Public Key Polic
Software Restric
Application Cor
IP Security Polic
Advanced Audi
Policy-based QoS
Administrative Templat
Preferences
User Configuration
Policy
Policy Setting
Enforce password history
5 passwords remembered
Maximum password age
90 days
Minimum password age
30 days
Minimum password length
8 characters
Minimum password length audit
Not Defined
Password must meet complexity requirements
Enabled
Relax minimum password length limits
Not Defined
Store passwords using reversible encryption
Not Defined

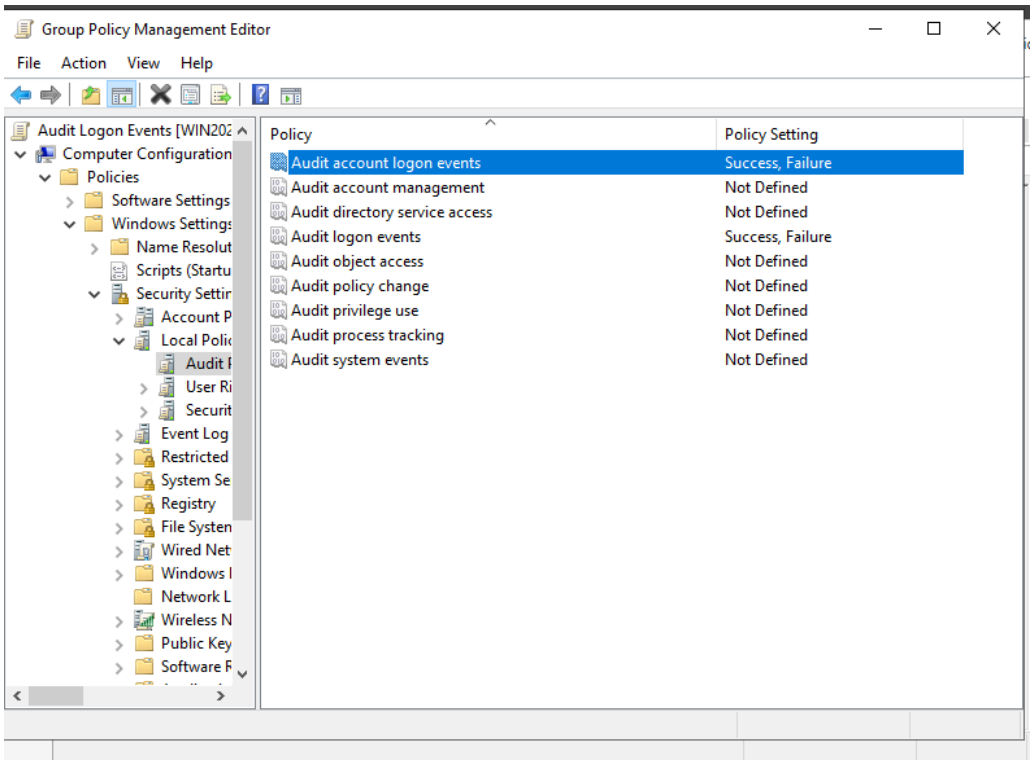

New GPO
Name:
Disable USB Storage
Source Starter GPO:
(none)
OK
Cancel

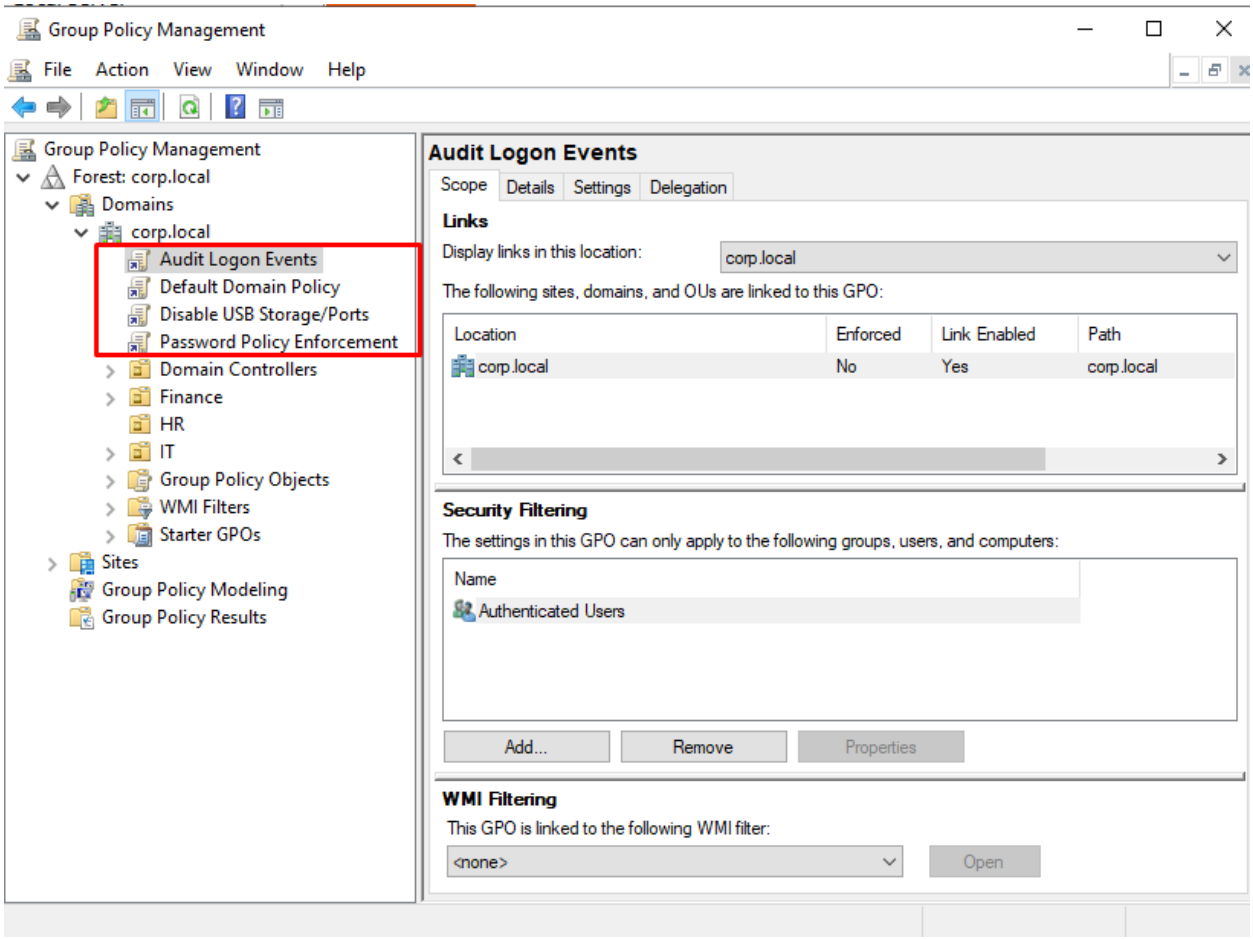

New GPO
Name:
Disable USB Storage/Ports
Source Starter GPO:
(none)
OK
Cancel


Group Policy Management Editor
File Action View Help
Kerberos
Kernel DM
Locale Ser
Logon
Mitigation
Net Logor
OS Policie
PIN Comp
Power Ma
Recovery
Remote A
Remote Pr
Removabl
Scripts
Security A
Server Ma
Service Co
Shutdown
Shutdown
Storage H
Storage Se
System Re
Troublesh
Trusted Pl
Removable Storage Access
All Removable Storage classes: Deny all access
Edit policy setting
Requirements:
At least Windows Vista
Description:
Configure access to all removable storage classes.
This policy setting takes precedence over any individual removable storage policy settings. To manage individual classes, use the policy settings available for each class.
If you enable this policy setting, no access is allowed to any removable storage class.
If you disable or do not configure this policy setting, write and read accesses are allowed to all removable storage classes.
Setting
Set time (in seconds) to force reboot
CD and DVD: Deny execute access
CD and DVD: Deny read access
CD and DVD: Deny write access
Custom Classes: Deny read access
Custom Classes: Deny write access
Floppy Drives: Deny execute access
Floppy Drives: Deny read access
Floppy Drives: Deny write access
Removable Disks: Deny execute access
Removable Disks: Deny read access
Removable Disks: Deny write access
All Removable Storage classes: Deny all access
All Removable Storage: Allow direct access in remote sessions
Tape Drives: Deny execute access
Tape Drives: Deny read access
Tape Drives: Deny write access
WPD Devices: Deny read access
WPD Devices: Deny write access
Extended
Standard
19 setting(s)


All Removable Storage classes: Deny all access
All Removable Storage classes: Deny all access
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Windows Vista
Options:
Help:
Configure access to all removable storage classes.
This policy setting takes precedence over any individual removable storage policy settings. To manage individual classes, use the policy settings available for each class.
If you enable this policy setting, no access is allowed to any removable storage class.
If you disable or do not configure this policy setting, write and read accesses are allowed to all removable storage classes.
OK
Cancel
Apply

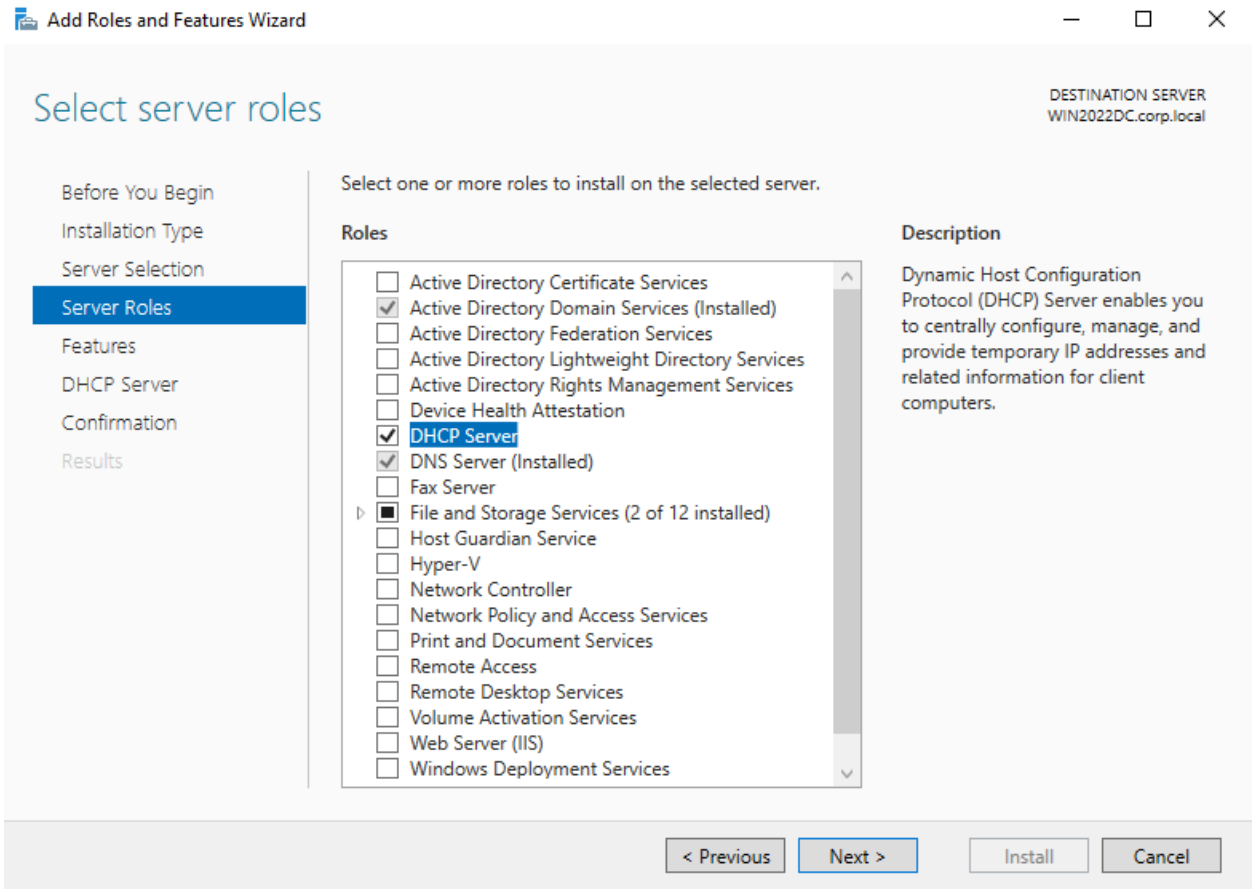

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: corp.local
Domains
corp.local
Audit Logon Ev
Default Domain
Disable USB Sto
Password Policy
Domain Contro
Finance
HR
IT
Group Policy Ob
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Audit Logon Events
Scope Details Settings Delegation
Links
Display links in this location: corp.local
The following sites, domains, and OUs are linked to this GPO:
Location Enforced Link Enabled Path
corp.local No Yes corp.local
Security Filtering
The settings in this GPO can only apply to the following groups, users, and computers:
Name
Authenticated Users
Add... Remove Properties
WMI Filtering
This GPO is linked to the following WMI filter:

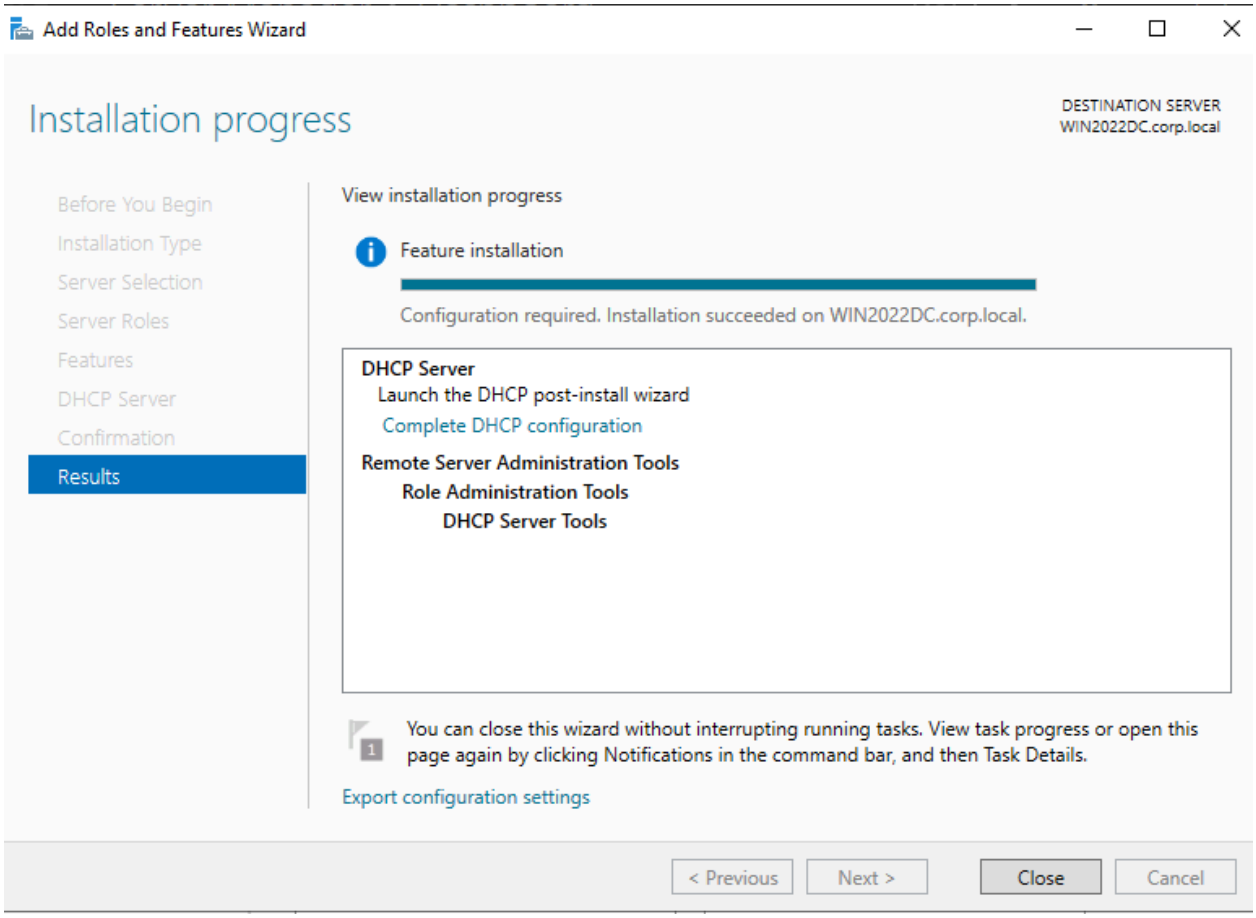

Group Policy Management Editor
File Action View Help
Audit Logon Events [WIN202
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolut
Scripts (Startu
Security Settir
Account P
Local Polic
Audit P
User Ri
Securit
Event Log
Restricted
System Se
Registry
File Systen
Wired Net
Windows I
Network L
Wireless N
Public Key
Software R
Policy
Policy Setting
Audit account logon events Success, Failure
Audit account management Not Defined
Audit directory service access Not Defined
Audit logon events Success, Failure
Audit object access Not Defined
Audit policy change Not Defined
Audit privilege use Not Defined
Audit process tracking Not Defined
Audit system events Not Defined

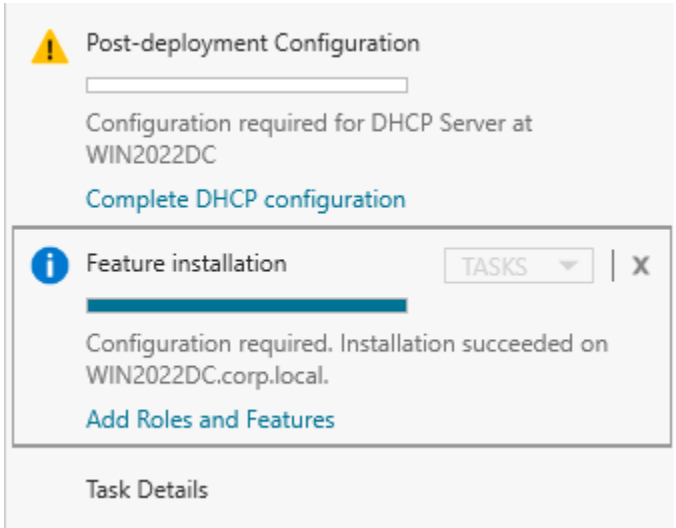


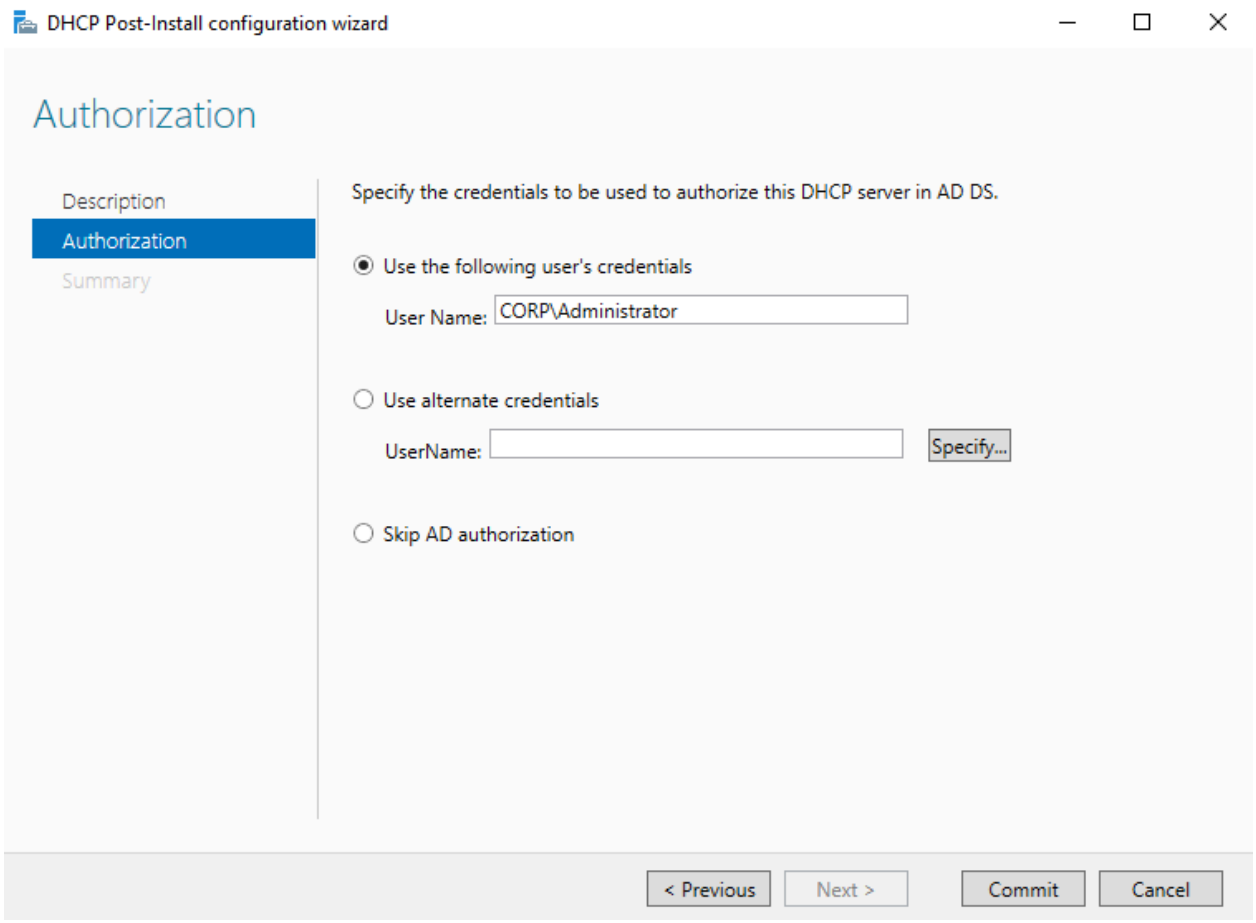
GPOs Successfully Created

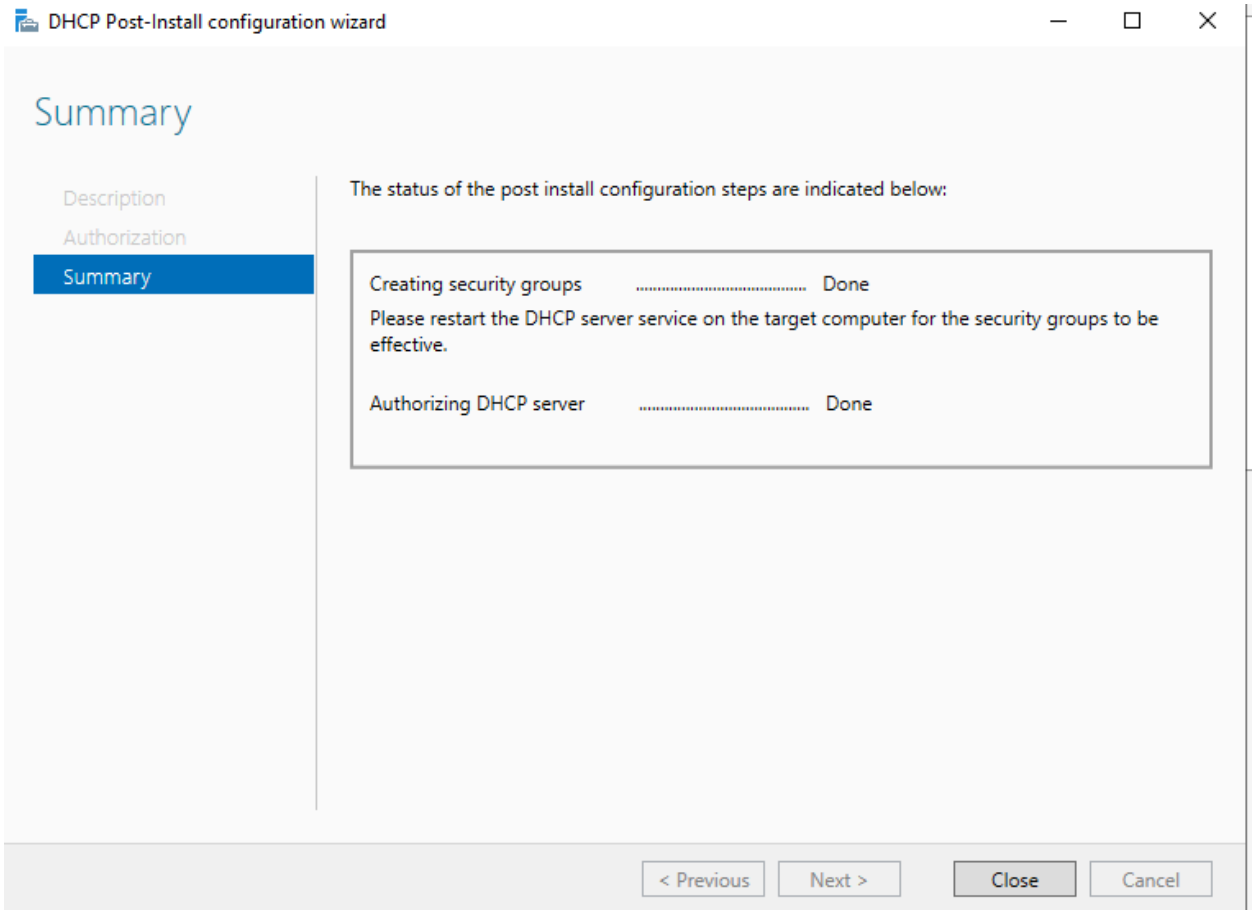
Install DHCP

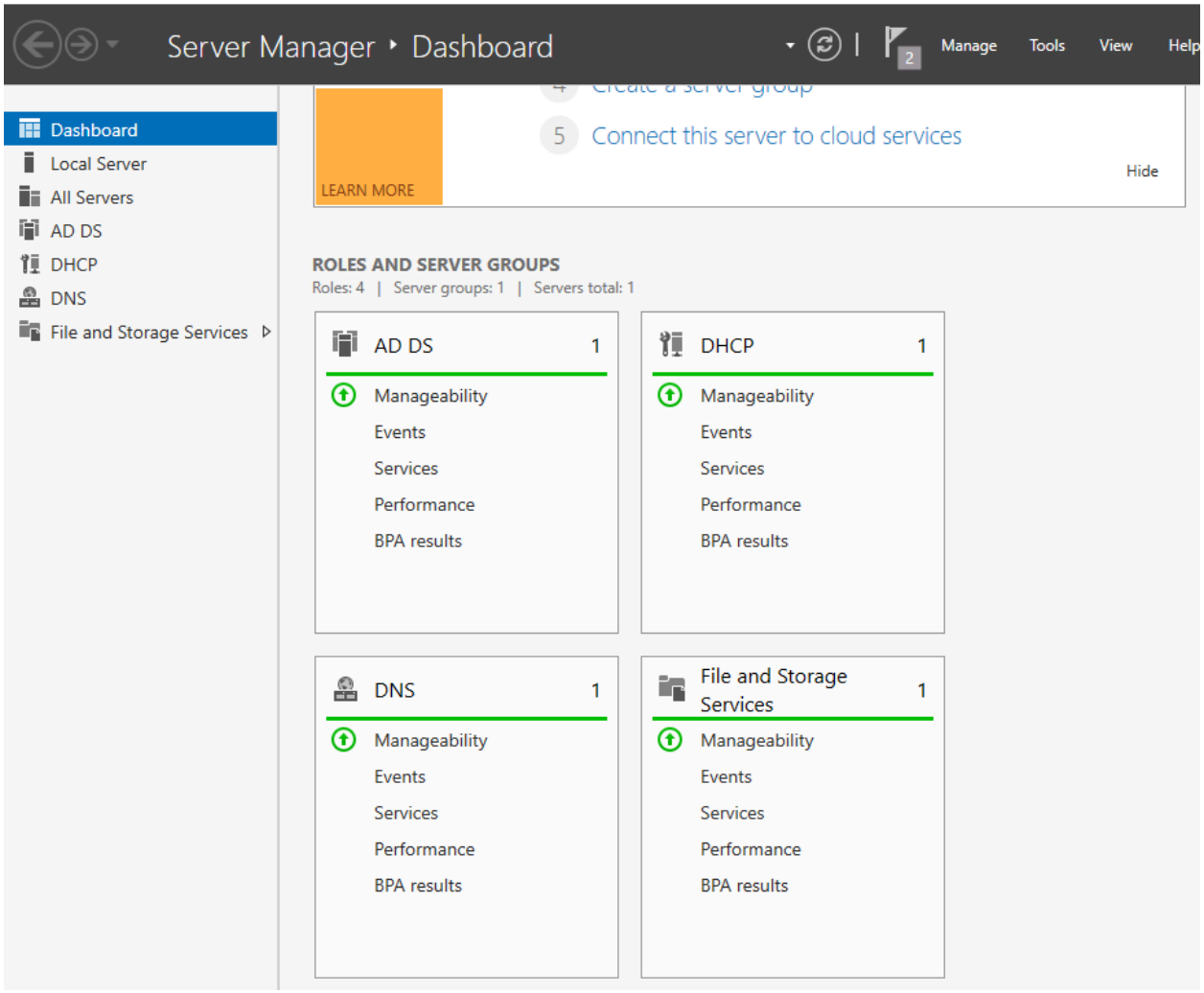



Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
WIN2022DC.corp.local
Before You Begin
Installation Type
Server Selection
Server Roles
Features
DHCP Server
Confirmation
Results
View installation progress
Feature installation
Configuration required. Installation succeeded on WIN2022DC.corp.local.
DHCP Server
Launch the DHCP post-install wizard
Complete DHCP configuration
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
< Previous
Next >
Close
Cancel


Post-deployment Configuration
Configuration required for DHCP Server at WIN2022DC
Complete DHCP configuration
Feature installation
TASKS
Configuration required. Installation succeeded on WIN2022DC.corp.local.
Add Roles and Features
Task Details

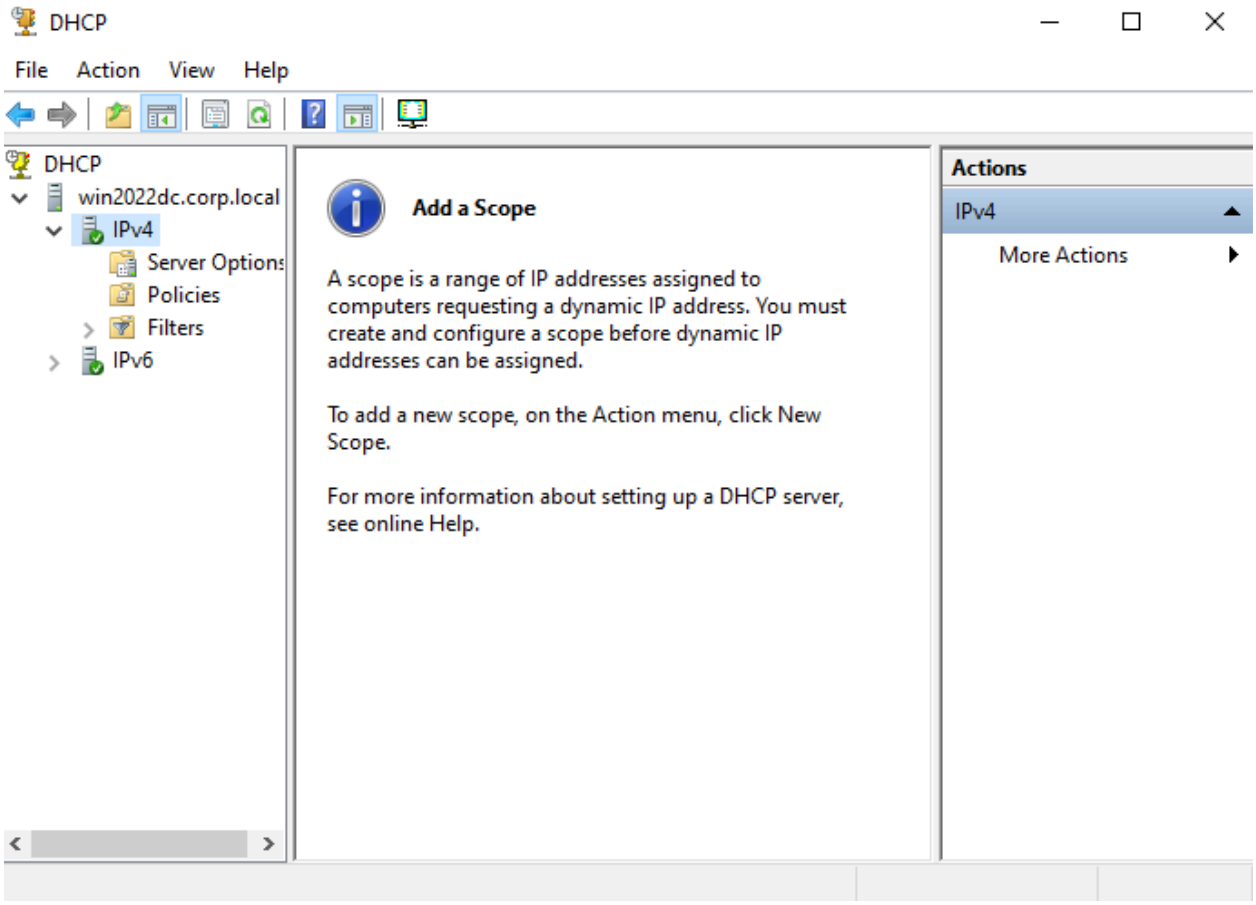

DHCP Post-Install configuration wizard
Authorization
Description
Authorization
Summary
Specify the credentials to be used to authorize this DHCP server in AD DS.
Use the following user's credentials
User Name:
CORP\Administrator
Use alternate credentials
UserName:
Specify...
Skip AD authorization
< Previous
Next >
Commit
Cancel

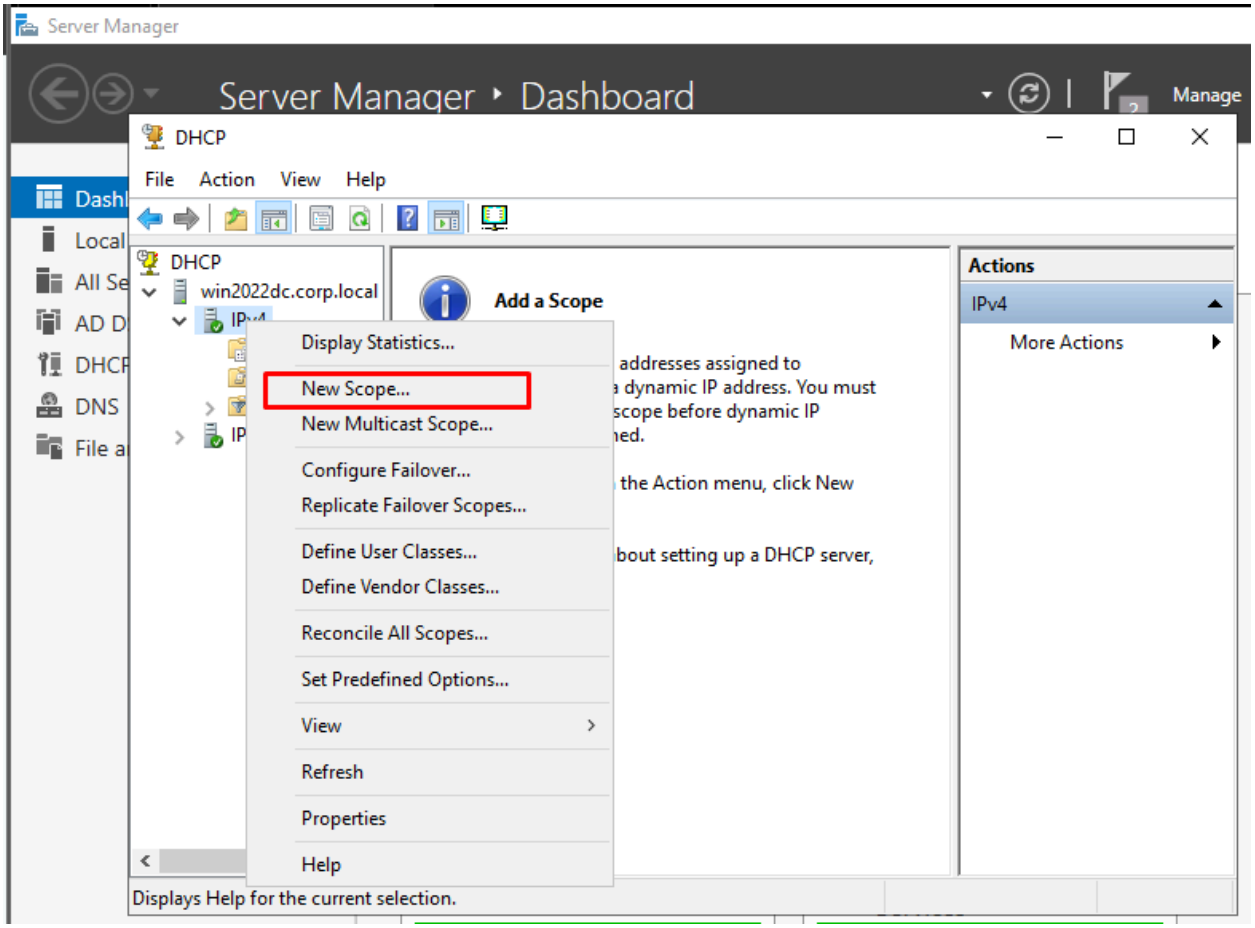

DHCP Post-Install configuration wizard
Summary
Description
Authorization
Summary
The status of the post install configuration steps are indicated below:
Creating security groups ..... Done
Please restart the DHCP server service on the target computer for the security groups to be effective.
Authorizing DHCP server ..... Done
< Previous
Next >
Close
Cancel

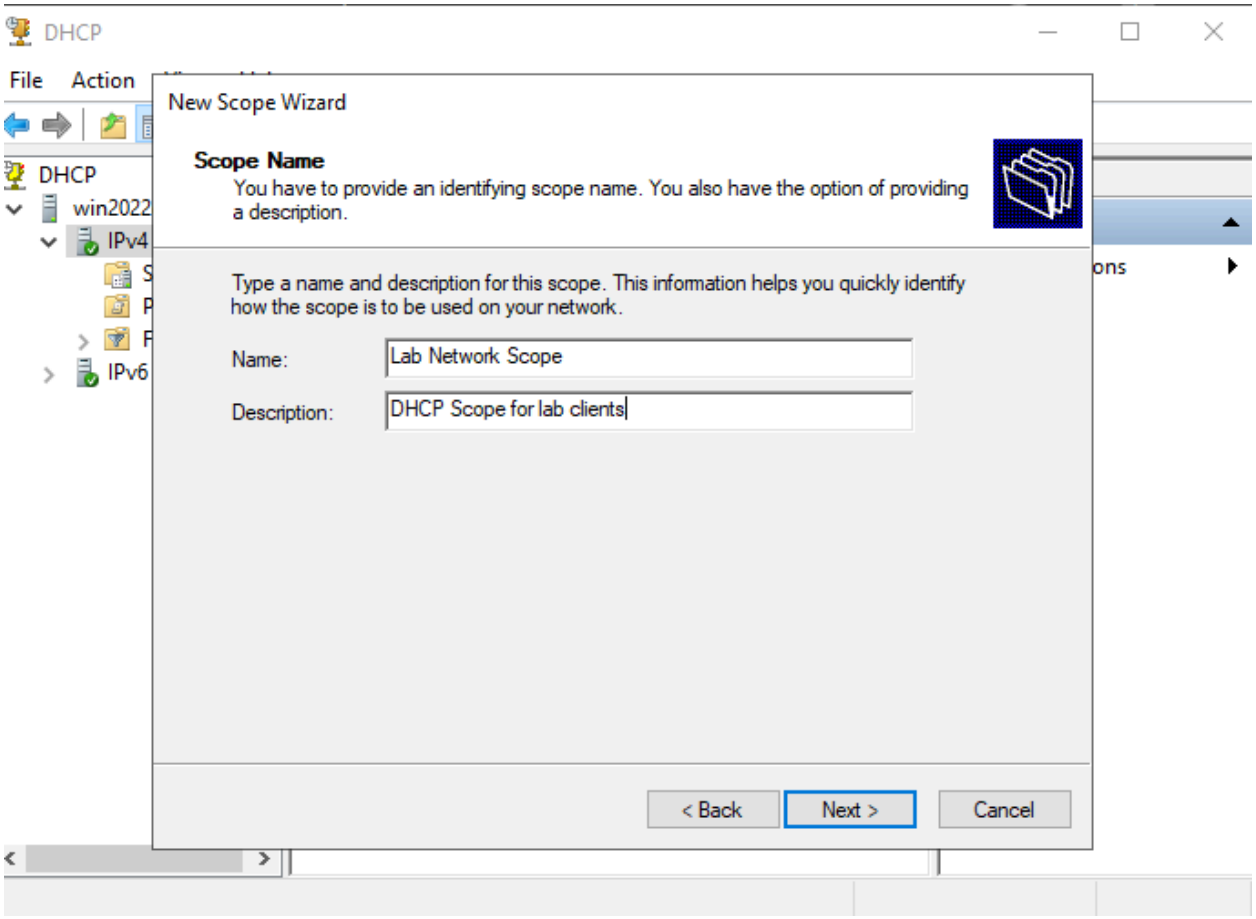


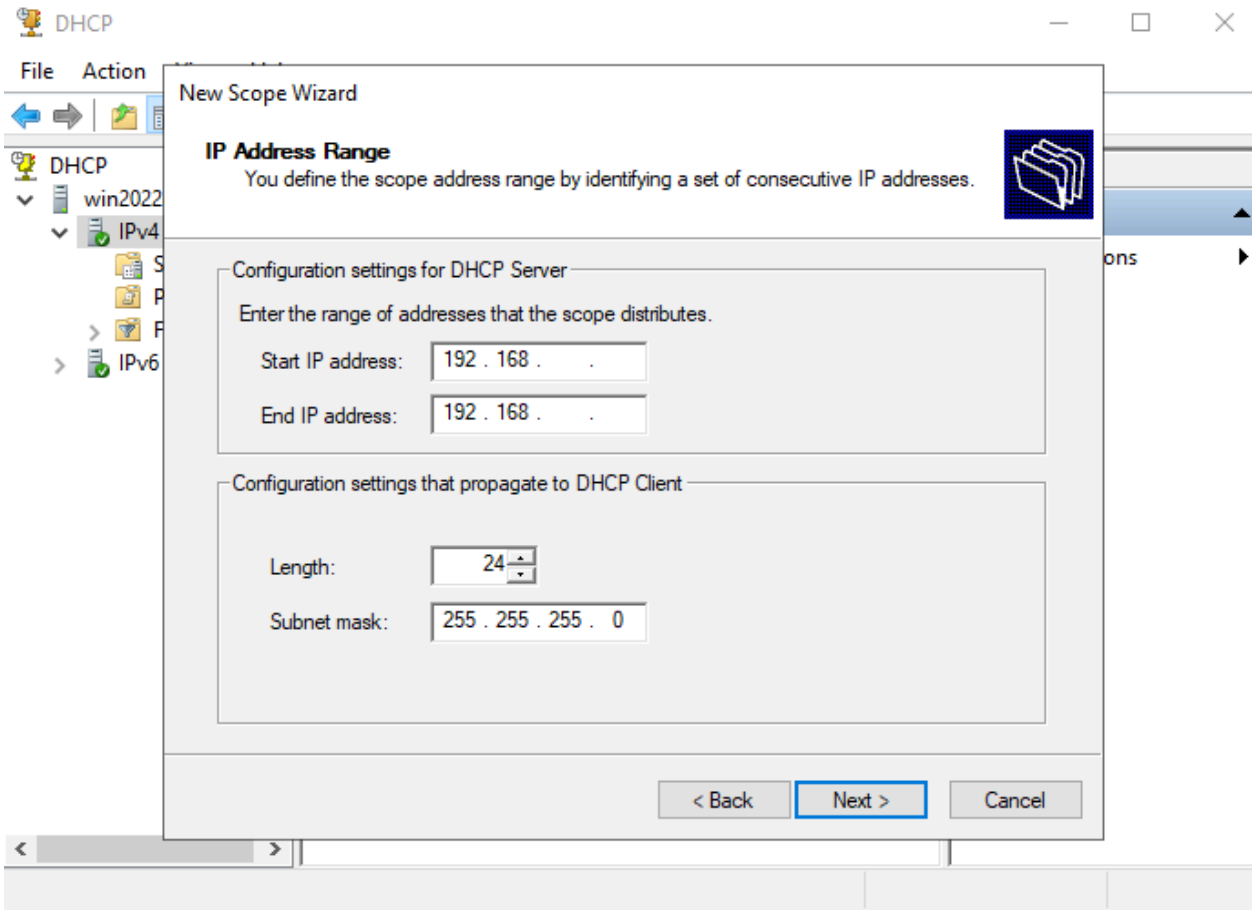
AD DS, DHCP, DNS Successfully Installed

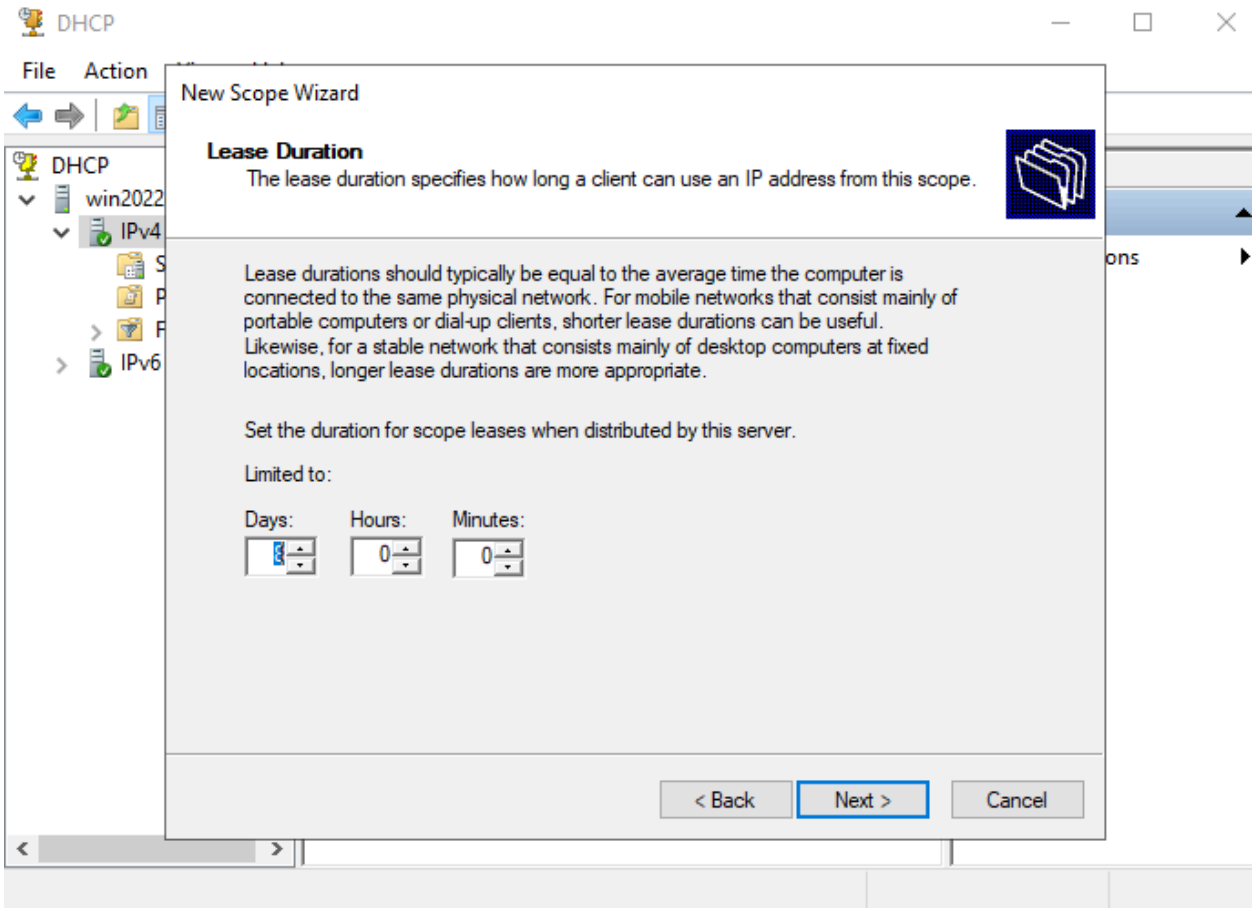
Create DHCP Scope

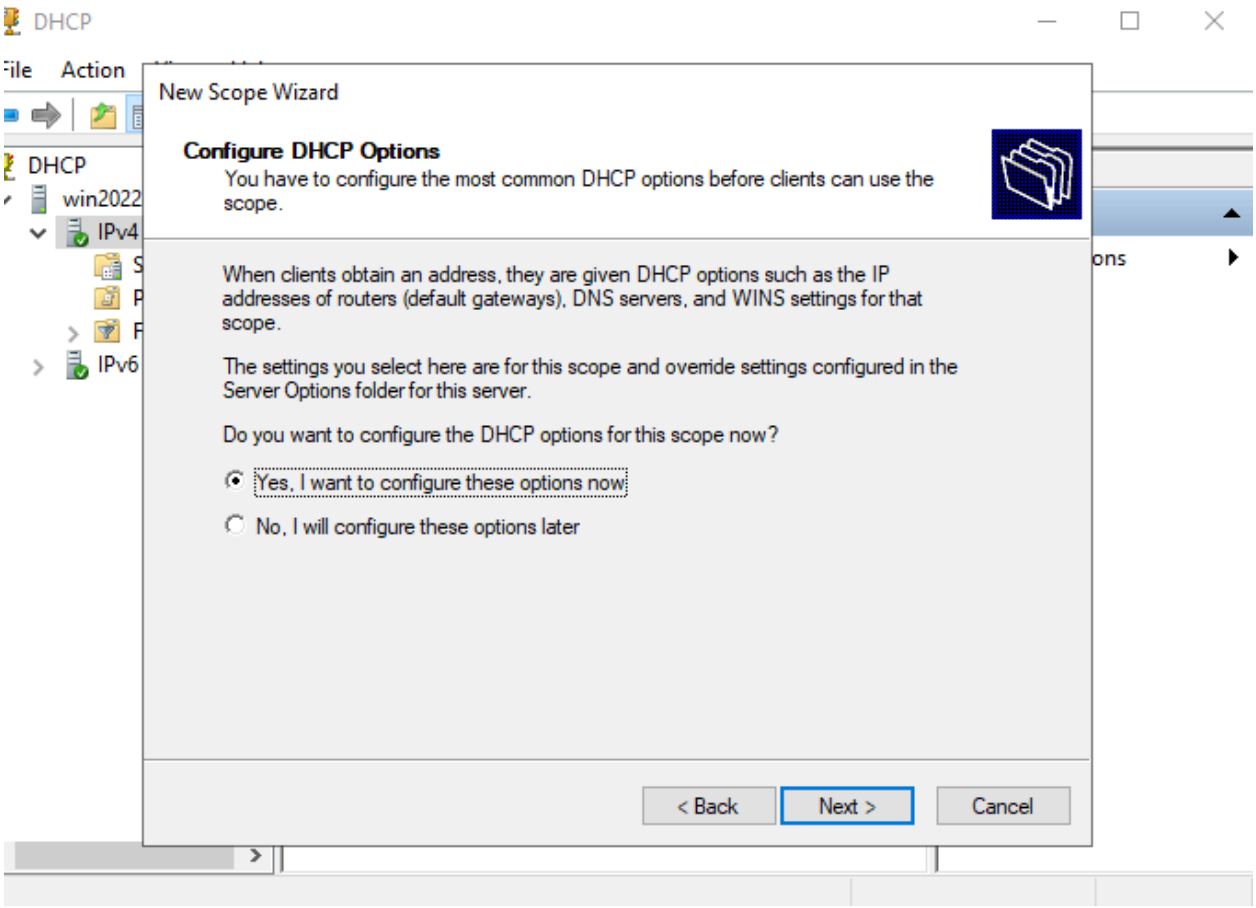


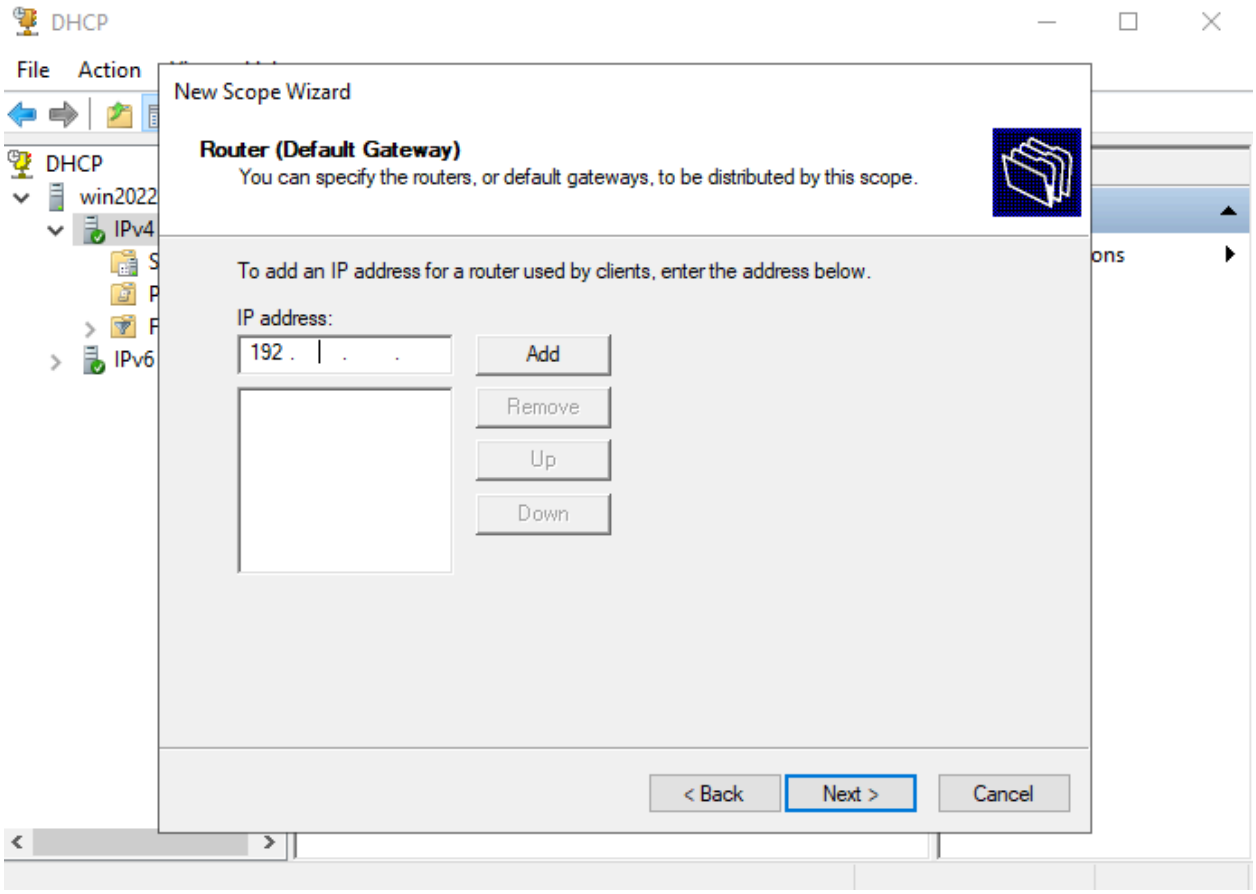

Server Manager
Server Manager ▸ Dashboard
Manage
DHCP
File Action View Help
DHCP
win2022dc.corp.local
IPv4
Add a Scope
addresses assigned to
a dynamic IP address. You must
scope before dynamic IP
ned.
the Action menu, click New
bout setting up a DHCP server,
Actions
IPv4
More Actions
Display Statistics...
New Scope...
New Multicast Scope...
Configure Failover...
Replicate Failover Scopes...
Define User Classes...
Define Vendor Classes...
Reconcile All Scopes...
Set Predefined Options...
View
Refresh
Properties
Help
Displays Help for the current selection.

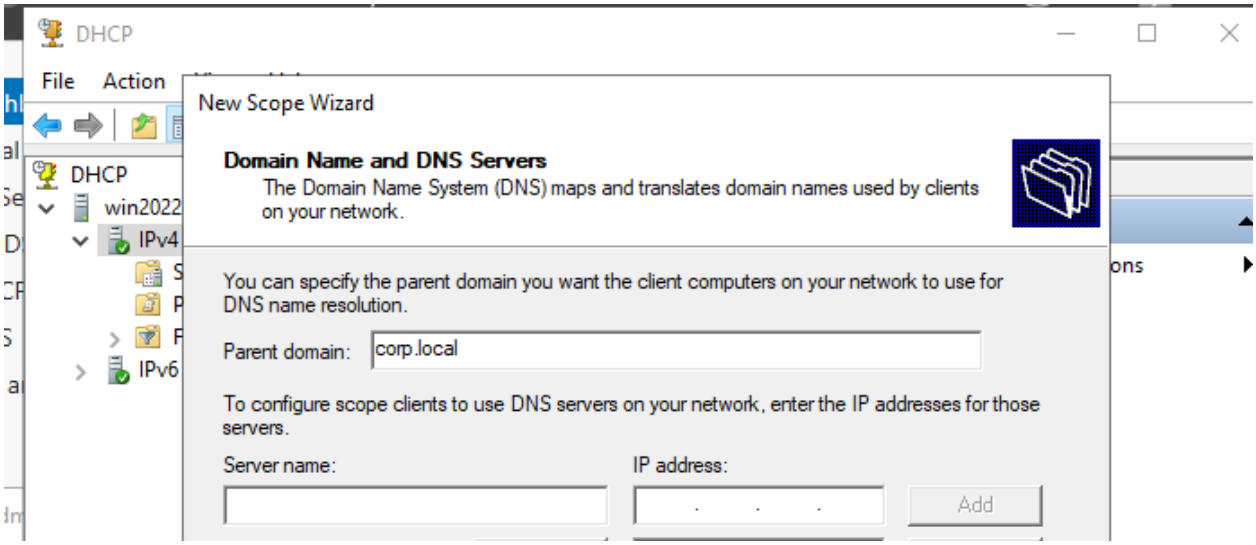

DHCP
File
Action
DHCP
win2022
IPv4
IPv6
New Scope Wizard
Scope Name
You have to provide an identifying scope name. You also have the option of providing a description.
Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.
Name:
Lab Network Scope
Description:
DHCP Scope for lab clients
< Back
Next >
Cancel

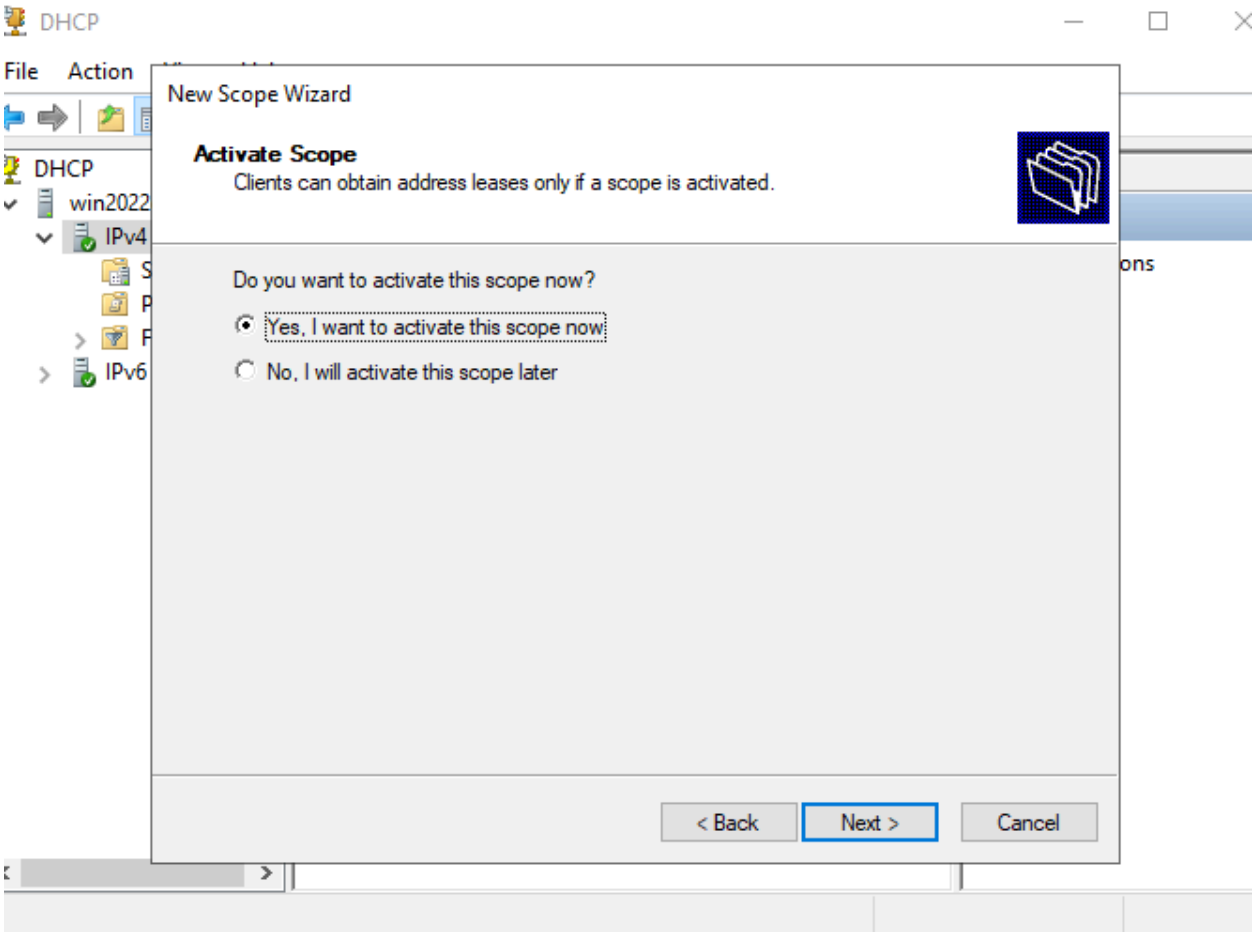

DHCP
File
Action
DHCP
win2022
IPv4
IPv6
New Scope Wizard
IP Address Range
You define the scope address range by identifying a set of consecutive IP addresses.
Configuration settings for DHCP Server
Enter the range of addresses that the scope distributes.
Start IP address:
192 . 168 .
End IP address:
192 . 168 .
Configuration settings that propagate to DHCP Client
Length:
24
Subnet mask:
255 . 255 . 255 . 0
< Back
Next >
Cancel

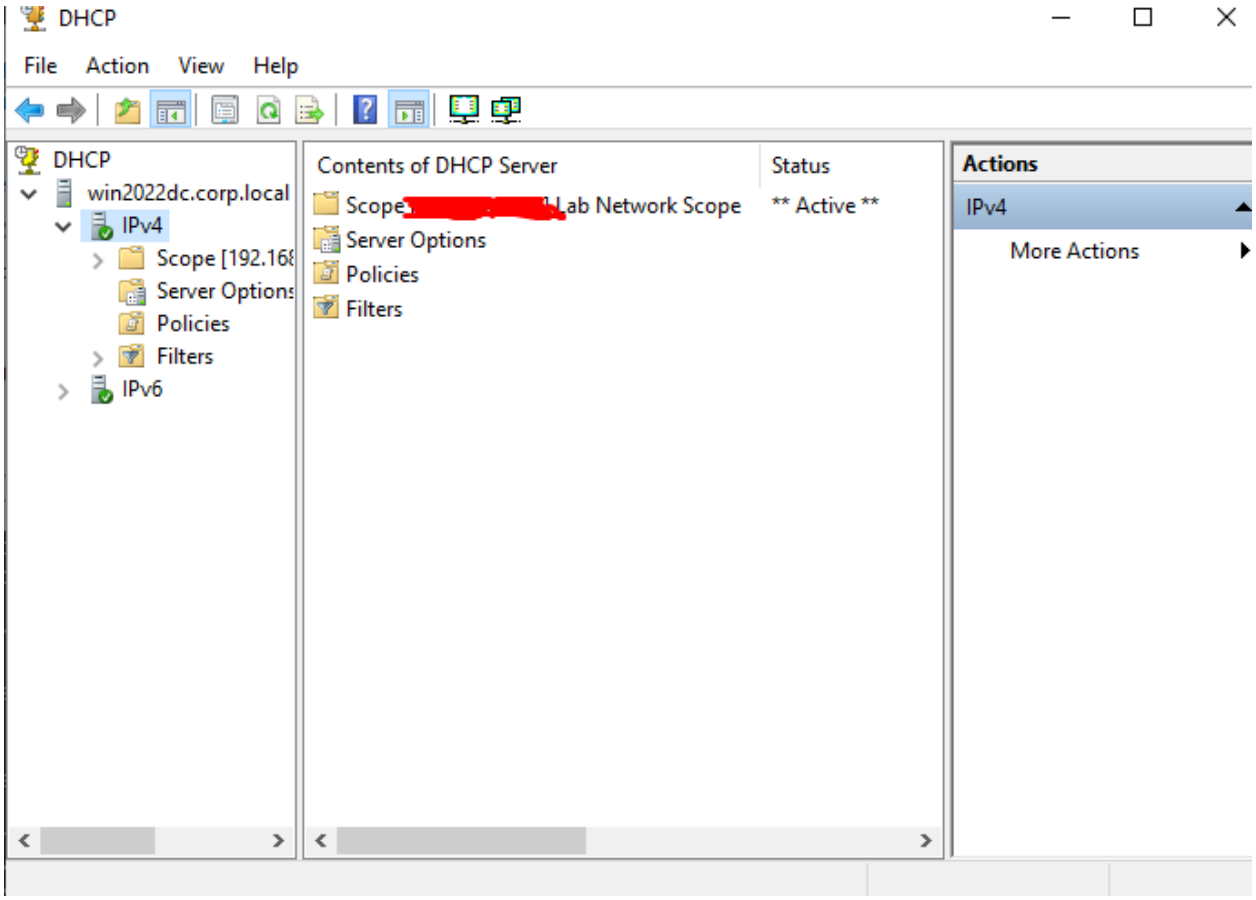

DHCP
File
Action
DHCP
win2022
IPv4
IPv6
New Scope Wizard
Lease Duration
The lease duration specifies how long a client can use an IP address from this scope.
Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that 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:
Hours:
Minutes:
0
0
< Back
Next >
Cancel


DHCP
File
Action
DHCP
win2022
IPv4
IPv6
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
< Back
Next >
Cancel


DHCP
File
Action
DHCP
win2022
IPv4
IPv6
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:
192 .
Add
Remove
Up
Down
< Back
Next >
Cancel

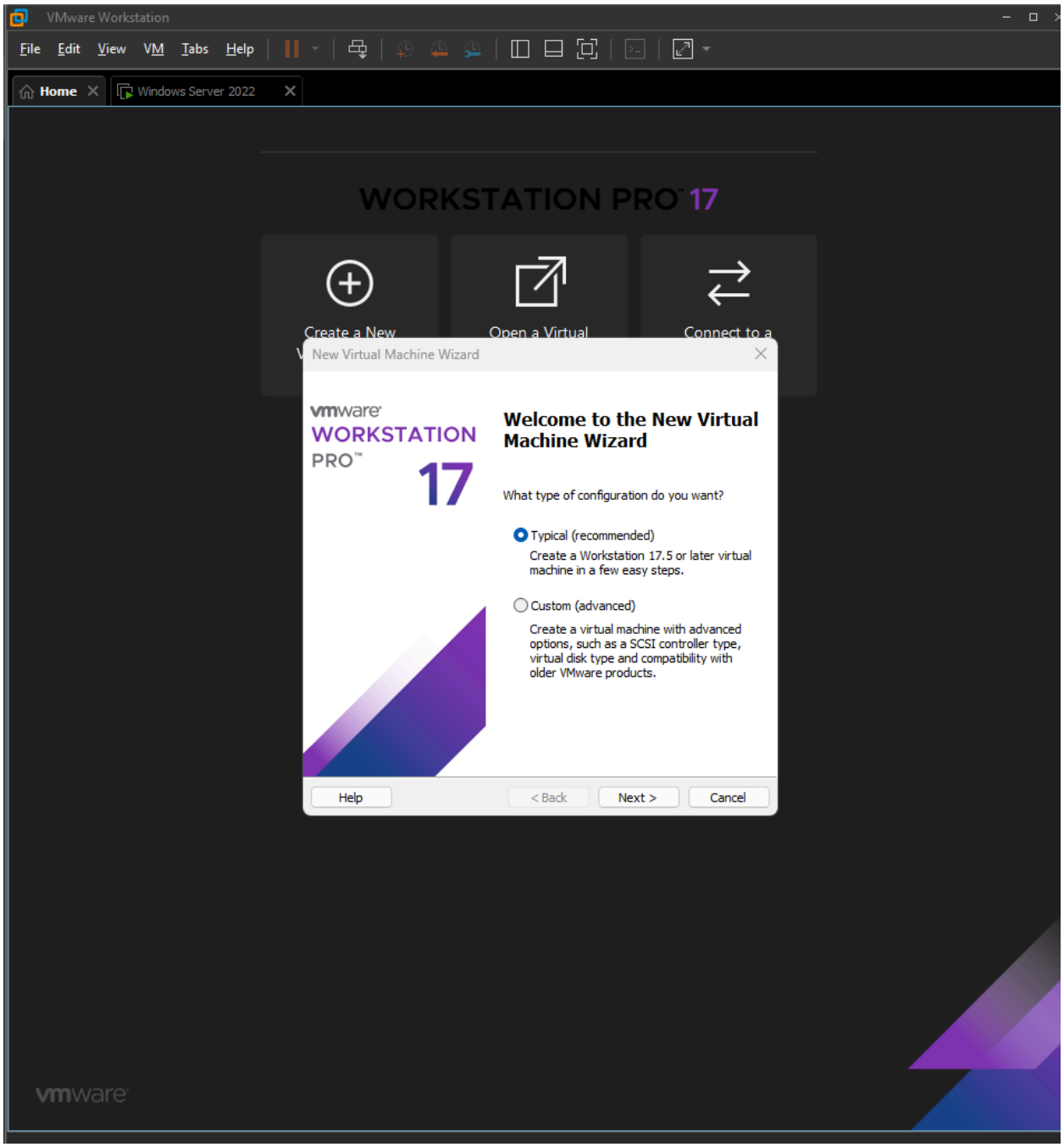

DHCP
File
Action
DHCP
win2022
IPv4
IPv6
New Scope Wizard
Domain Name and DNS Servers
The Domain Name System (DNS) maps and translates domain names used by clients on your network.
You can specify the parent domain you want the client computers on your network to use for DNS name resolution.
Parent domain:
corp.local
To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.
Server name:
IP address:
Add

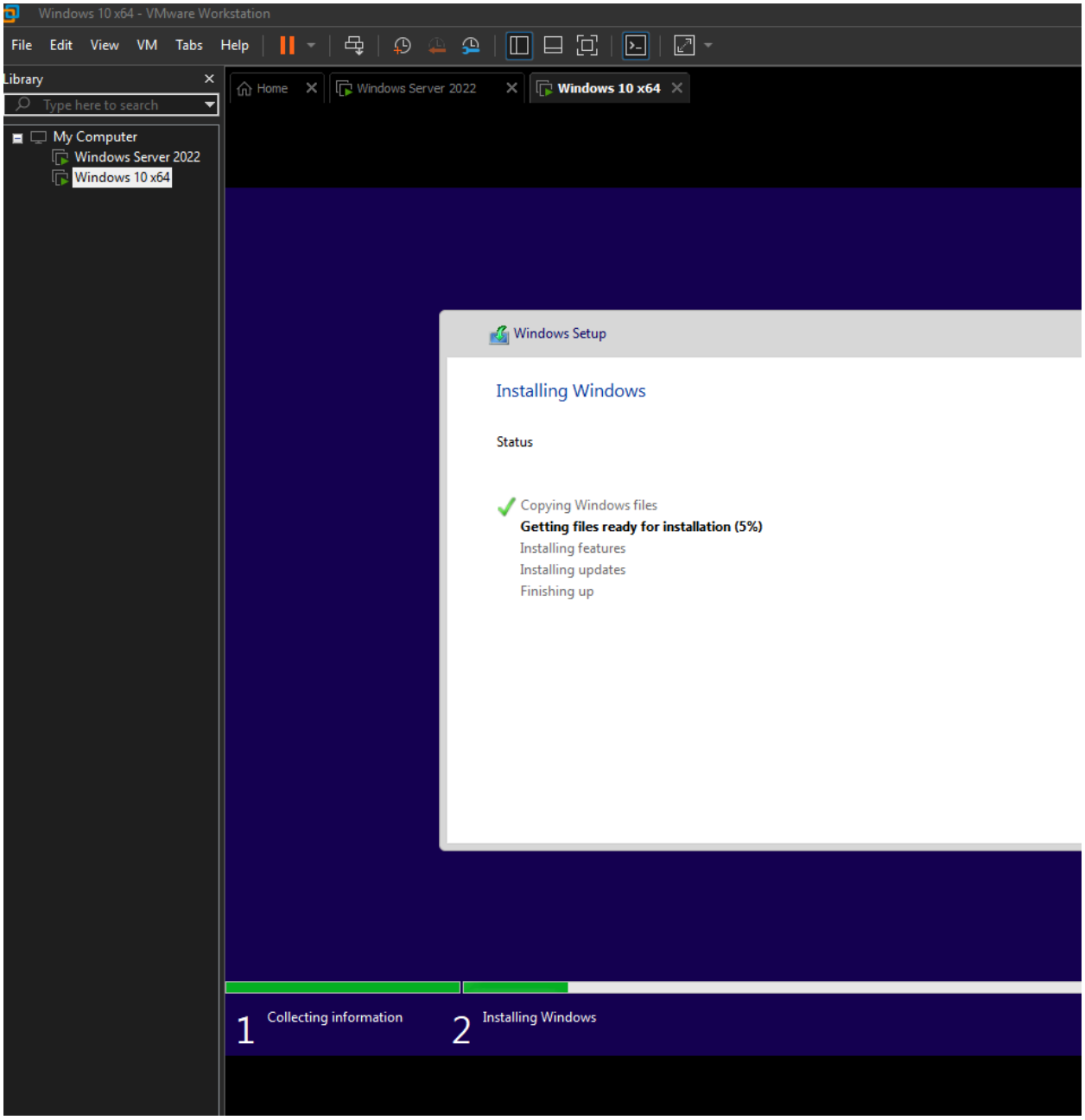

DHCP
File
Action
DHCP
win2022
IPv4
IPv6
New Scope Wizard
Activate Scope
Clients can obtain address leases only if a scope is activated.
Do you want to activate this scope now?
Yes, I want to activate this scope now
No, I will activate this scope later
< Back
Next >
Cancel



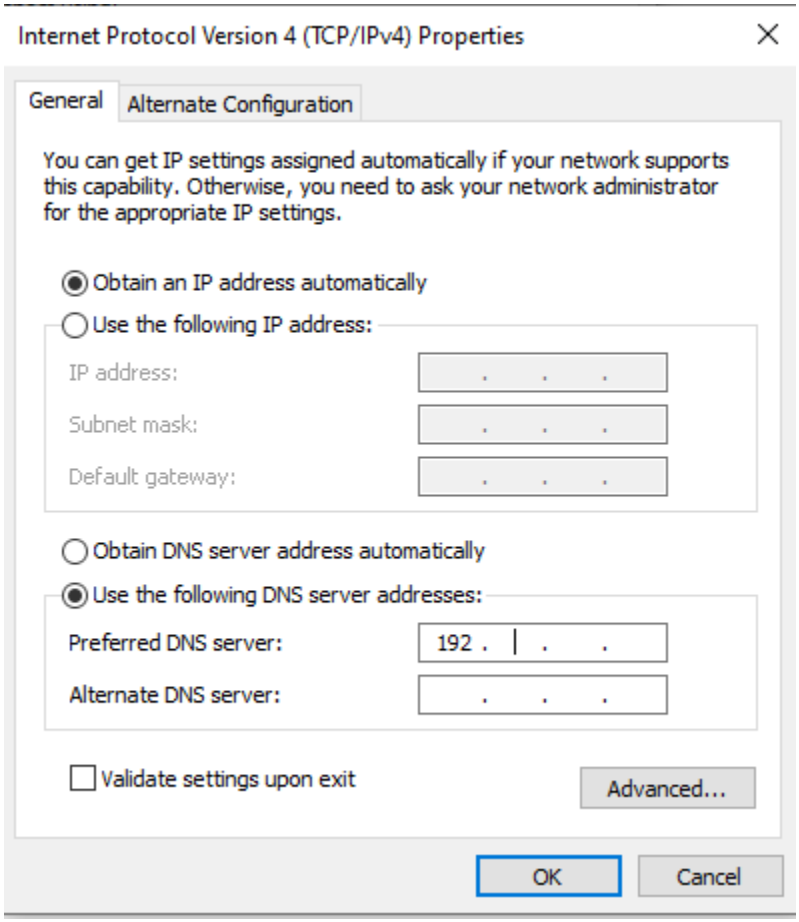
Configured DHCP scope for lab network with IP range and DNS settings

Create new Windows 10 VM with VMware (Acting as user)

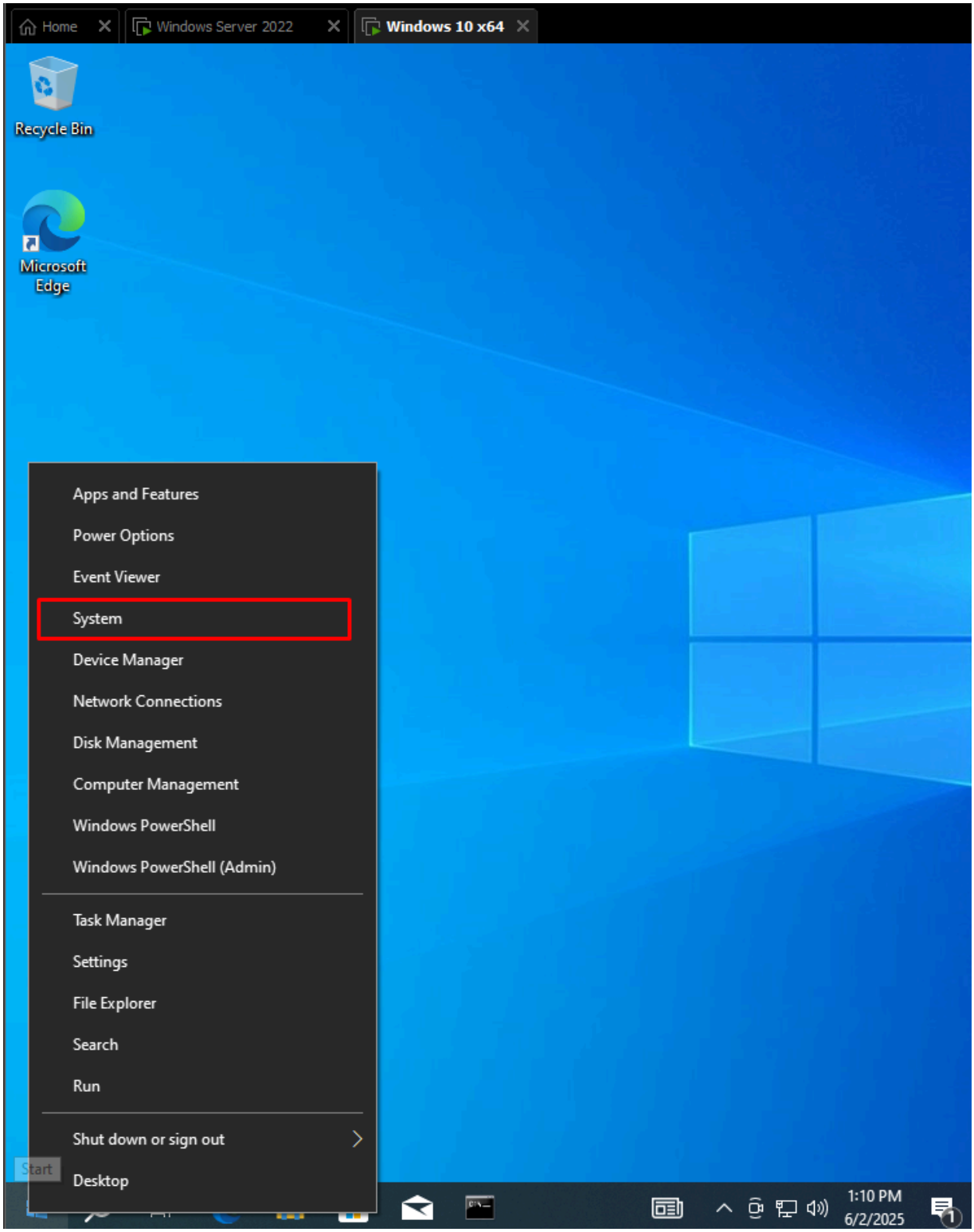


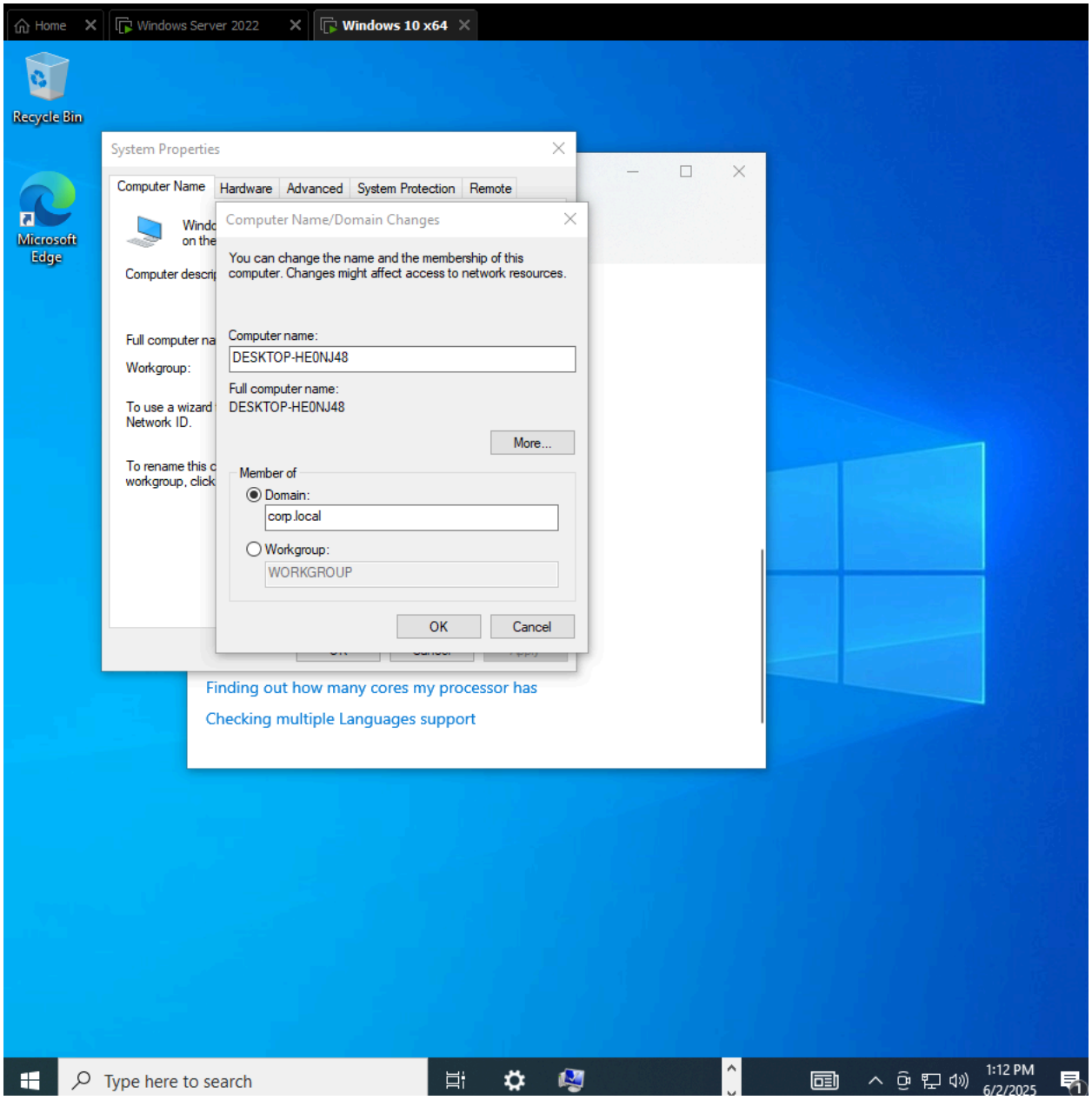

Windows 10 x64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows Server 2022
Windows 10 x64
Home
Windows Server 2022
Windows 10 x64
Windows Setup
Installing Windows
Status
Copying Windows files
Getting files ready for installation (5%)
Installing features
Installing updates
Finishing up
1 Collecting information
2 Installing Windows

Set DNS on new Windows 10 VM to the Windows Server 2022 static Domain Controller IP



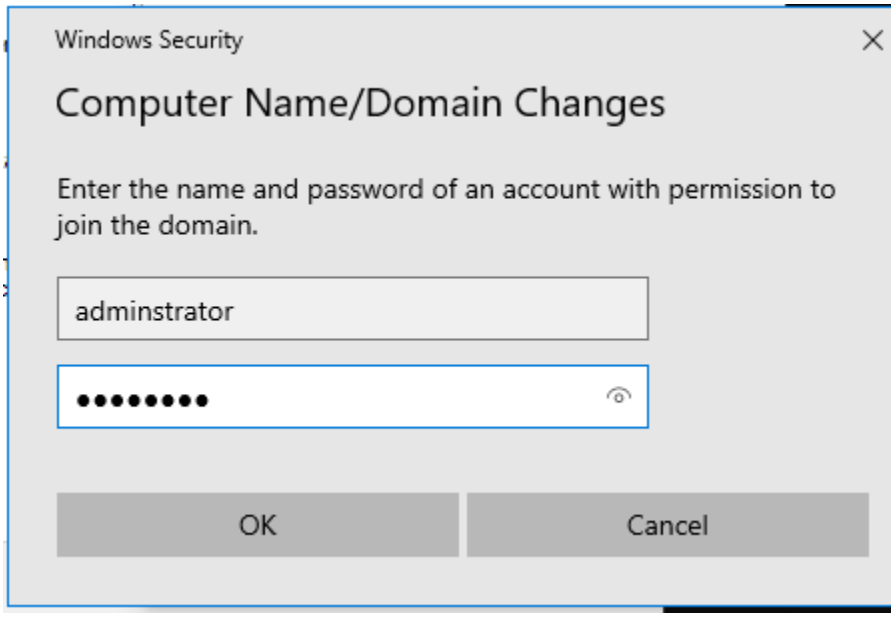
Windows 10 VM: Connect to CORP.LOCAL domain created by Windows Server 2022

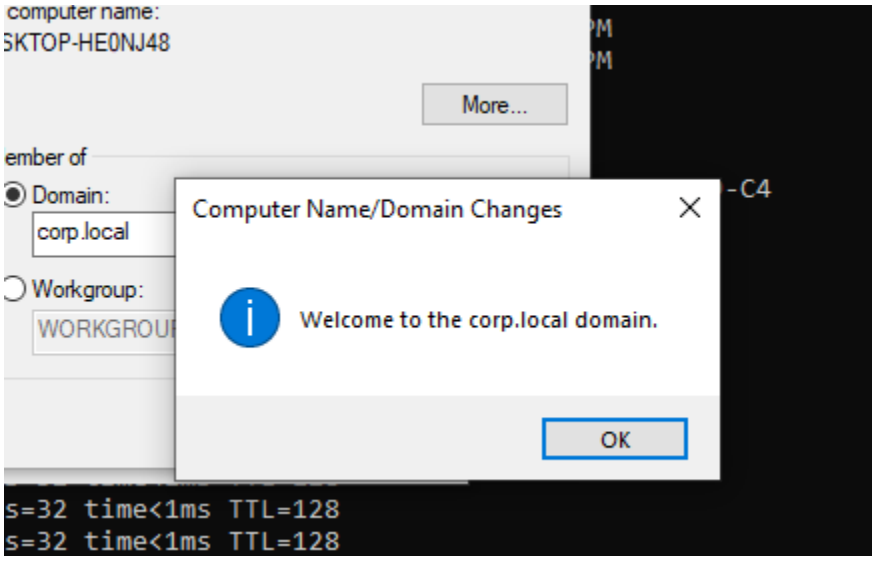




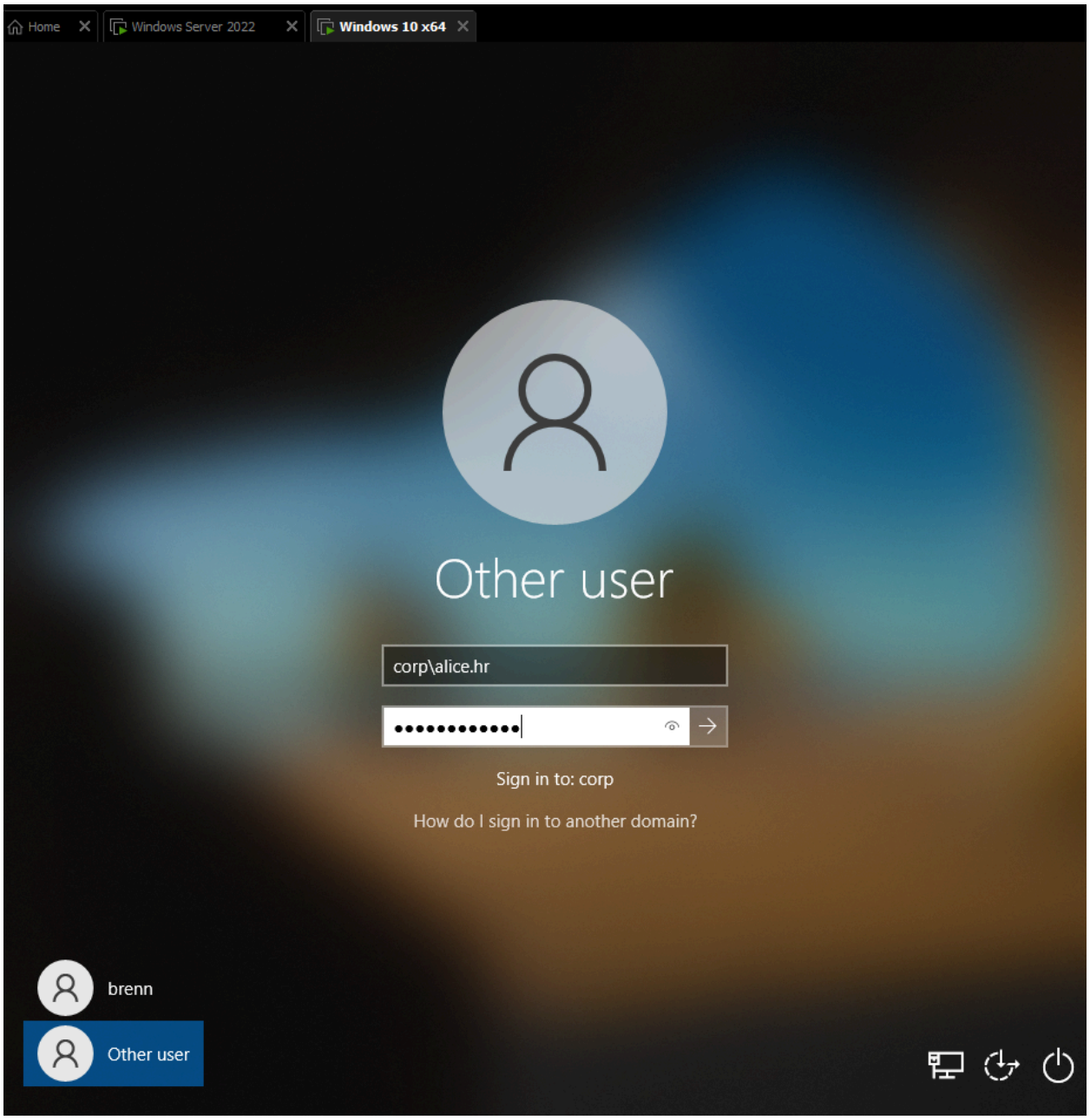

```
C:\Windows\system32>ipconfig /registerdns

Windows IP Configuration

Registration of the DNS resource records for all adapters of this computer has been initiated. Any errors will be r
eported in the Event Viewer in 15 minutes.
```

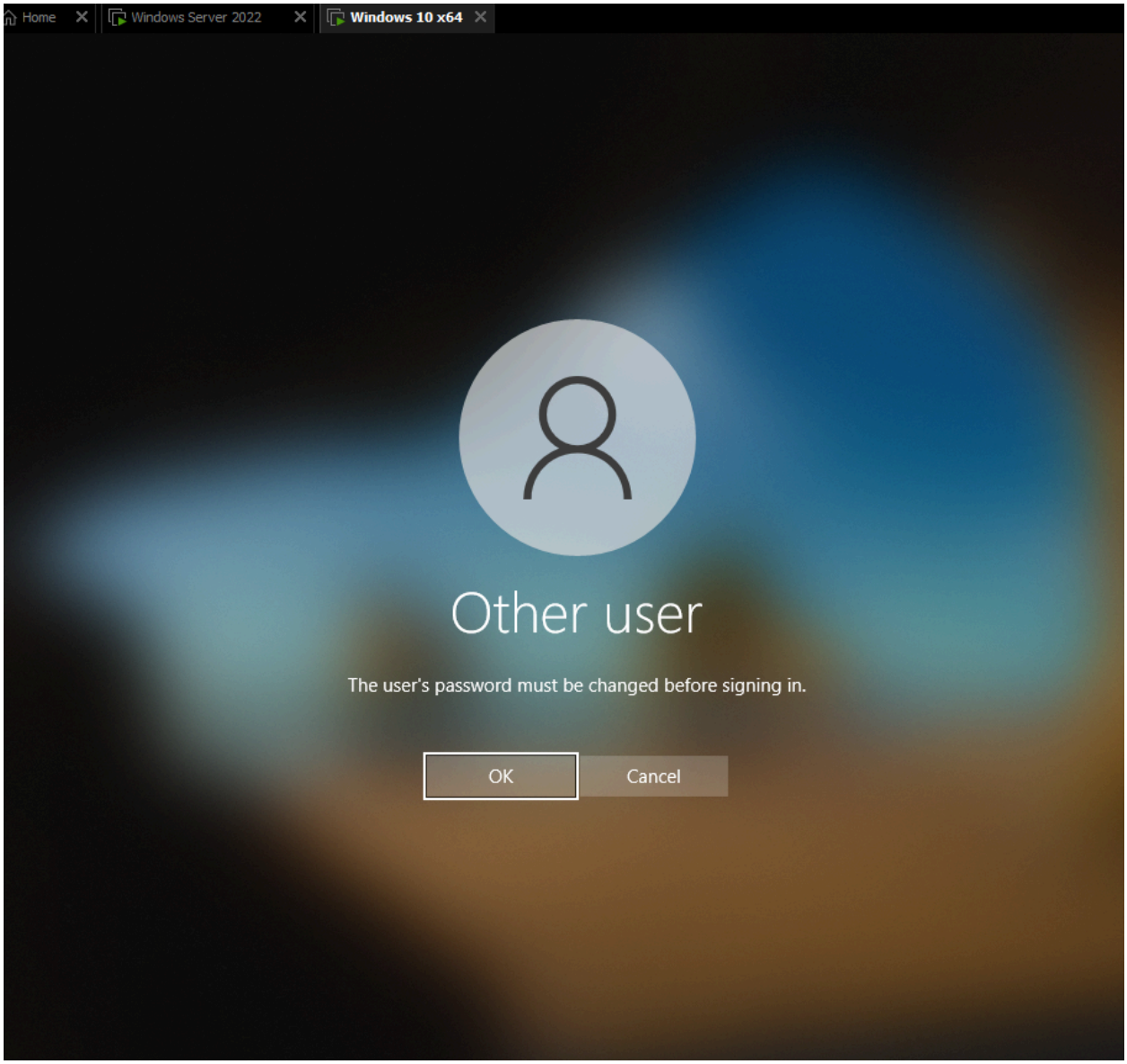
```
C:\Windows\system32>ping corp.local

Pinging corp.local [192.168.137.222] with 32 bytes of data:
Reply from 192.168.137.222: bytes=32 time<1ms TTL=128
Reply from 192.168.137.222: bytes=32 time<1ms TTL=128
Reply from 192.168.137.222: bytes=32 time<1ms TTL=128
```

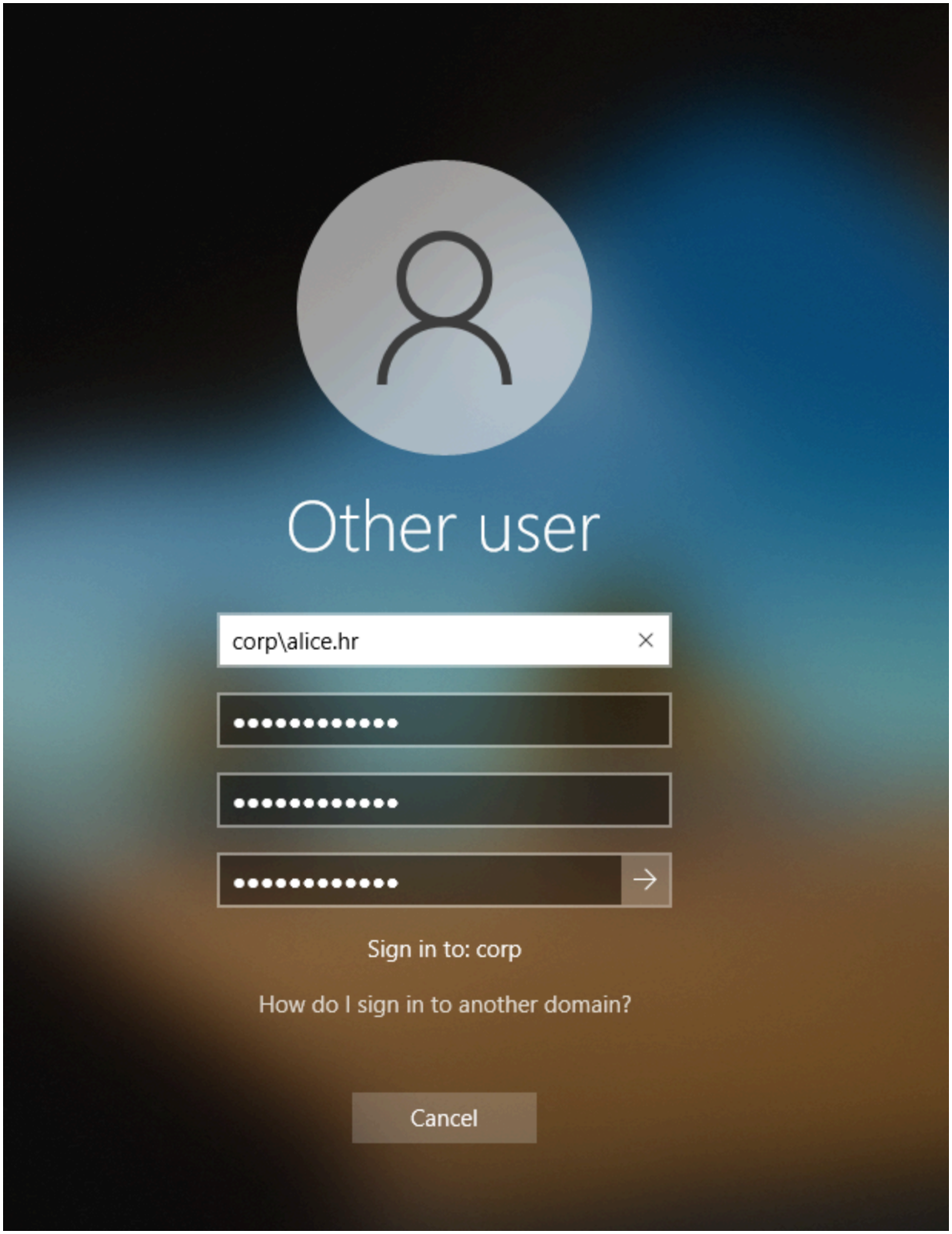


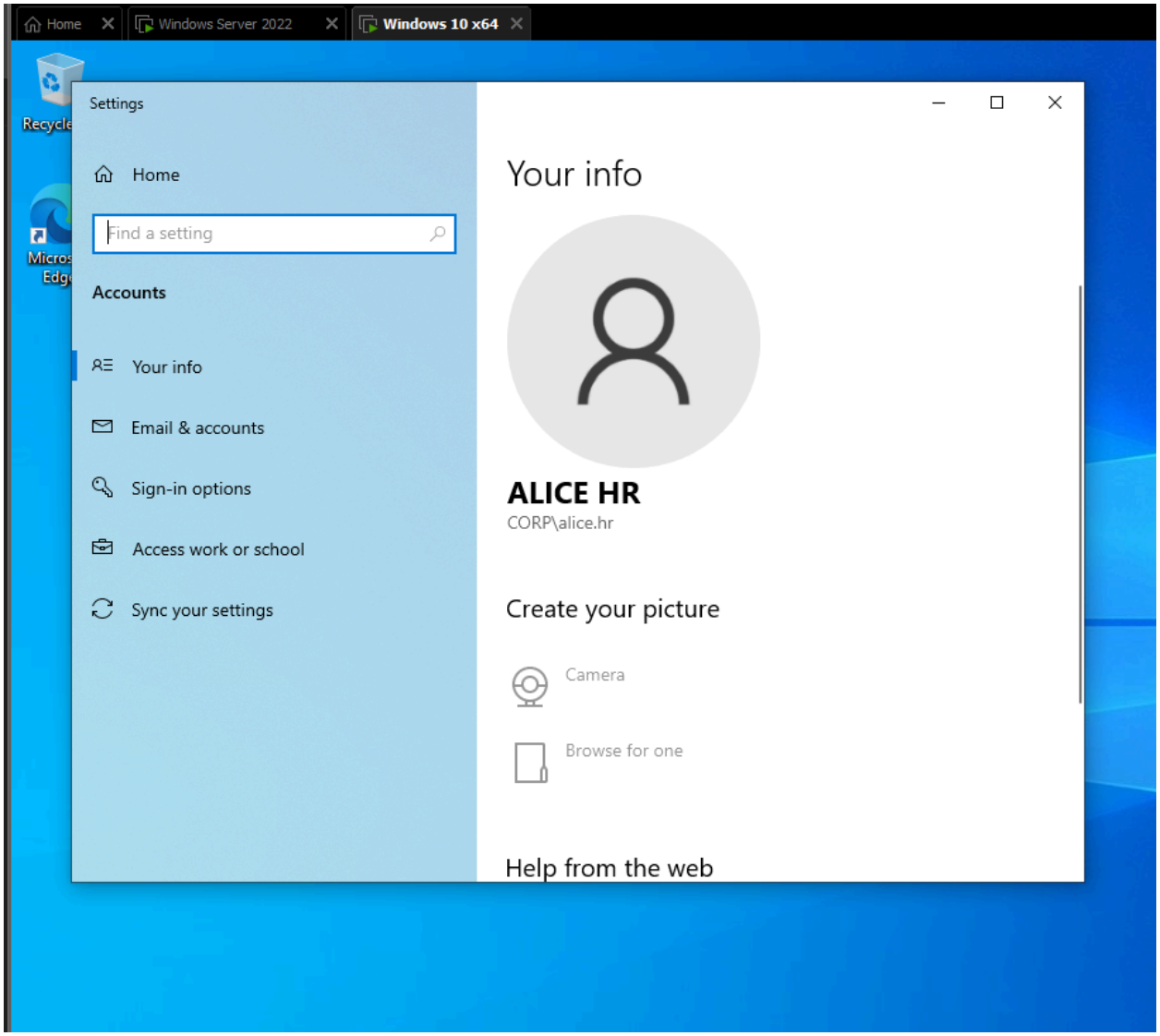


Windows 10 VM: Log in to an account of the Corp.local domain: alice.hr



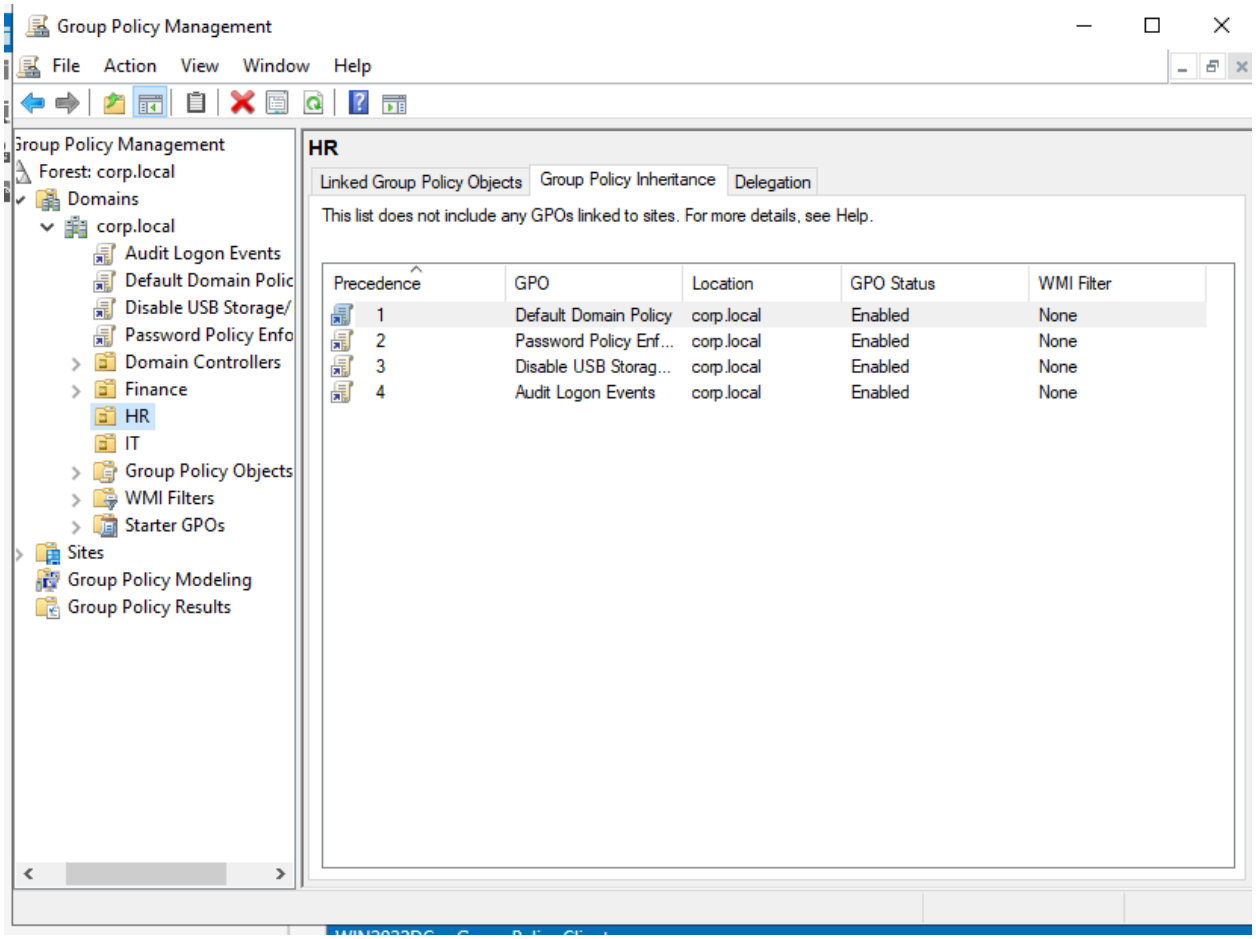

Home
Windows Server 2022
Windows 10 x64
Other user
The user's password must be changed before signing in.
OK
Cancel


Other user
corp\alice.hr
Sign in to: corp
How do I sign in to another domain?
Cancel

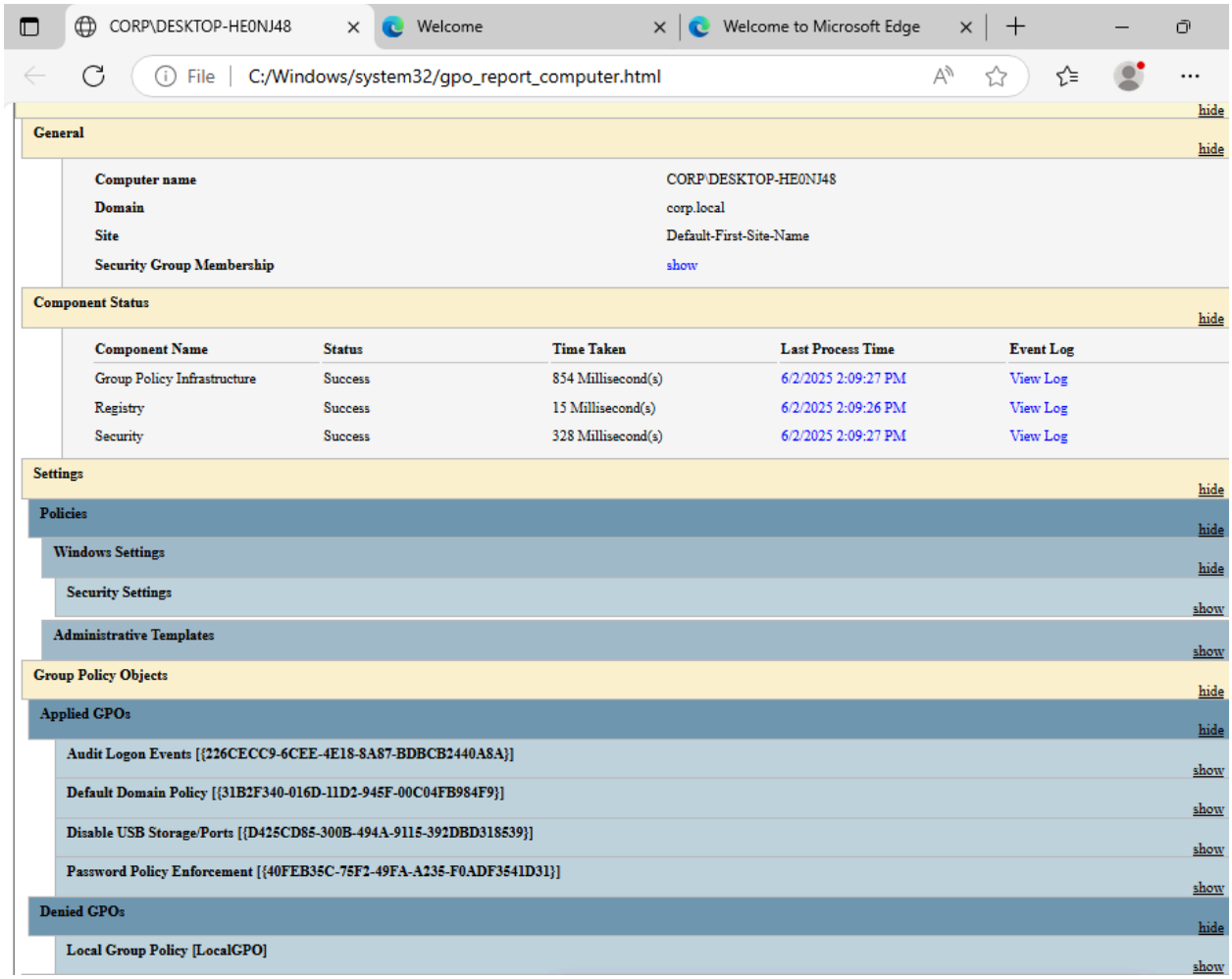

Home
Windows Server 2022
Windows 10 x64
Recycle
Settings
Home
Find a setting
Accounts
Your info
Email & accounts
Sign-in options
Access work or school
Sync your settings
Your info
ALICE HR
CORP\alice.hr
Create your picture
Camera
Browse for one
Help from the web

```
C:\Users\alice.hr>gpupdate /force
Updating policy...

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

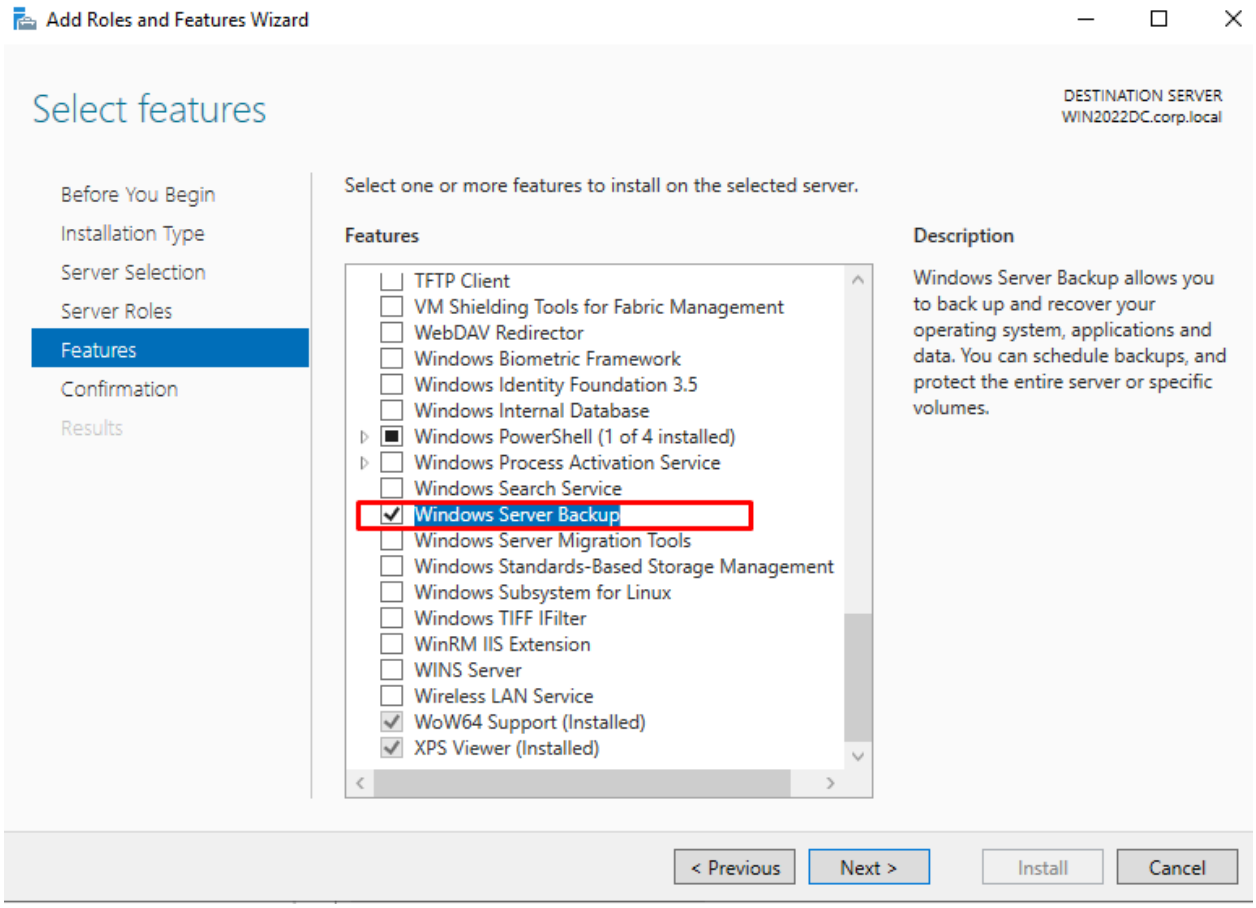
1. Check GPO Application on Client

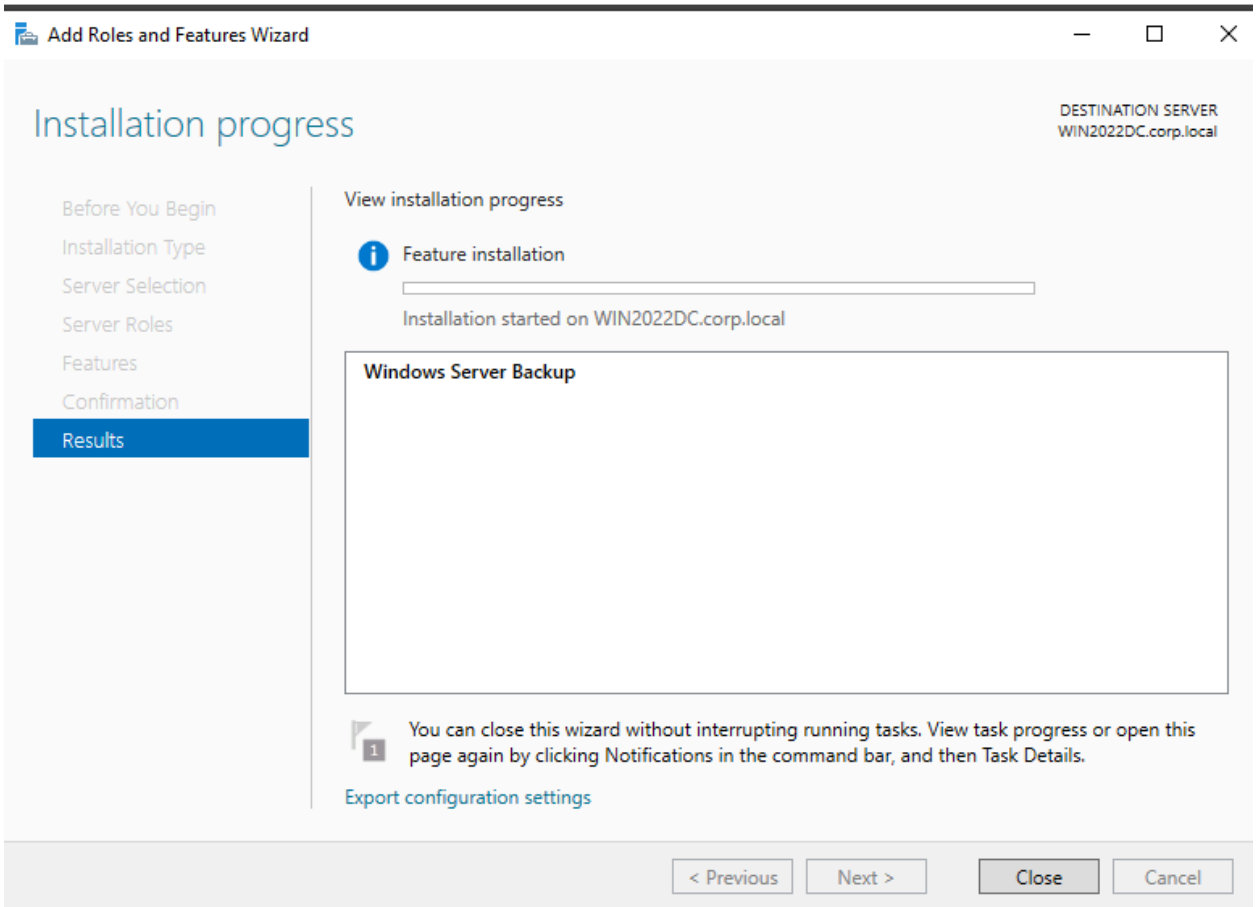


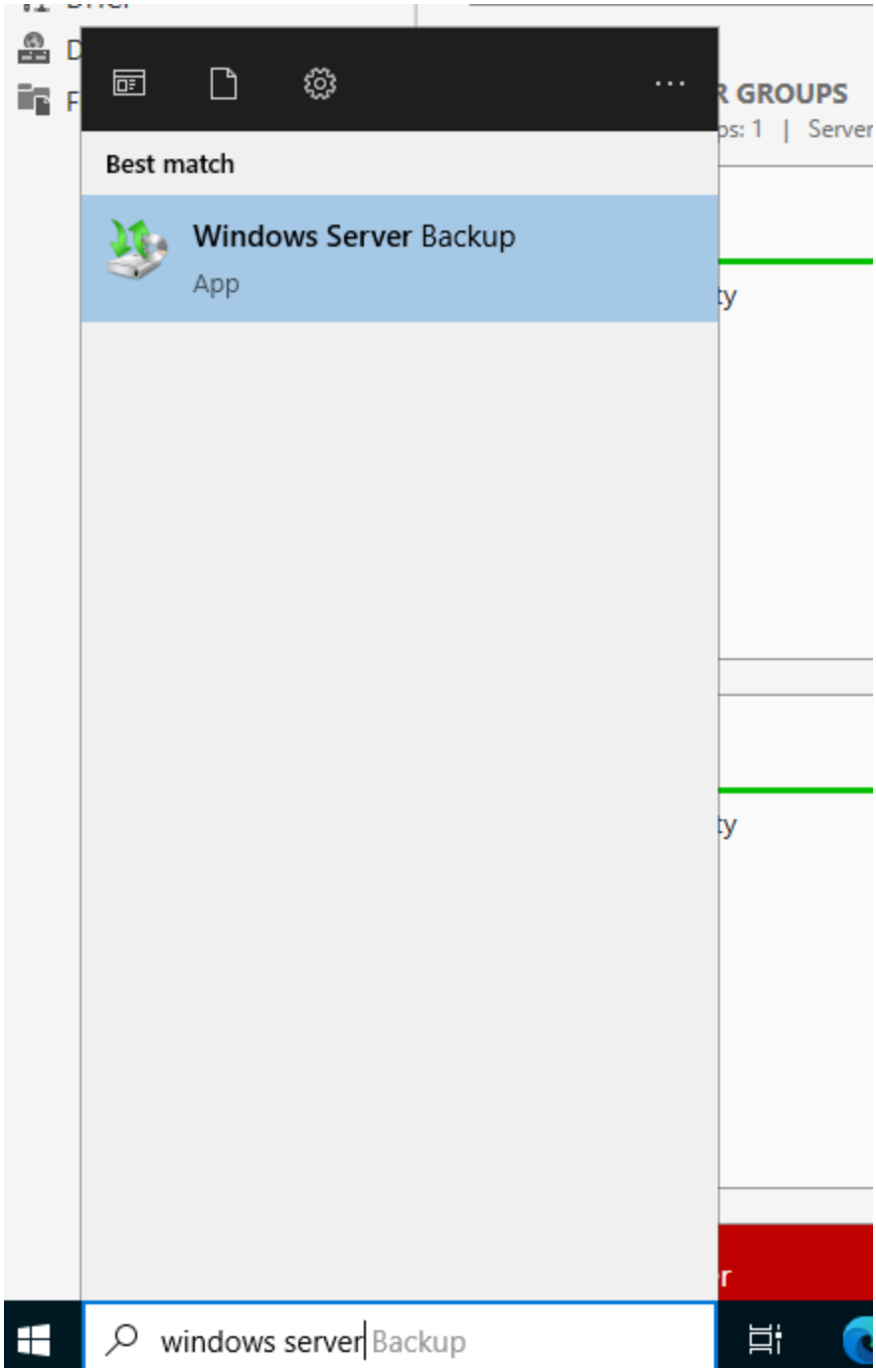

```
C:\Windows\system32>gpresult /scope computer /h gpo_report_computer.html
```

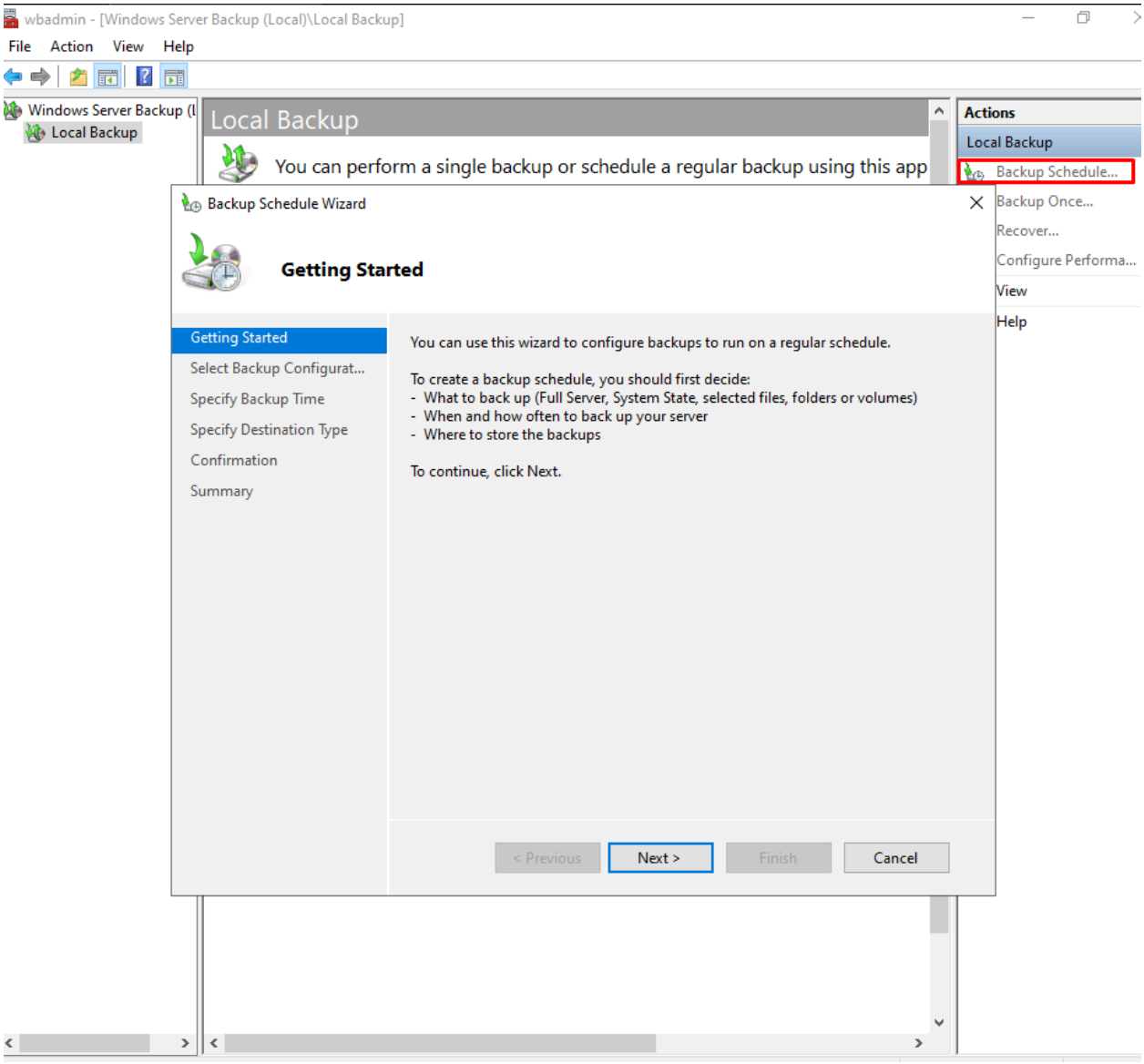

CORP\DESKTOP-HE0NJ48
Welcome
Welcome to Microsoft Edge
File | C:/Windows/system32/gpo_report_computer.html
hide
General
hide
Computer name CORP\DESKTOP-HE0NJ48
Domain corp.local
Site Default-First-Site-Name
Security Group Membership show
Component Status
hide
Component Name | Status | Time Taken | Last Process Time | Event Log
Group Policy Infrastructure | Success | 854 Millisecond(s) | 6/2/2025 2:09:27 PM | View Log
Registry | Success | 15 Millisecond(s) | 6/2/2025 2:09:26 PM | View Log
Security | Success | 328 Millisecond(s) | 6/2/2025 2:09:27 PM | View Log
Settings
hide
Policies
hide
Windows Settings
hide
Security Settings
show
Administrative Templates
show
Group Policy Objects
hide
Applied GPOs
hide
Audit Logon Events [{226CECC9-6CEE-4E18-8A87-BDBCB2440A8A}]
show
Default Domain Policy [{31B2F340-016D-11D2-945F-00C04FB984F9}]
show
Disable USB Storage/Ports [{D425CD85-300B-494A-9115-392DBD318539}]
show
Password Policy Enforcement [{40FEB35C-75F2-49FA-A235-F0ADF3541D31}]
show
Denied GPOs
hide
Local Group Policy [LocalGPO]
show

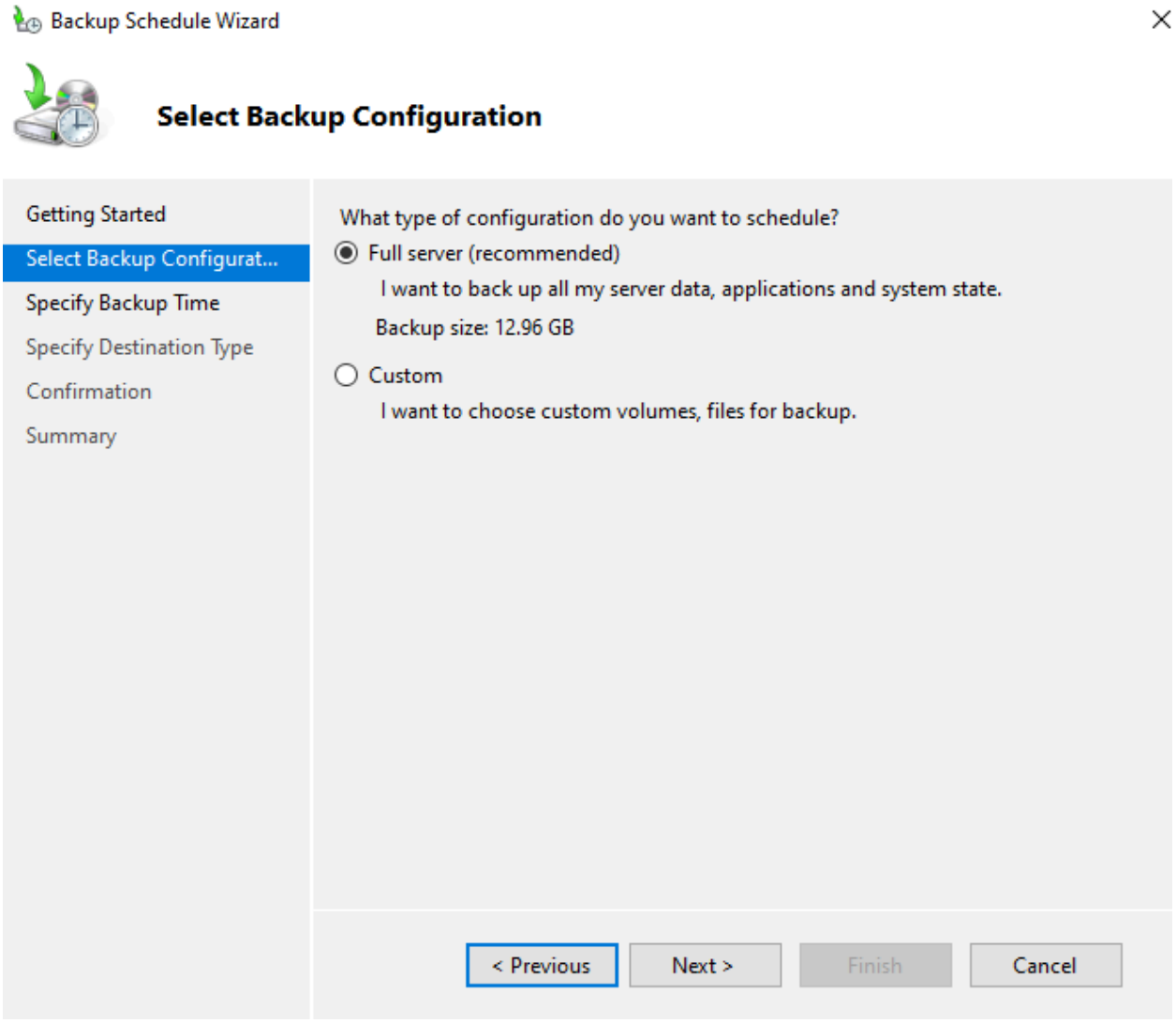
Windows Server 2022: Create Windows Server Backup

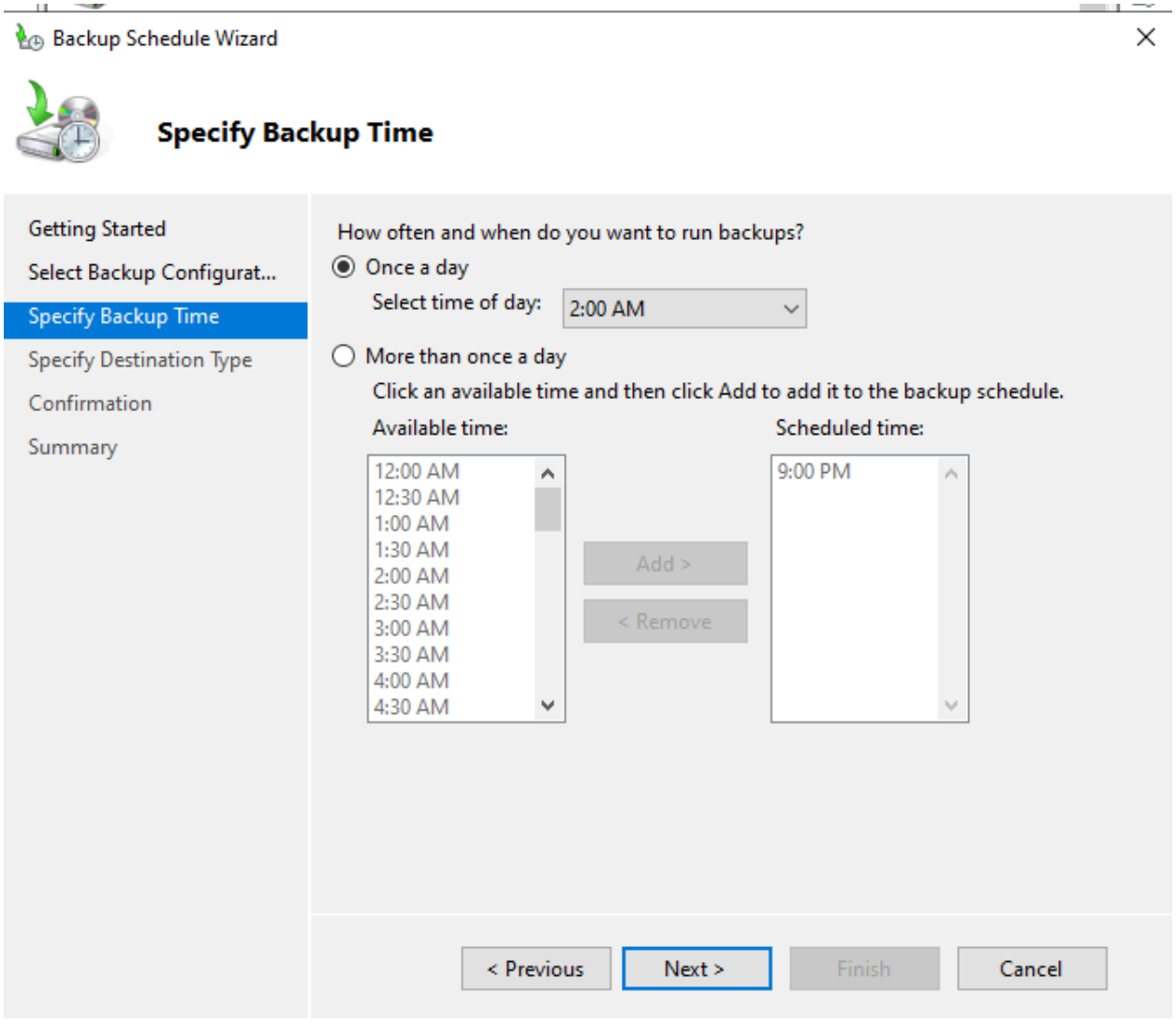


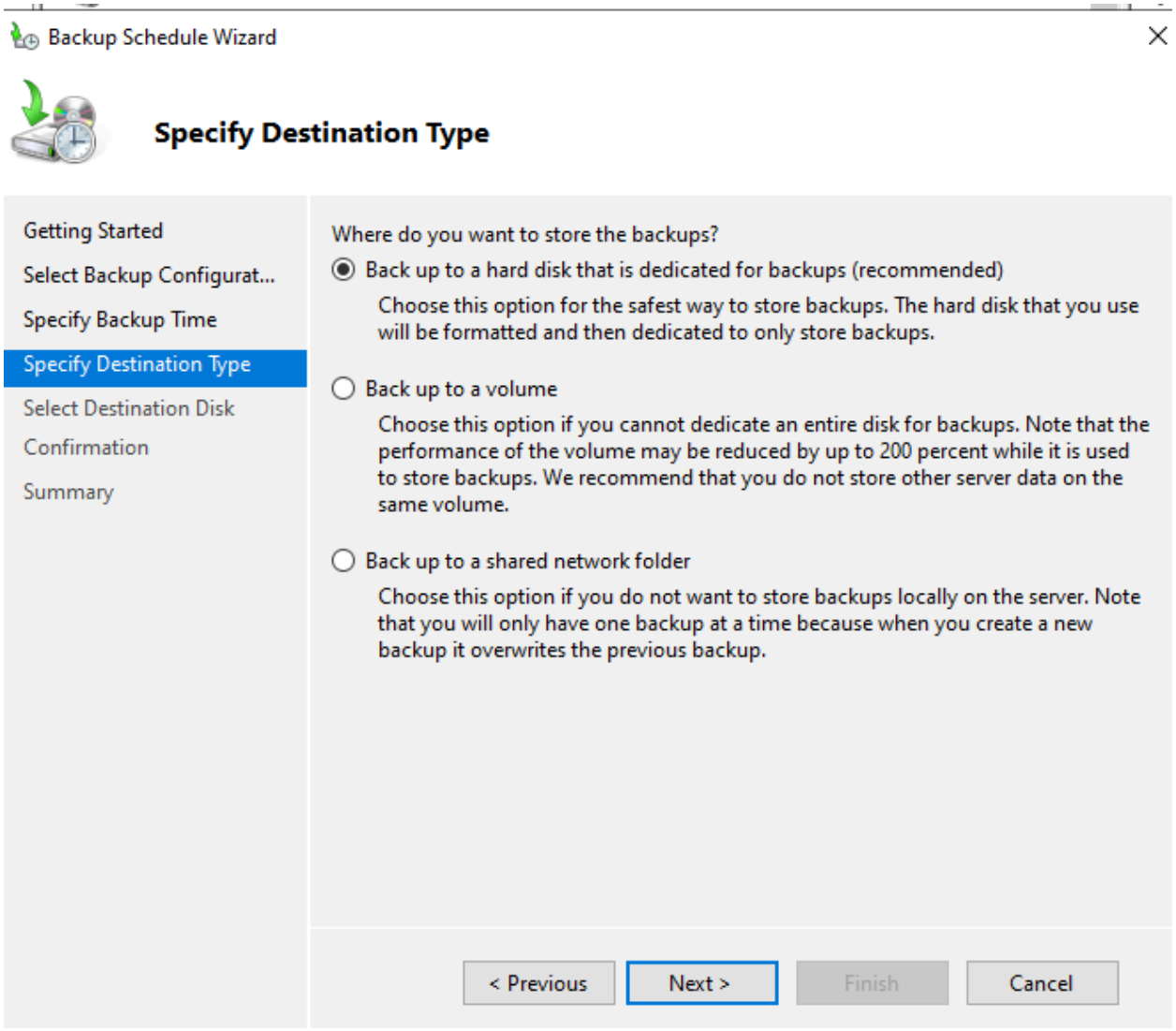

Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
WIN2022DC.corp.local
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
View installation progress
Feature installation
Installation started on WIN2022DC.corp.local
Windows Server Backup
You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.
Export configuration settings
< Previous
Next >
Close
Cancel

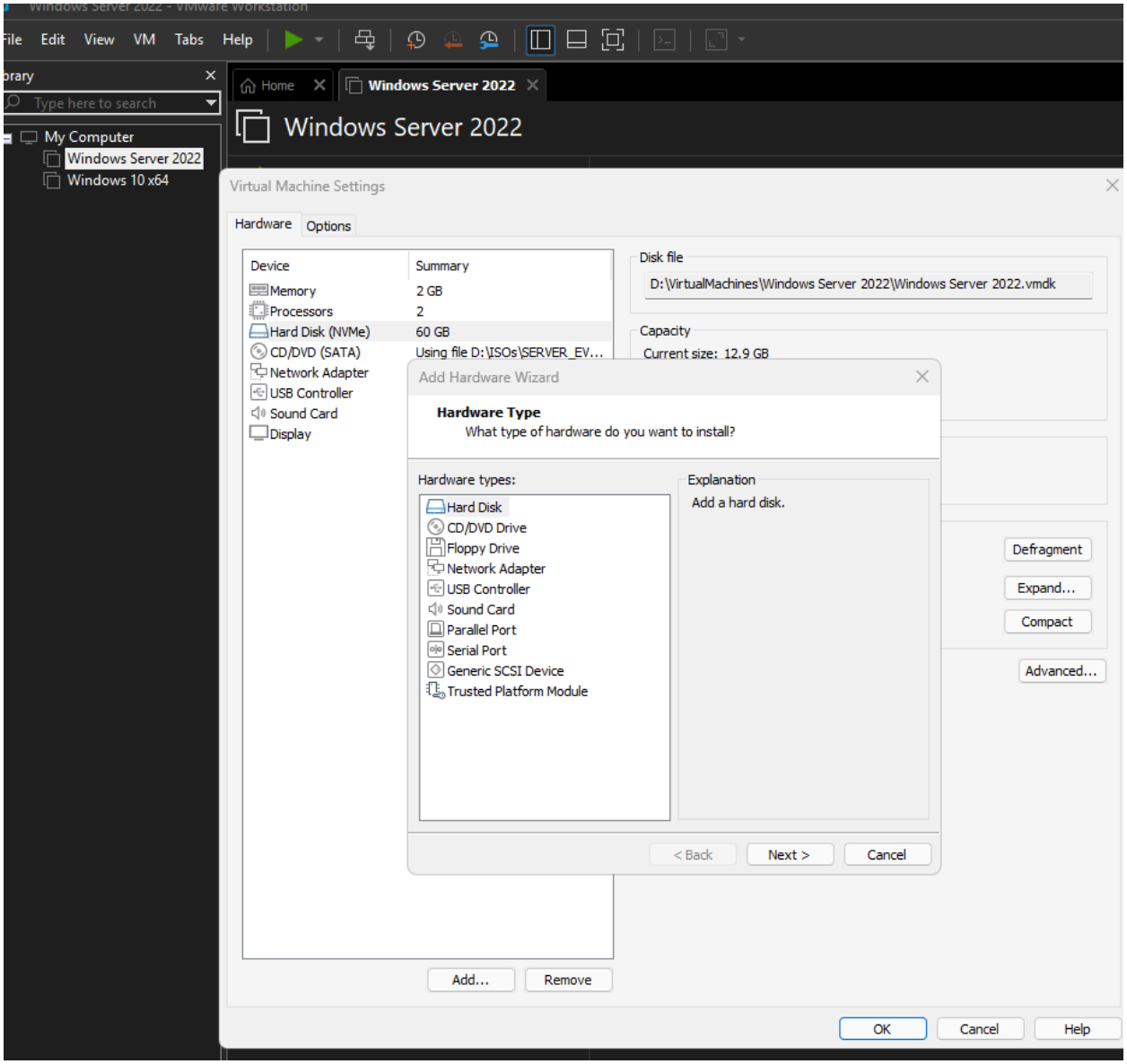

Best match
Windows Server Backup
App
windows server Backup

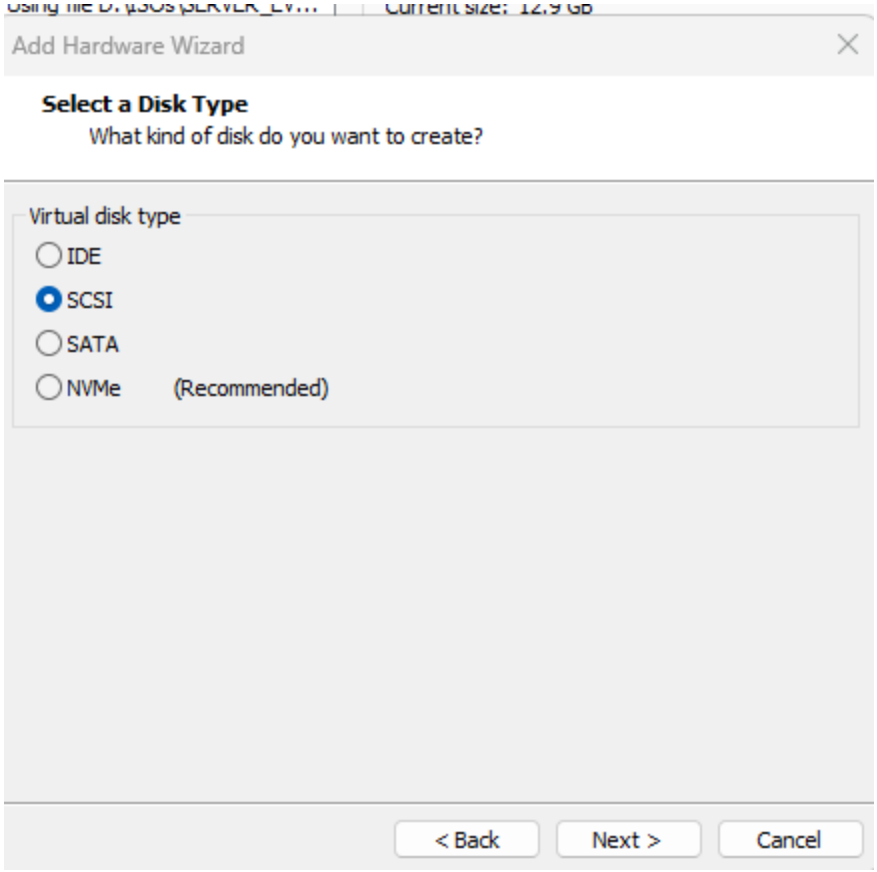

wbadmin - [Windows Server Backup (Local)\Local Backup]
File Action View Help
Windows Server Backup (L
Local Backup
Local Backup
You can perform a single backup or schedule a regular backup using this app
Actions
Local Backup
Backup Schedule...
Backup Once...
Recover...
Configure Performa...
View
Help
Backup Schedule Wizard
Getting Started
Getting Started
Select Backup Configurat...
Specify Backup Time
Specify Destination Type
Confirmation
Summary
You can use this wizard to configure backups to run on a regular schedule.
To create a backup schedule, you should first decide:
- What to back up (Full Server, System State, selected files, folders or volumes)
- When and how often to back up your server
- Where to store the backups
To continue, click Next.
< Previous
Next >
Finish
Cancel

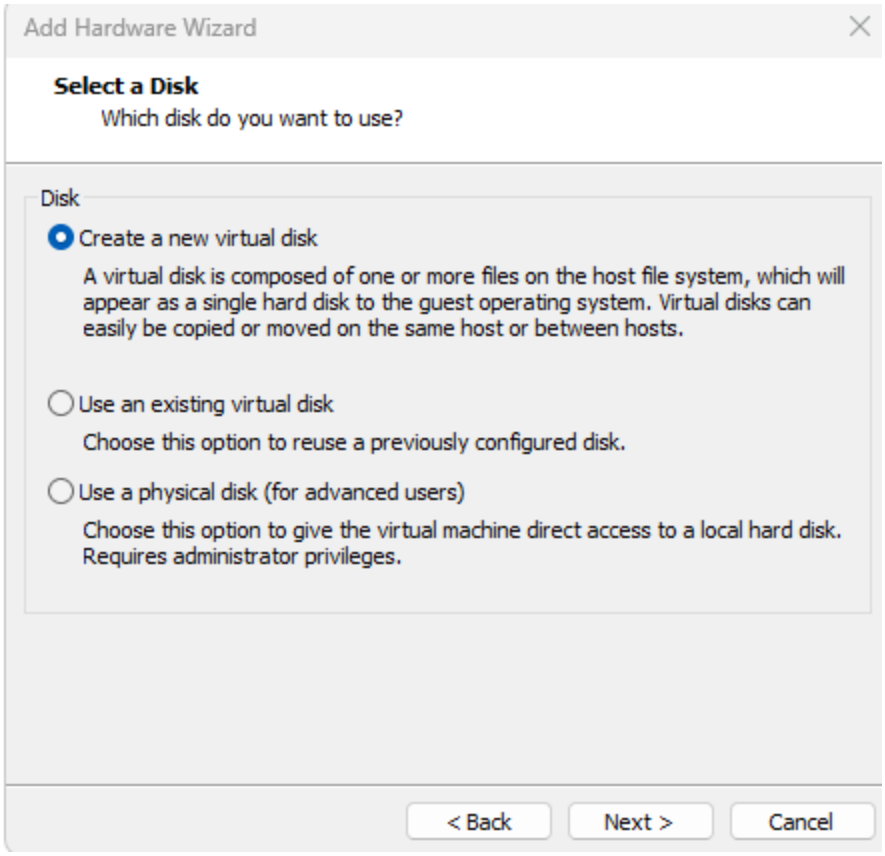

Backup Schedule Wizard
Select Backup Configuration
Getting Started
Select Backup Configurat...
Specify Backup Time
Specify Destination Type
Confirmation
Summary
What type of configuration do you want to schedule?
Full server (recommended)
I want to back up all my server data, applications and system state.
Backup size: 12.96 GB
Custom
I want to choose custom volumes, files for backup.
< Previous
Next >
Finish
Cancel

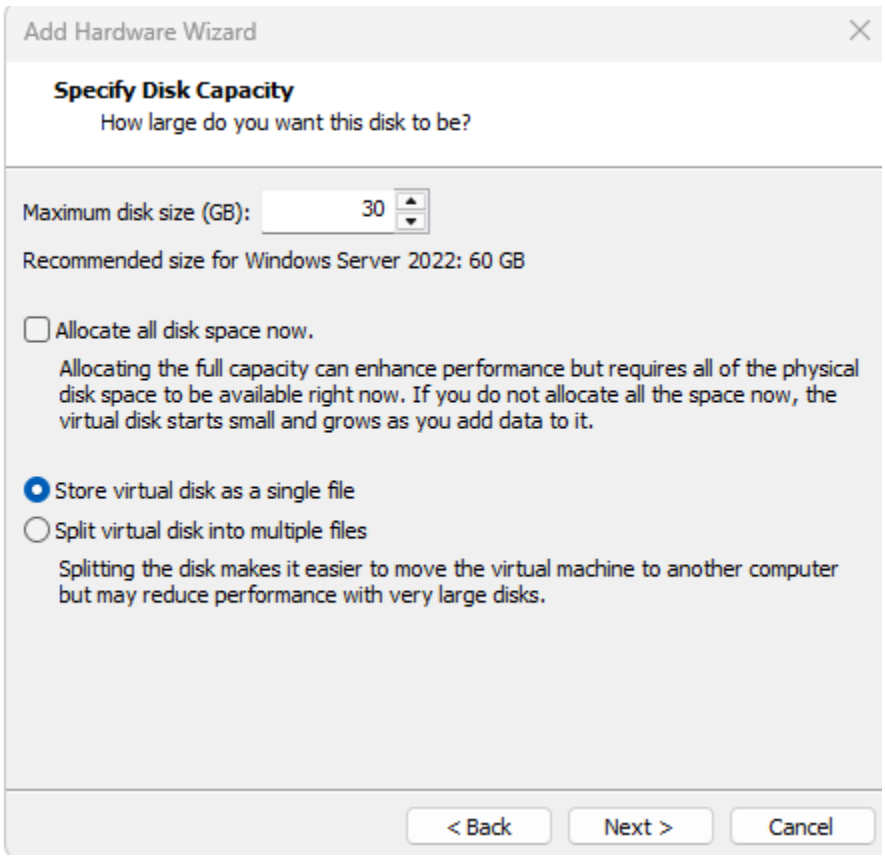

Backup Schedule Wizard
Specify Backup Time
Getting Started
Select Backup Configurat...
Specify Backup Time
Specify Destination Type
Confirmation
Summary
How often and when do you want to run backups?
Once a day
Select time of day:
2:00 AM
More than once a day
Click an available time and then click Add to add it to the backup schedule.
Available time:
12:00 AM
12:30 AM
1:00 AM
1:30 AM
2:00 AM
2:30 AM
3:00 AM
3:30 AM
4:00 AM
4:30 AM
Add >
< Remove
Scheduled time:
9:00 PM
< Previous
Next >
Finish
Cancel

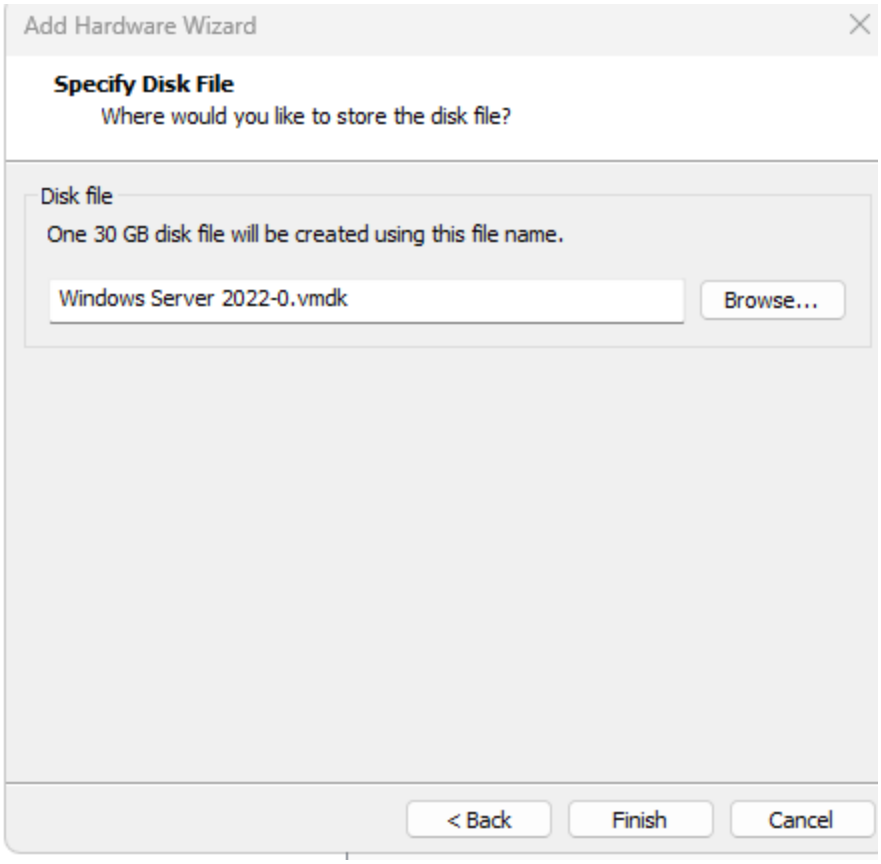

Backup Schedule Wizard
Specify Destination Type
Getting Started
Select Backup Configurat...
Specify Backup Time
Specify Destination Type
Select Destination Disk
Confirmation
Summary
Where do you want to store the backups?
Back up to a hard disk that is dedicated for backups (recommended)
Choose this option for the safest way to store backups. The hard disk that you use will be formatted and then dedicated to only store backups.
Back up to a volume
Choose this option if you cannot dedicate an entire disk for backups. Note that the performance of the volume may be reduced by up to 200 percent while it is used to store backups. We recommend that you do not store other server data on the same volume.
Back up to a shared network folder
Choose this option if you do not want to store backups locally on the server. Note that you will only have one backup at a time because when you create a new backup it overwrites the previous backup.
< Previous
Next >
Finish
Cancel

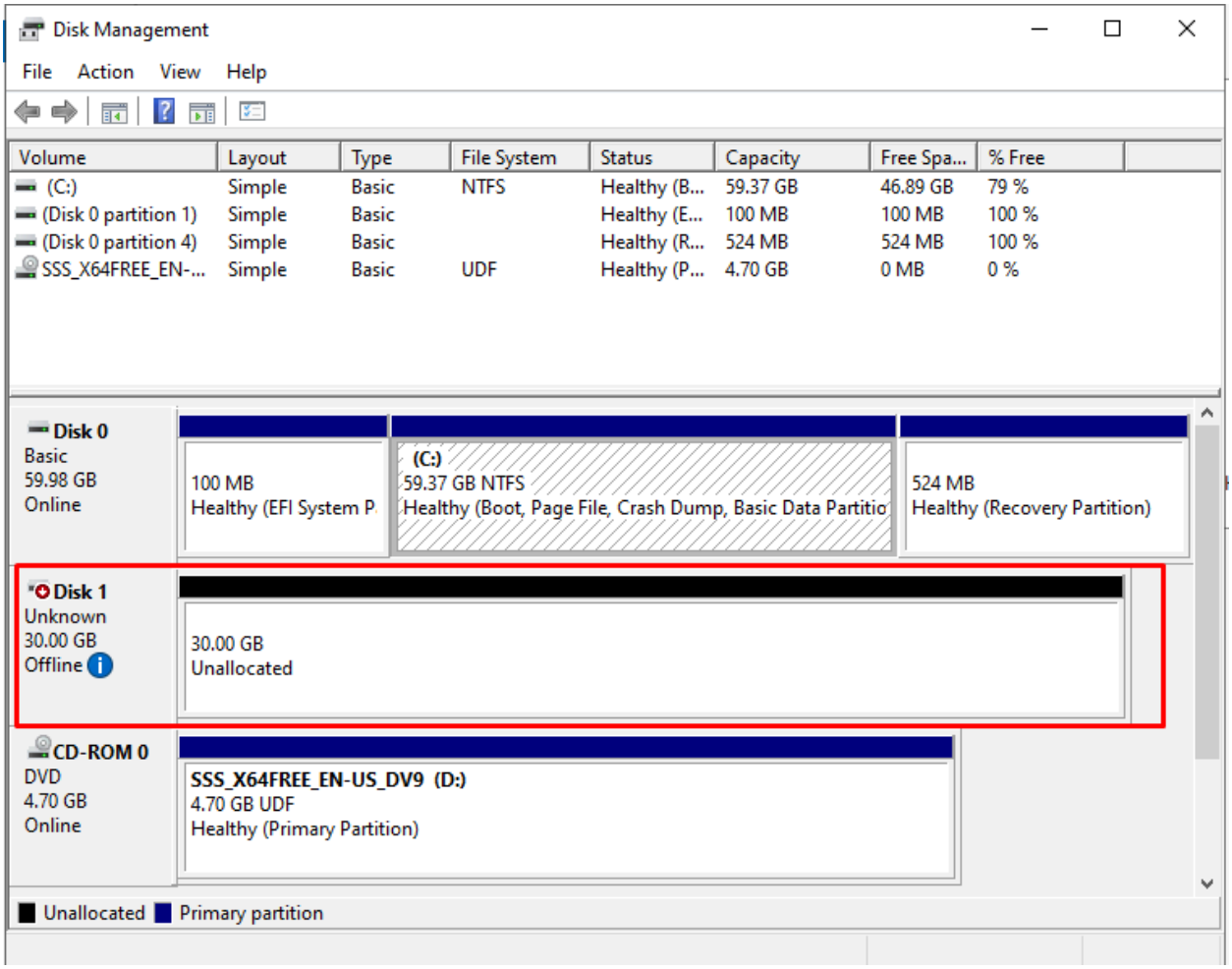

Windows Server 2022 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows Server 2022
Windows 10 x64
Home
Windows Server 2022
Windows Server 2022
Virtual Machine Settings
Hardware
Options
Device
Summary
Memory
2 GB
Processors
2
Hard Disk (NVMe)
60 GB
CD/DVD (SATA)
Using file D:\ISOs\SERVER_EV...
Network Adapter
USB Controller
Sound Card
Display
Disk file
D:\VirtualMachines\Windows Server 2022\Windows Server 2022.vmdk
Capacity
Current size: 12.9 GB
Add Hardware Wizard
Hardware Type
What type of hardware do you want to install?
Hardware types:
Hard Disk
CD/DVD Drive
Floppy Drive
Network Adapter
USB Controller
Sound Card
Parallel Port
Serial Port
Generic SCSI Device
Trusted Platform Module
Explanation
Add a hard disk.
< Back
Next >
Cancel
Defragment
Expand...
Compact
Advanced...
Add...
Remove
OK
Cancel
Help

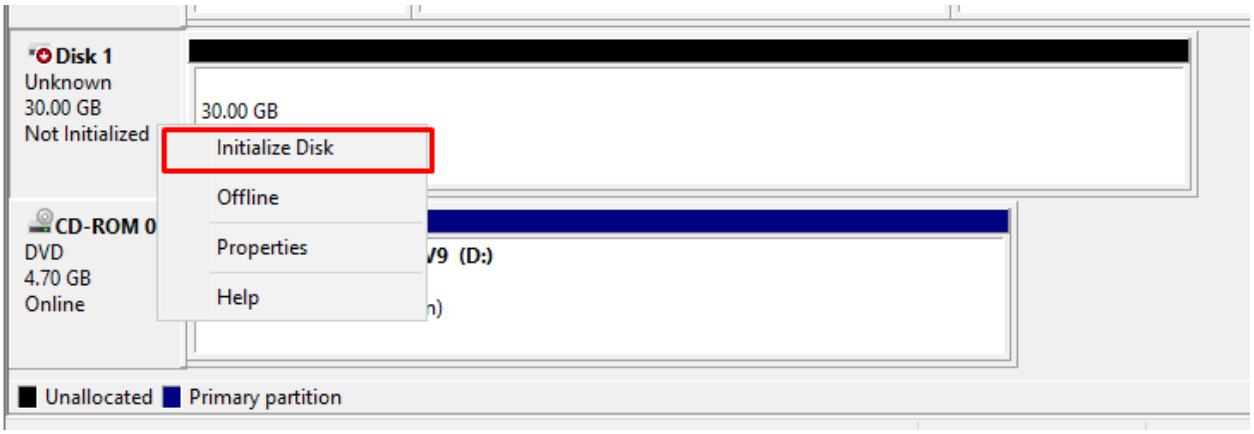

Add Hardware Wizard
Select a Disk Type
What kind of disk do you want to create?
Virtual disk type
IDE
SCSI
SATA
NVMe
(Recommended)
< Back
Next >
Cancel

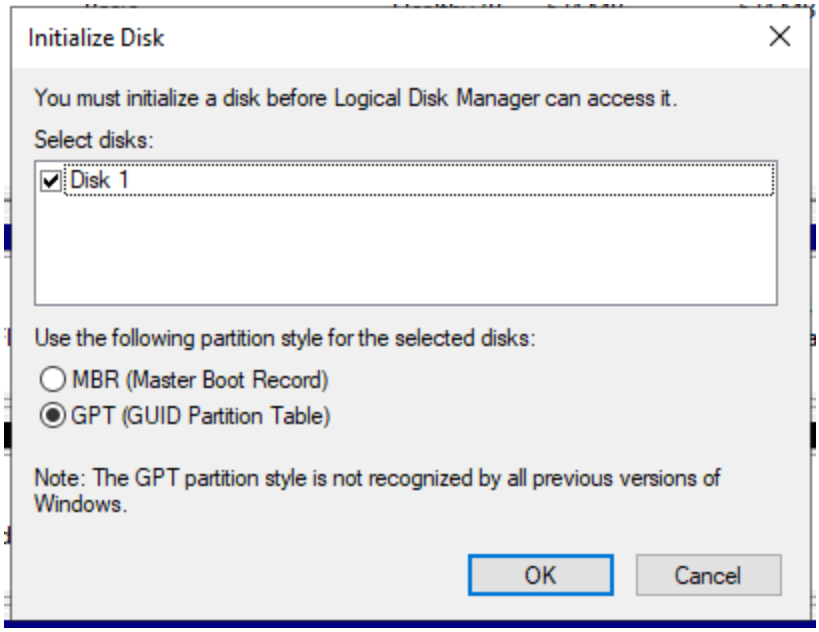

Add Hardware Wizard
Select a Disk
Which disk do you want to use?
Disk
Create a new virtual disk
A virtual disk is composed of one or more files on the host file system, which will appear as a single hard disk to the guest operating system. Virtual disks can easily be copied or moved on the same host or between hosts.
Use an existing virtual disk
Choose this option to reuse a previously configured disk.
Use a physical disk (for advanced users)
Choose this option to give the virtual machine direct access to a local hard disk. Requires administrator privileges.
< Back
Next >
Cancel

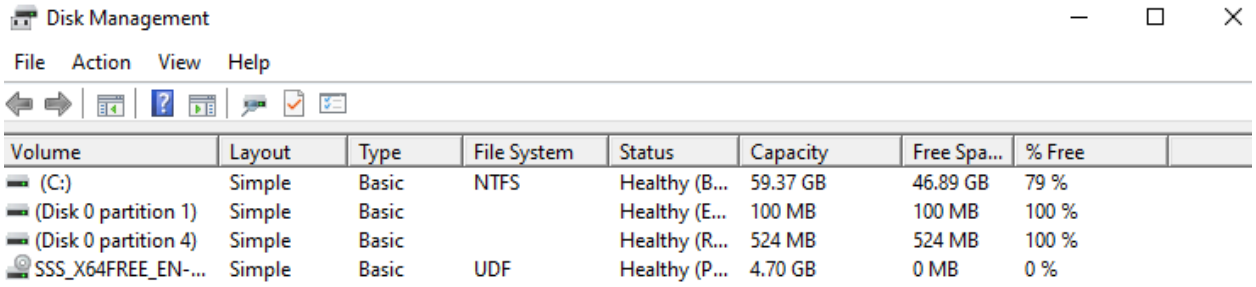

Add Hardware Wizard
Specify Disk Capacity
How large do you want this disk to be?
Maximum disk size (GB):
30
Recommended size for Windows Server 2022: 60 GB
Allocate all disk space now.
Allocating the full capacity can enhance performance but requires all of the physical disk space to be available right now. If you do not allocate all the space now, the virtual disk starts small and grows as you add data to it.
Store virtual disk as a single file
Split virtual disk into multiple files
Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.
< Back
Next >
Cancel

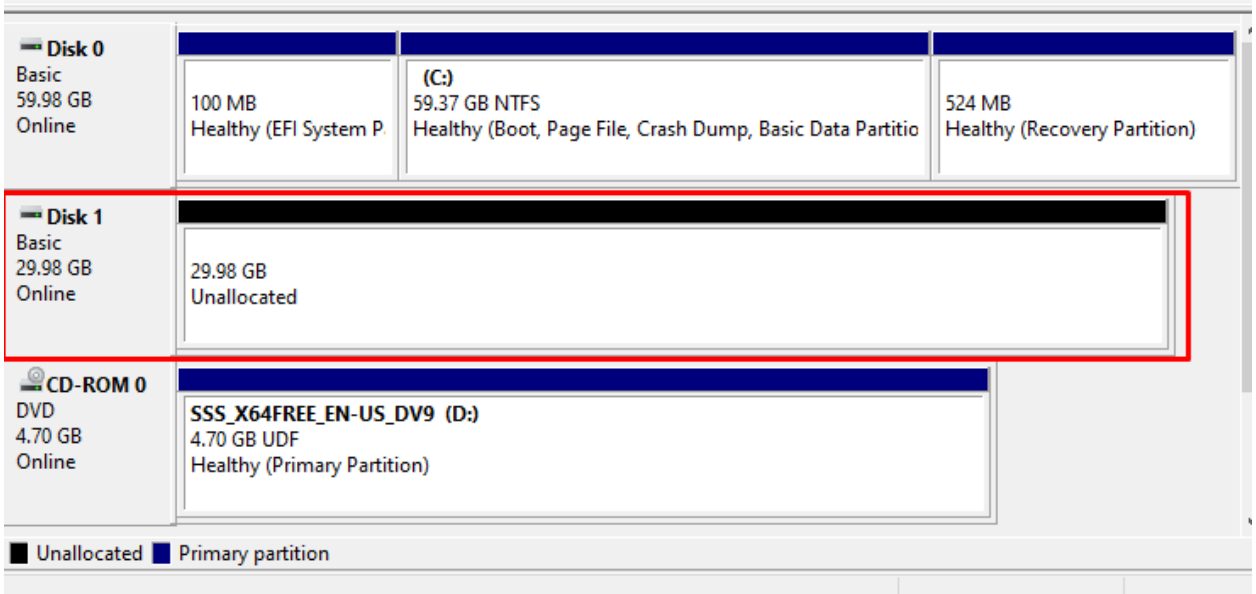

Add Hardware Wizard
Specify Disk File
Where would you like to store the disk file?
Disk file
One 30 GB disk file will be created using this file name.
Windows Server 2022-0.vmdk
Browse...
< Back
Finish
Cancel

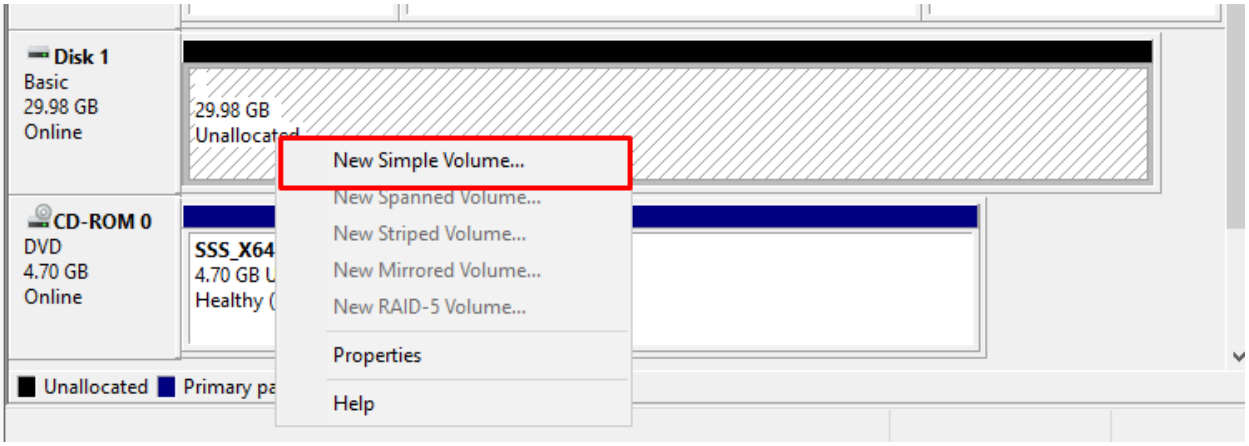

Disk Management
File Action View Help
Volume Layout Type File System Status Capacity Free Spa... % Free
(C:) Simple Basic NTFS Healthy (B... 59.37 GB 46.89 GB 79 %
(Disk 0 partition 1) Simple Basic Healthy (E... 100 MB 100 MB 100 %
(Disk 0 partition 4) Simple Basic Healthy (R... 524 MB 524 MB 100 %
SSS_X64FREE_EN-... Simple Basic UDF Healthy (P... 4.70 GB 0 MB 0 %
Disk 0
Basic
59.98 GB
Online
100 MB
Healthy (EFI System P
(C:)
59.37 GB NTFS
Healthy (Boot, Page File, Crash Dump, Basic Data Partitio
524 MB
Healthy (Recovery Partition)
Disk 1
Unknown
30.00 GB
Offline
30.00 GB
Unallocated
CD-ROM 0
DVD
4.70 GB
Online
SSS_X64FREE_EN-US_DV9 (D:)
4.70 GB UDF
Healthy (Primary Partition)
Unallocated
Primary partition

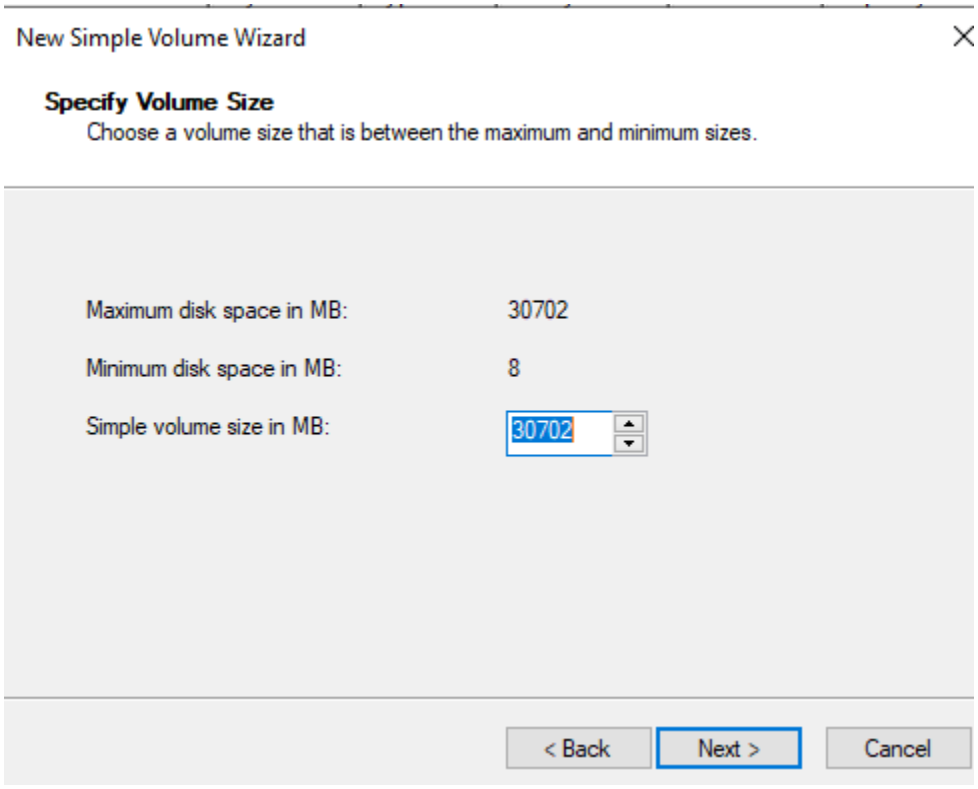

Disk 1
Unknown
30.00 GB
Not Initialized
30.00 GB
Initialize Disk
Offline
Properties
Help
CD-ROM 0
DVD
4.70 GB
Online
Unallocated
Primary partition

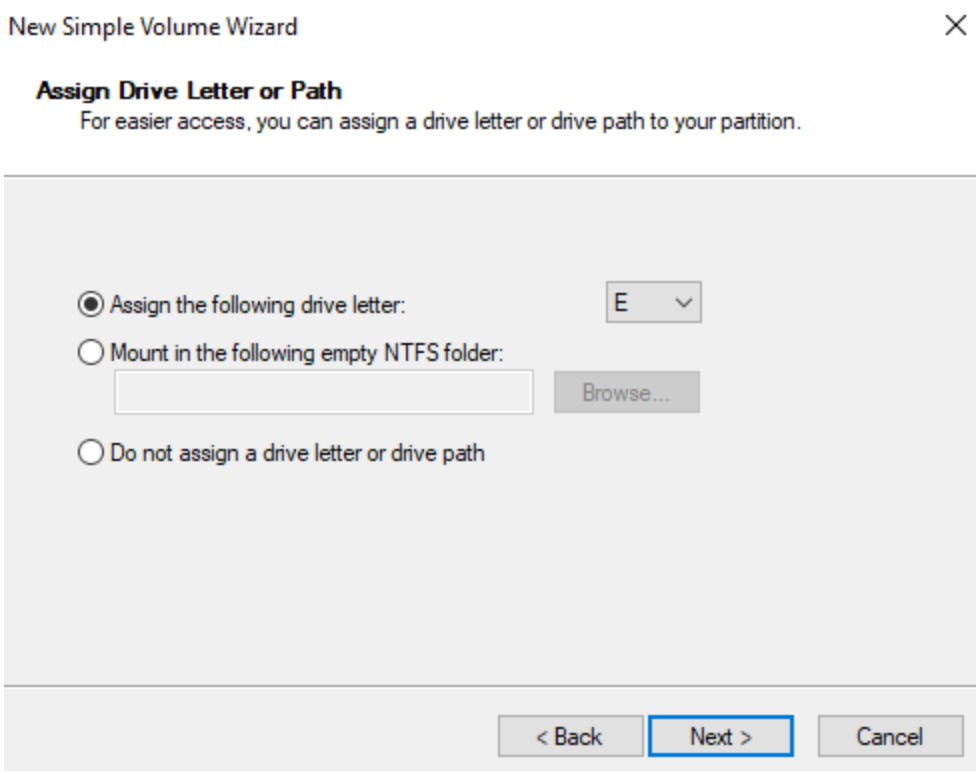

Initialize Disk
You must initialize a disk before Logical Disk Manager can access it.
Select disks:
Disk 1
Use the following partition style for the selected disks:
MBR (Master Boot Record)
GPT (GUID Partition Table)
Note: The GPT partition style is not recognized by all previous versions of Windows.
OK
Cancel

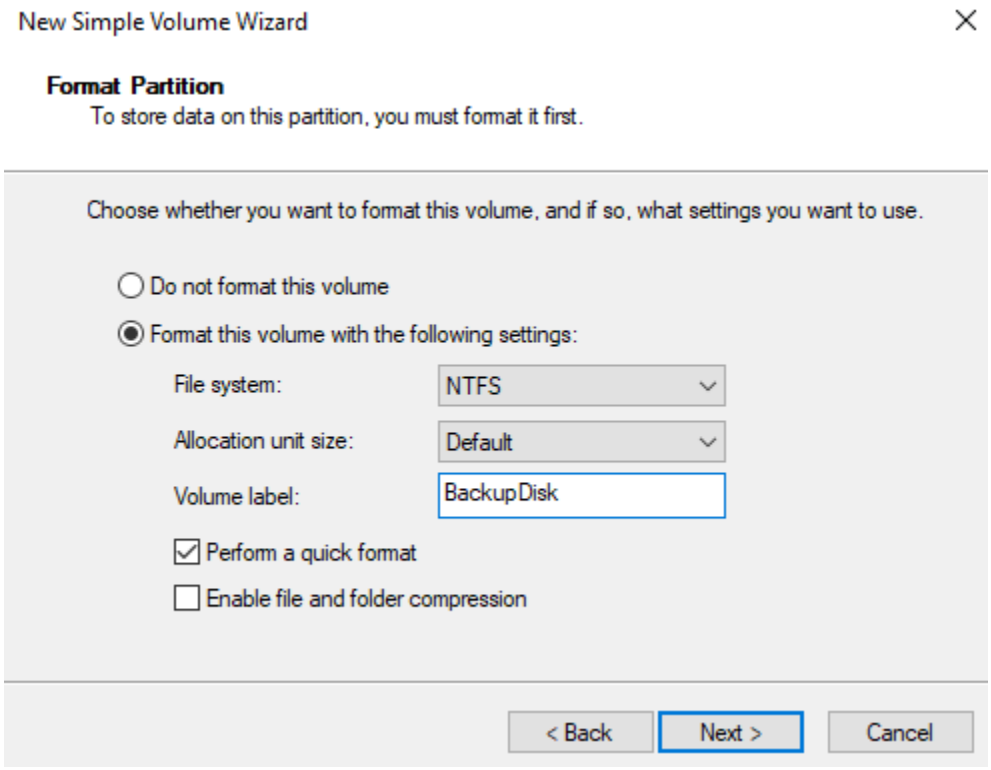

Disk Management
File Action View Help
Volume Layout Type File System Status Capacity Free Spa... % Free
(C:) Simple Basic NTFS Healthy (B... 59.37 GB 46.89 GB 79 %
(Disk 0 partition 1) Simple Basic Healthy (E... 100 MB 100 MB 100 %
(Disk 0 partition 4) Simple Basic Healthy (R... 524 MB 524 MB 100 %
SSS_X64FREE_EN-... Simple Basic UDF Healthy (P... 4.70 GB 0 MB 0 %

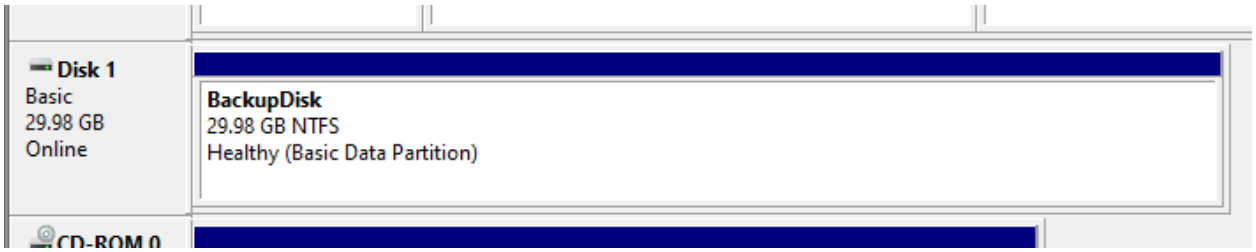

Disk 0
Basic
59.98 GB
Online
100 MB
Healthy (EFI System P
(C:)
59.37 GB NTFS
Healthy (Boot, Page File, Crash Dump, Basic Data Partitio
524 MB
Healthy (Recovery Partition)
Disk 1
Basic
29.98 GB
Online
29.98 GB
Unallocated
CD-ROM 0
DVD
4.70 GB
Online
SSS_X64FREE_EN-US_DV9 (D:)
4.70 GB UDF
Healthy (Primary Partition)
Unallocated
Primary partition


Disk 1
Basic
29.98 GB
Online
29.98 GB
Unallocated
New Simple Volume...
New Spanned Volume...
New Striped Volume...
New Mirrored Volume...
New RAID-5 Volume...
Properties
Help
CD-ROM 0
DVD
4.70 GB
Online
SSS_X64
4.70 GB U
Healthy (
Unallocated
Primary pa


New Simple Volume Wizard
Specify Volume Size
Choose a volume size that is between the maximum and minimum sizes.
Maximum disk space in MB:
30702
Minimum disk space in MB:
8
Simple volume size in MB:
30702
< Back
Next >
Cancel


New Simple Volume Wizard
Assign Drive Letter or Path
For easier access, you can assign a drive letter or drive path to your partition.
Assign the following drive letter:
E
Mount in the following empty NTFS folder:
Browse...
Do not assign a drive letter or drive path
< Back
Next >
Cancel


New Simple Volume Wizard
Format Partition
To store data on this partition, you must format it first.
Choose whether you want to format this volume, and if so, what settings you want to use.
Do not format this volume
Format this volume with the following settings:
File system:
NTFS
Allocation unit size:
Default
Volume label:
BackupDisk
Perform a quick format
Enable file and folder compression
< Back
Next >
Cancel



Backup Schedule Wizard

Select Destination Disk

- Getting Started
- Select Backup Configurat...
- Specify Backup Time
- Specify Destination Type
- Select Destination Disk
- Confirmation
- Summary

Select one or more disks to store your backups. You can use multiple backup disks if you want to store disks offsite.

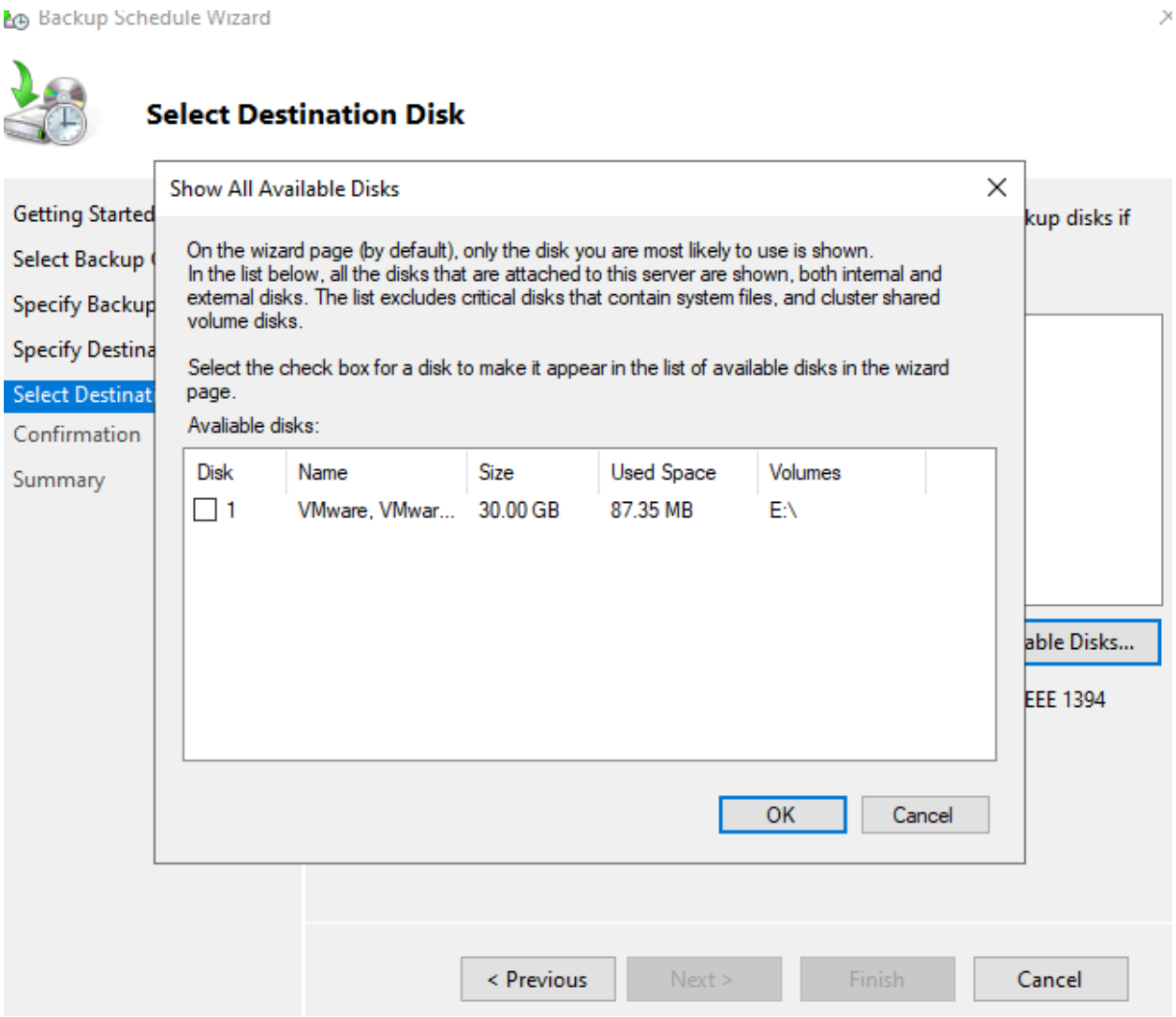
Available disks:

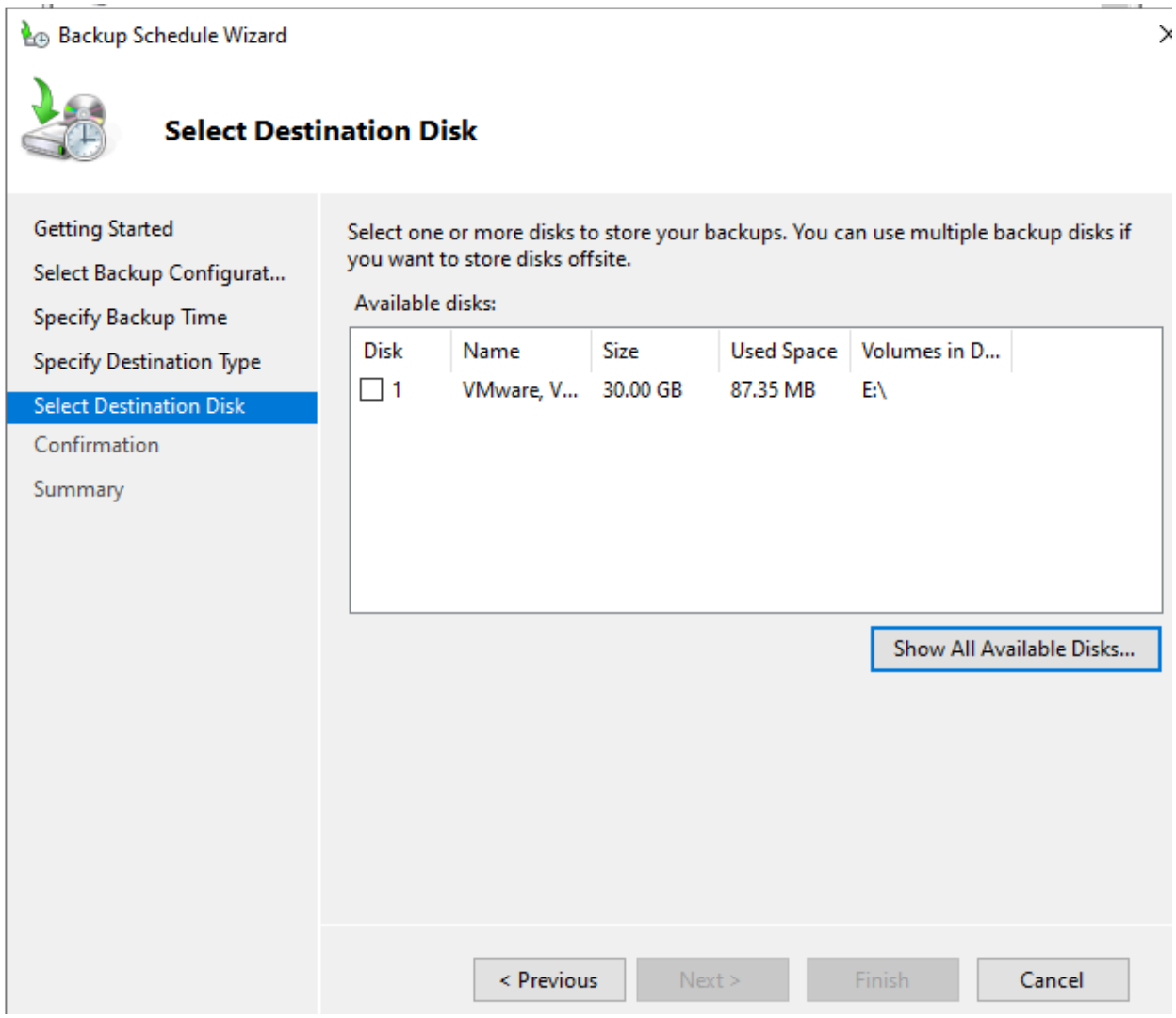
Disk	Name	Size	Used Space	Volumes in D...

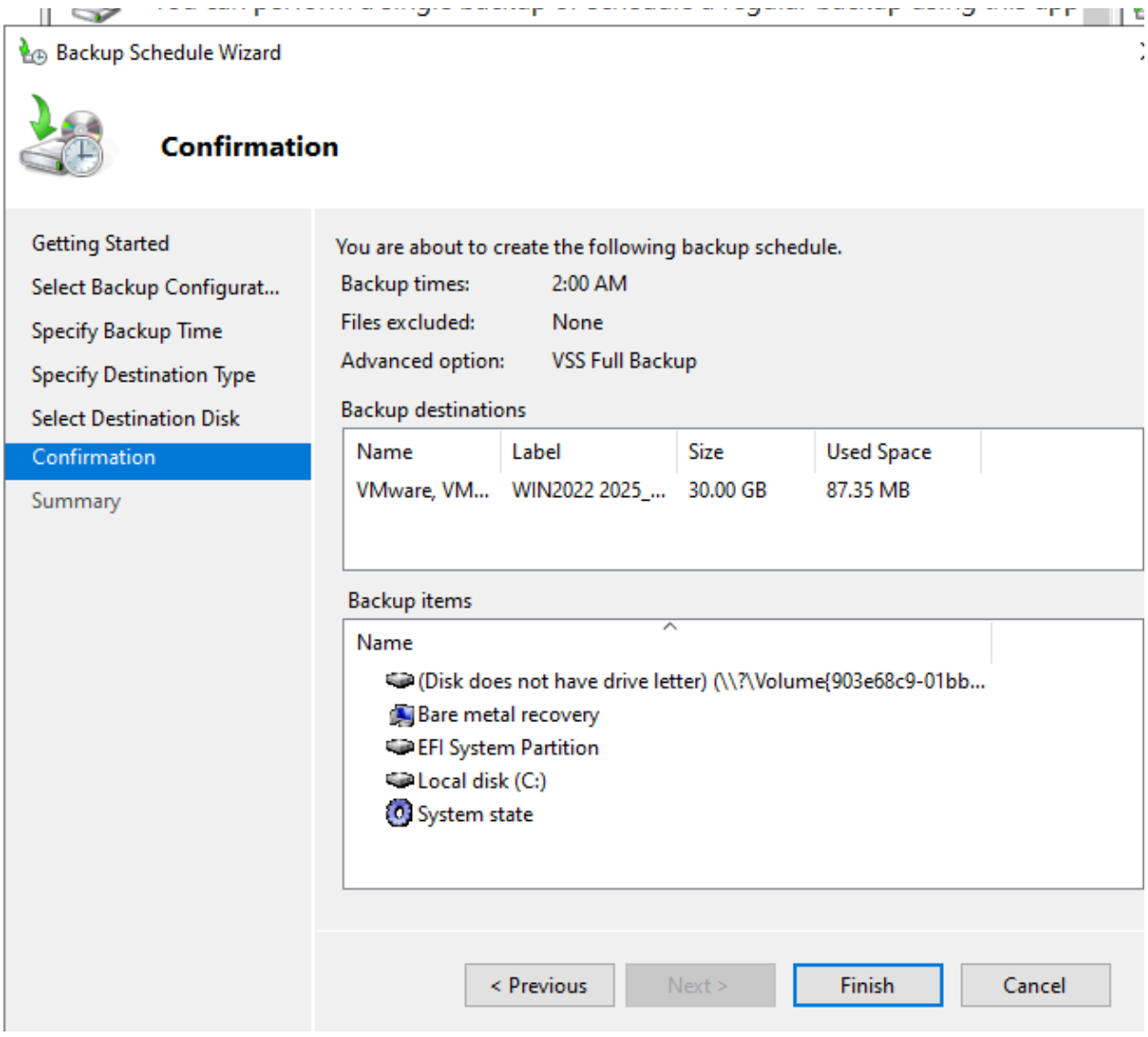
Show All Available Disks...

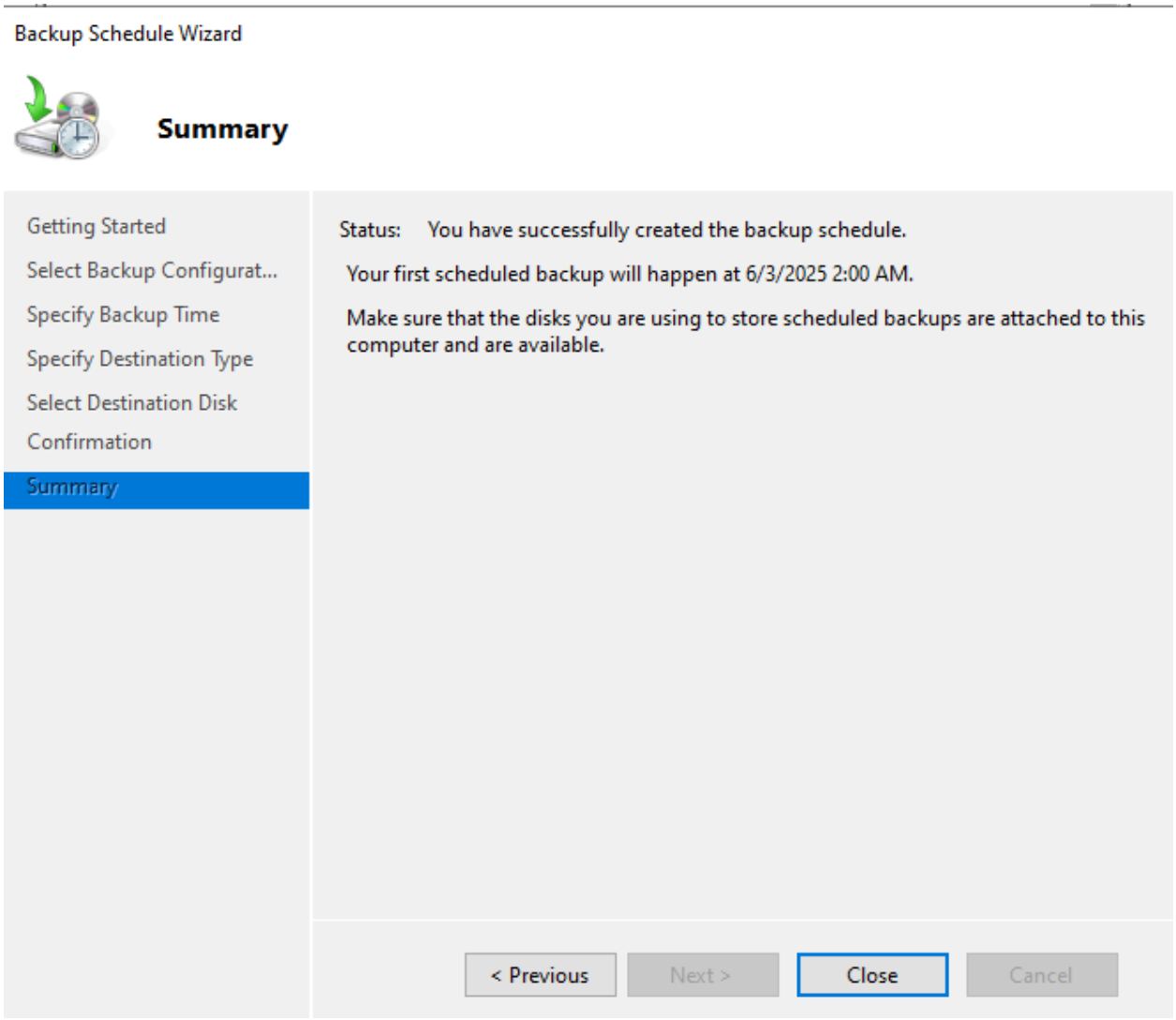
No external disks or disks attached to Universal Serial Bus (USB) or IEEE 1394 ports were found.

< Previous | Next > | Finish | Cancel


Backup Schedule Wizard
Select Destination Disk
Getting Started
Select Backup
Specify Backup
Specify Destina
Select Destinat
Confirmation
Summary
Show All Available Disks
On the wizard page (by default), only the disk you are most likely to use is shown.
In the list below, all the disks that are attached to this server are shown, both internal and external disks. The list excludes critical disks that contain system files, and cluster shared volume disks.
Select the check box for a disk to make it appear in the list of available disks in the wizard page.
Avaliable disks:
Disk
Name
Size
Used Space
Volumes
1
VMware, VMwar...
30.00 GB
87.35 MB
E:\
OK
Cancel
kup disks if
able Disks...
EEE 1394
< Previous
Next >
Finish
Cancel


Backup Schedule Wizard
Select Destination Disk
Getting Started
Select Backup Configurat...
Specify Backup Time
Specify Destination Type
Select Destination Disk
Confirmation
Summary
Select one or more disks to store your backups. You can use multiple backup disks if you want to store disks offsite.
Available disks:
Disk
Name
Size
Used Space
Volumes in D...
1
VMware, V...
30.00 GB
87.35 MB
E:\
Show All Available Disks...
< Previous
Next >
Finish
Cancel

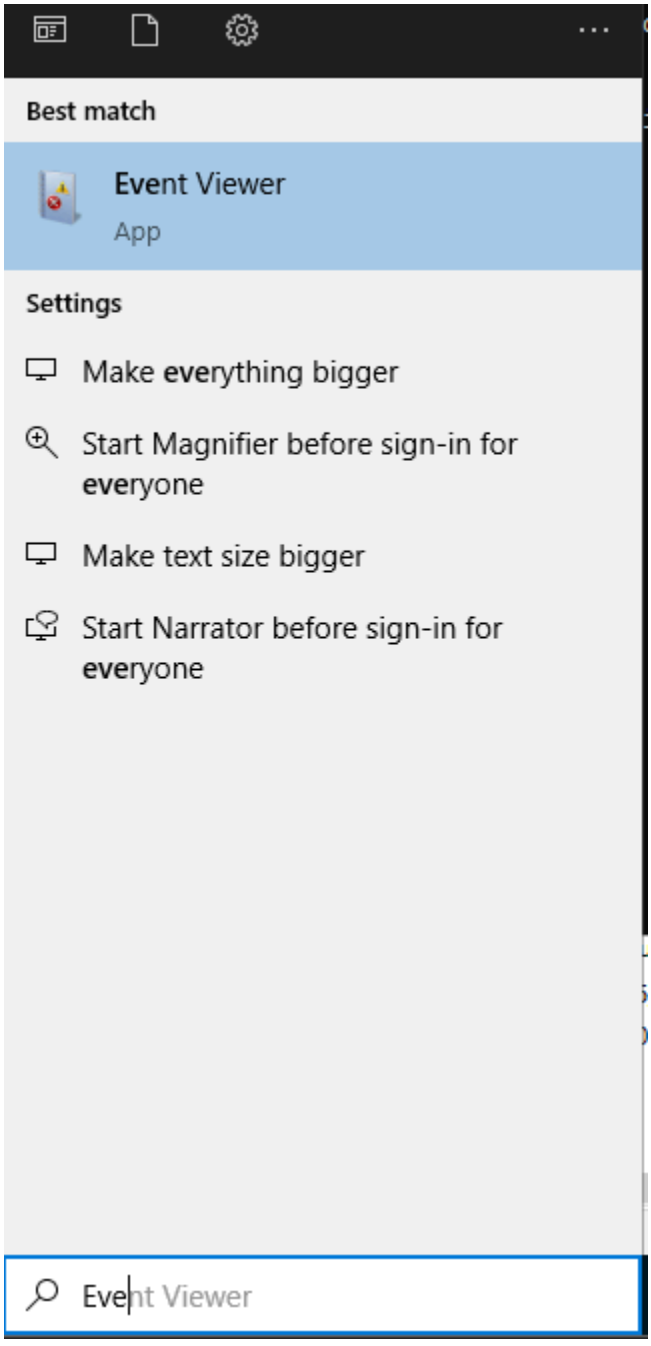

Backup Schedule Wizard
Confirmation
Getting Started
Select Backup Configurat...
Specify Backup Time
Specify Destination Type
Select Destination Disk
Confirmation
Summary
You are about to create the following backup schedule.
Backup times: 2:00 AM
Files excluded: None
Advanced option: VSS Full Backup
Backup destinations
Name
Label
Size
Used Space
VMware, VM...
WIN2022 2025_...
30.00 GB
87.35 MB
Backup items
Name
(Disk does not have drive letter) (\\?\Volume{903e68c9-01bb...
Bare metal recovery
EFI System Partition
Local disk (C:)
System state
< Previous
Next >
Finish
Cancel

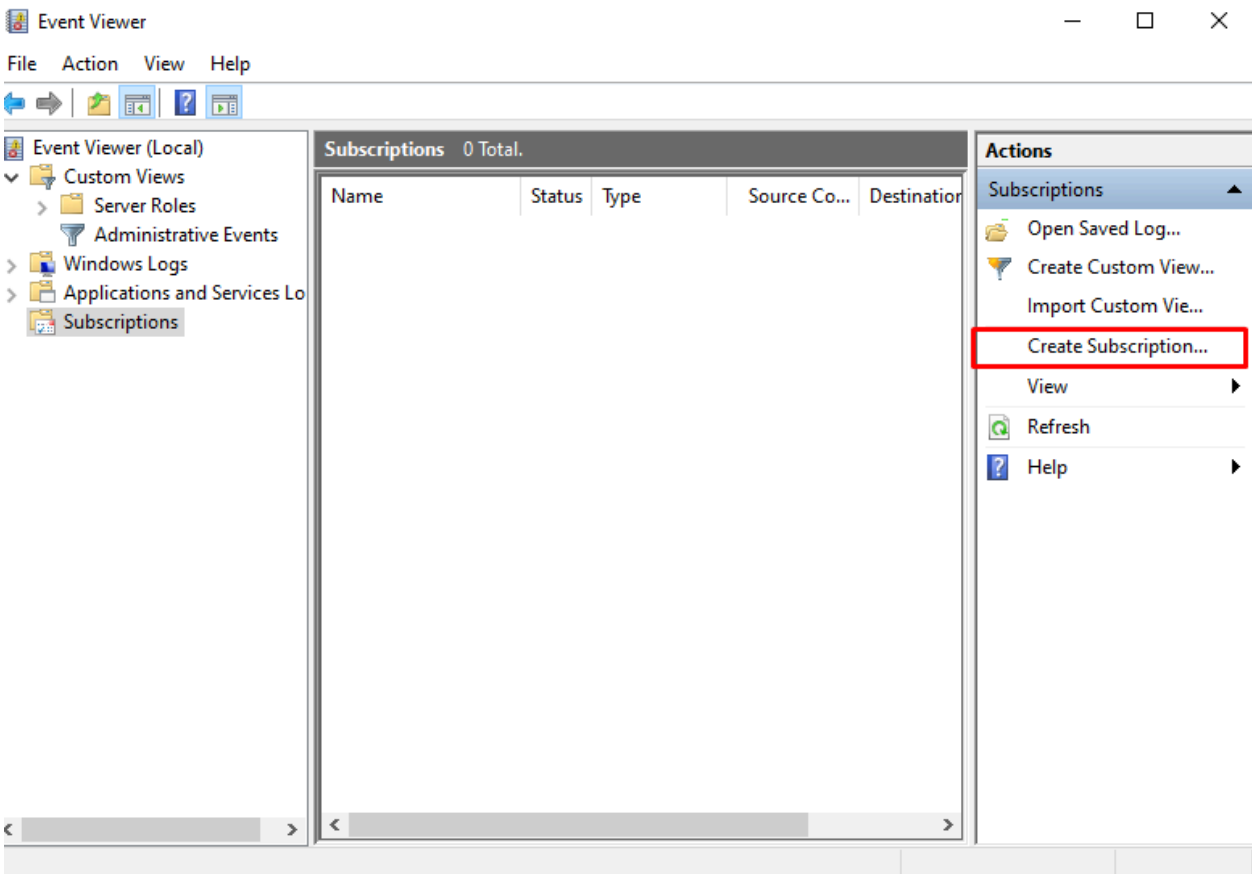


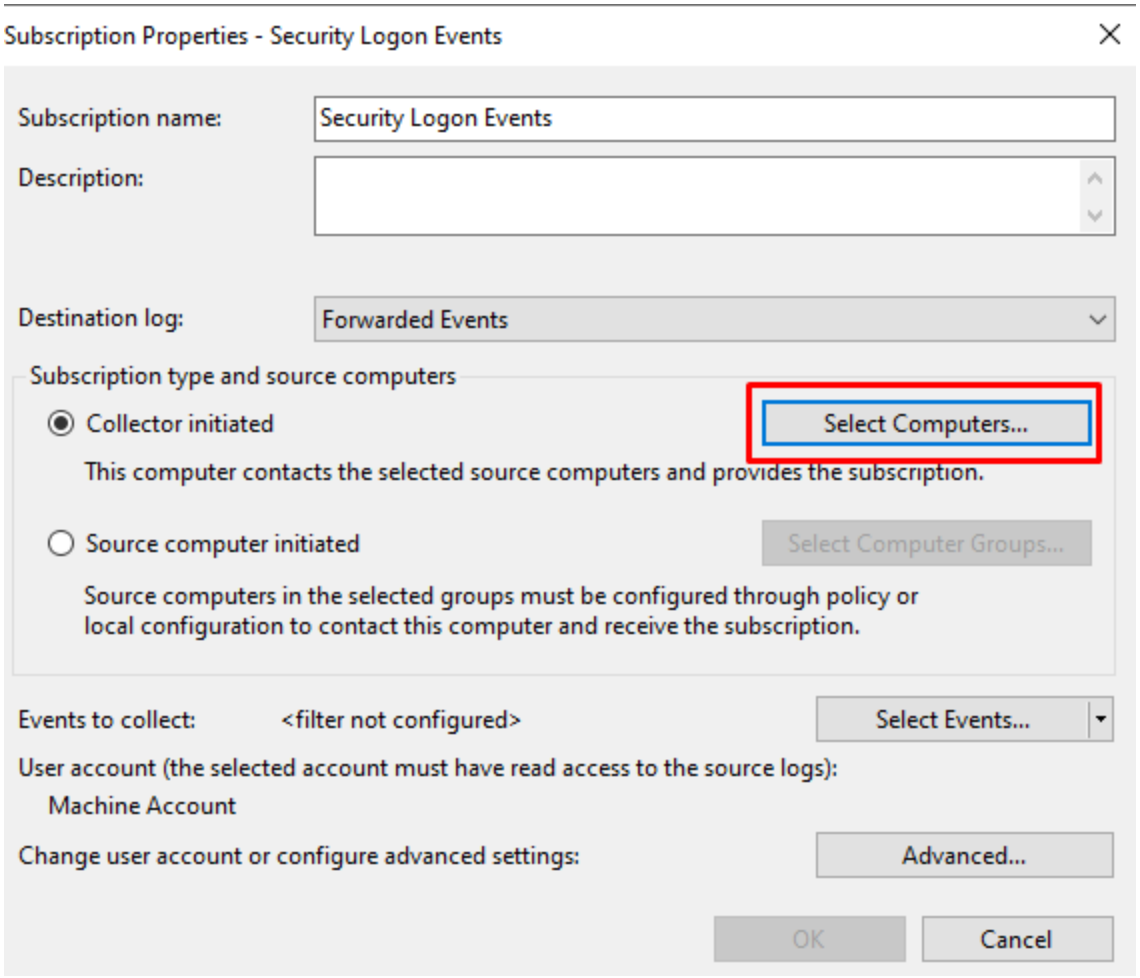
Backup successful scheduled and created to run every day.

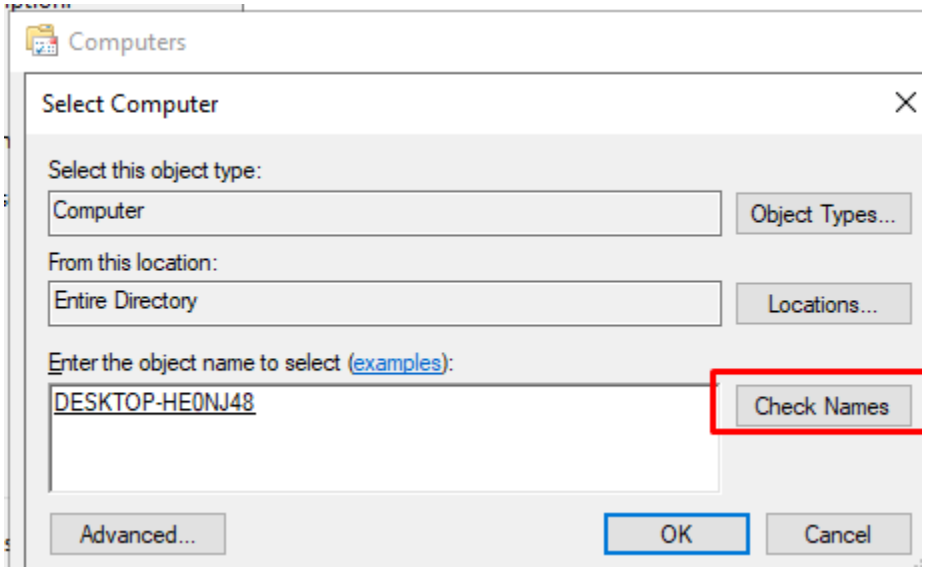
Next Step: Set Up Windows Event Forwarding (WEF)

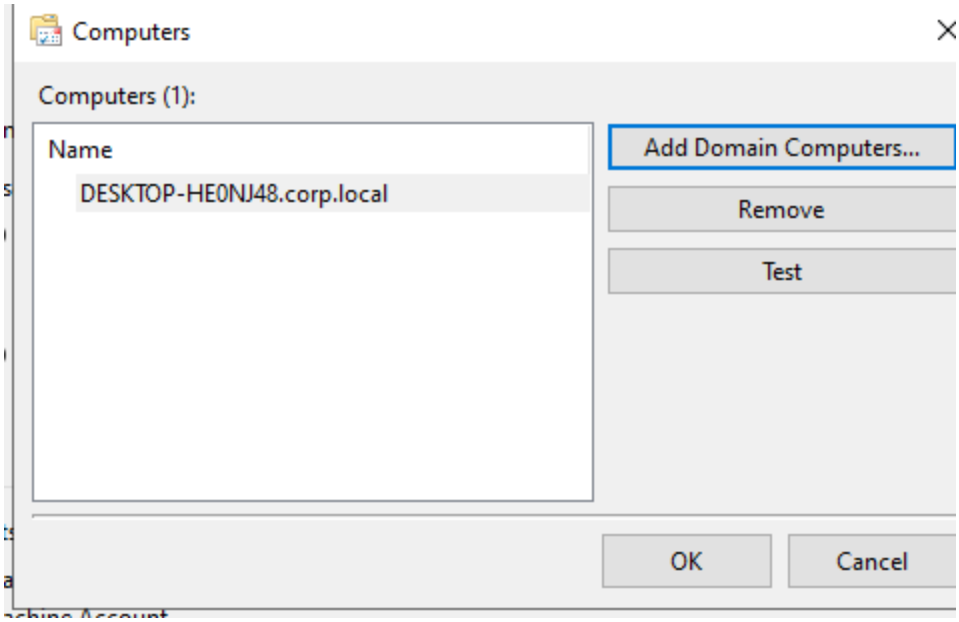
```
C:\Users\Administrator>winrm quickconfig
WinRM service is already running on this machine.
WinRM is already set up for remote management on this computer.

C:\Users\Administrator>_
```

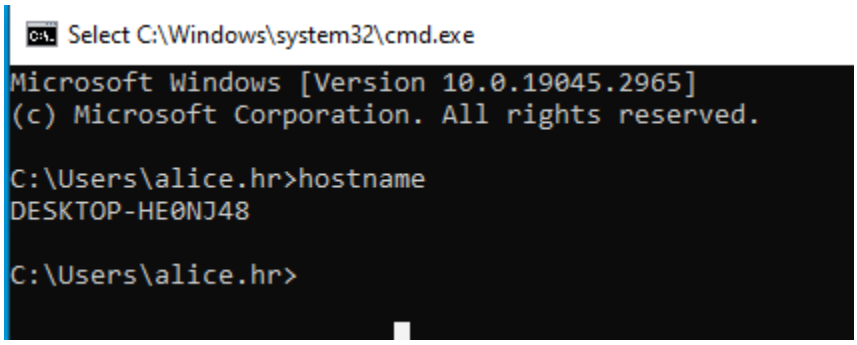


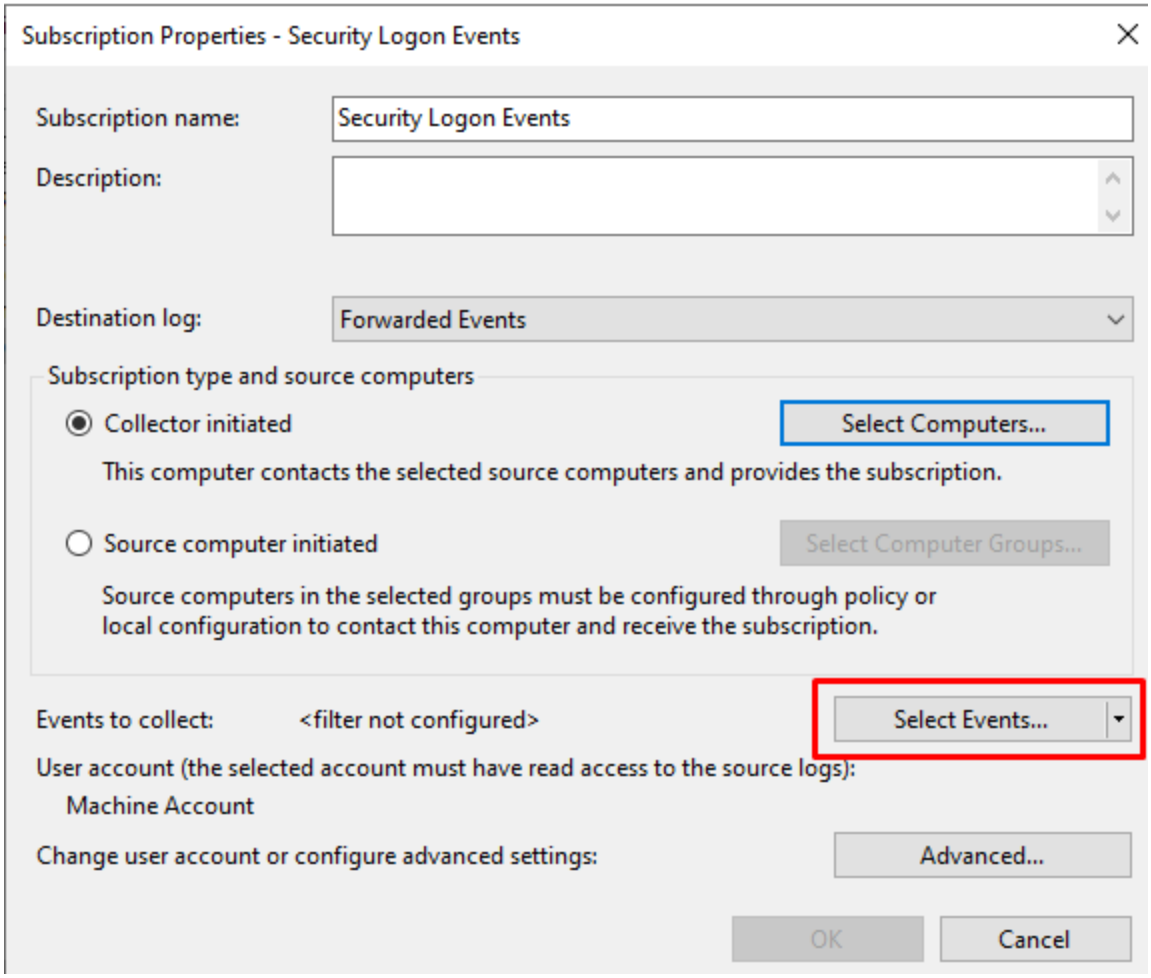

Event Viewer
File
Action
View
Help
Event Viewer (Local)
Custom Views
Server Roles
Administrative Events
Windows Logs
Applications and Services Lo
Subscriptions
Subscriptions 0 Total.
Name
Status
Type
Source Co...
Destinatior
Actions
Subscriptions
Open Saved Log...
Create Custom View...
Import Custom Vie...
Create Subscription...
View
Refresh
Help

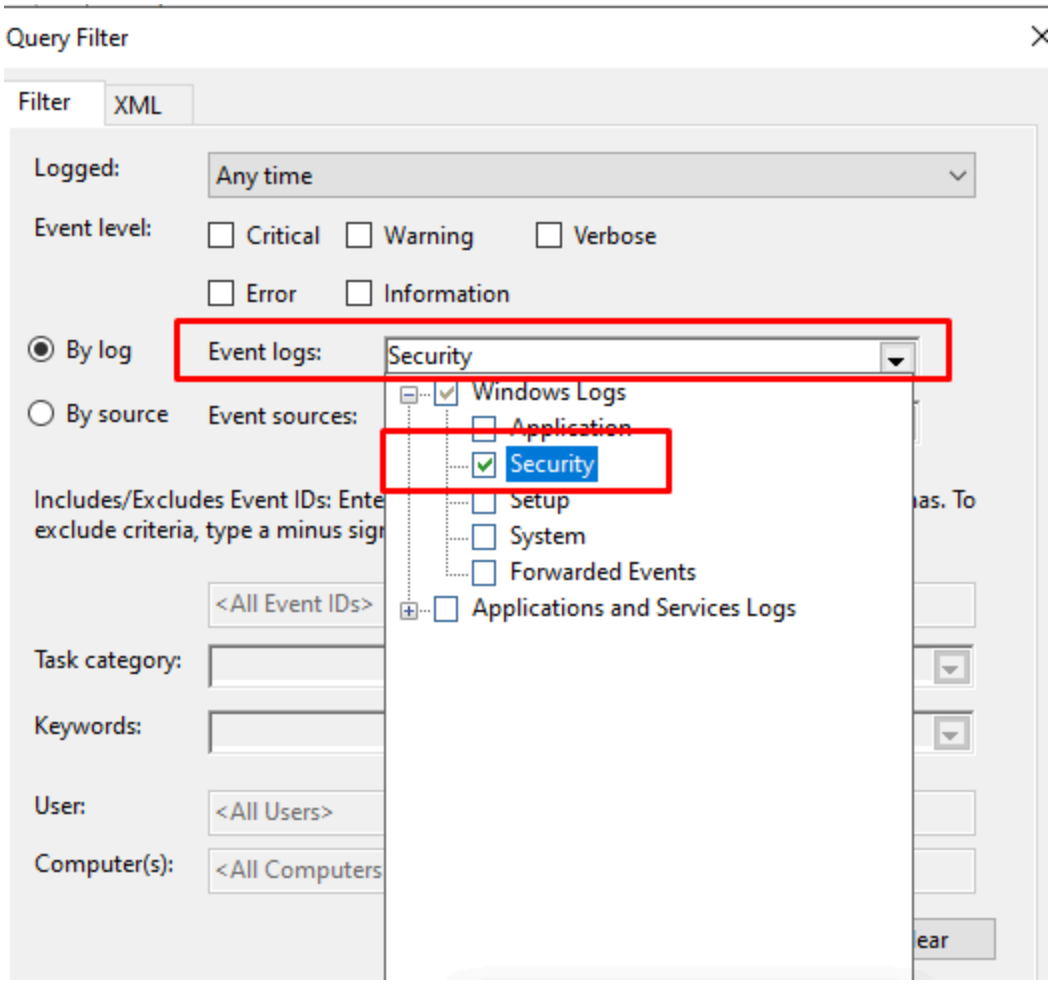

Subscription Properties - Security Logon Events
Subscription name:
Security Logon Events
Description:
Destination log:
Forwarded Events
Subscription type and source computers
Collector initiated
Select Computers...
This computer contacts the selected source computers and provides the subscription.
Source computer initiated
Select Computer Groups...
Source computers in the selected groups must be configured through policy or local configuration to contact this computer and receive the subscription.
Events to collect:
<filter not configured>
Select Events...
User account (the selected account must have read access to the source logs):
Machine Account
Change user account or configure advanced settings:
Advanced...
OK
Cancel

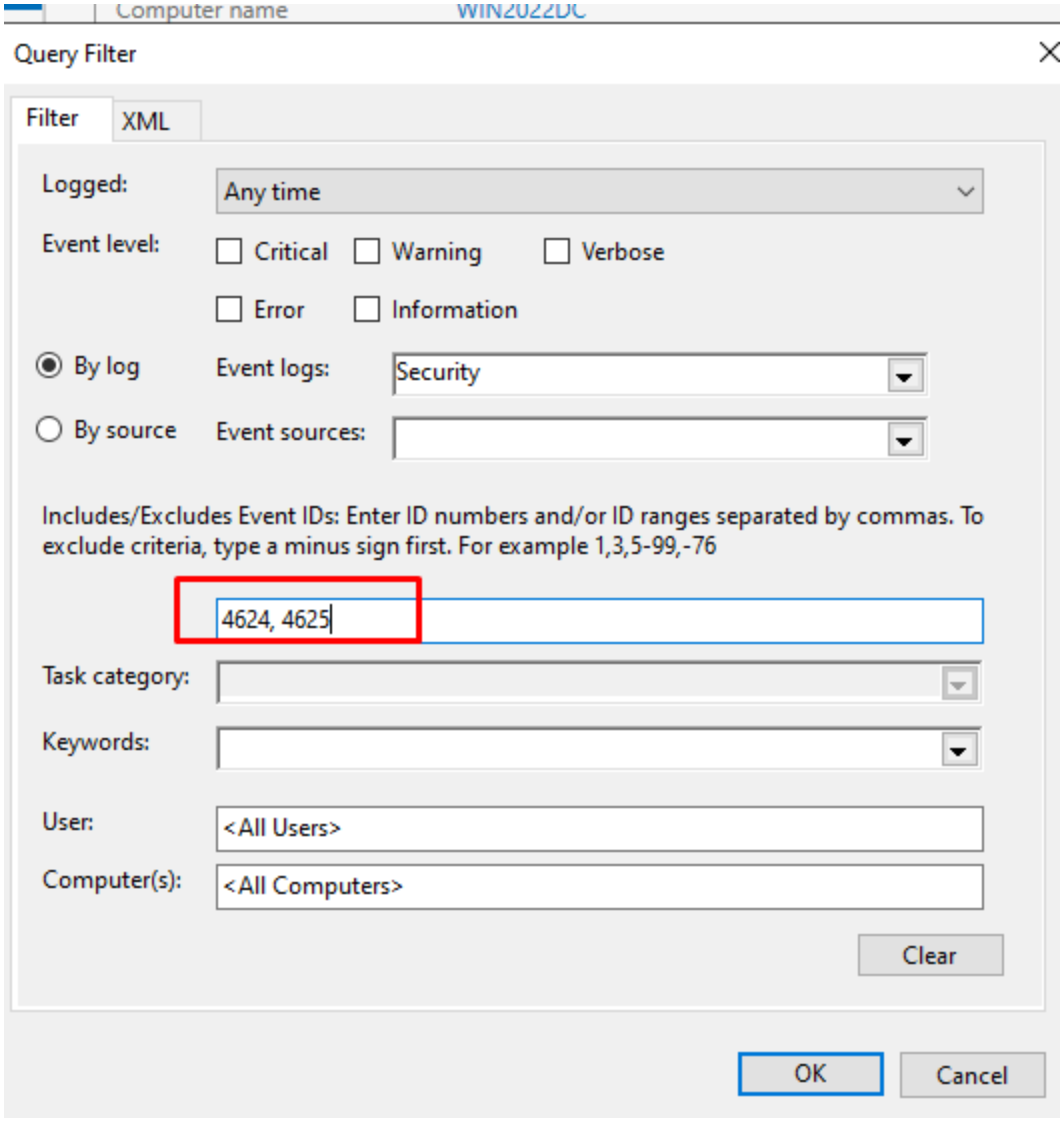

Computers
Select Computer
Select this object type:
Computer
Object Types...
From this location:
Entire Directory
Locations...
Enter the object name to select (examples):
DESKTOP-HE0NJ48
Check Names
Advanced...
OK
Cancel

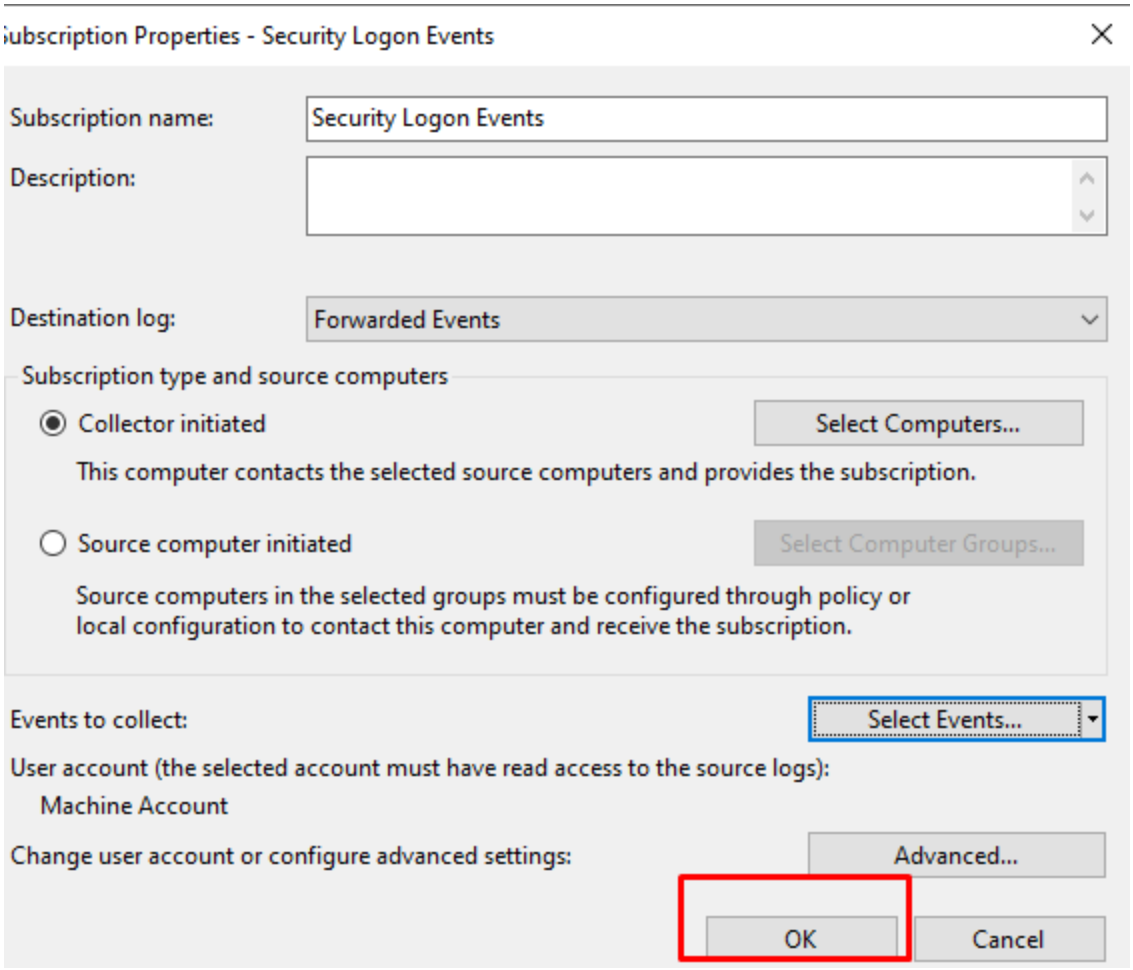

Computers
Computers (1):
Name
DESKTOP-HE0NJ48.corp.local
Add Domain Computers...
Remove
Test
OK
Cancel

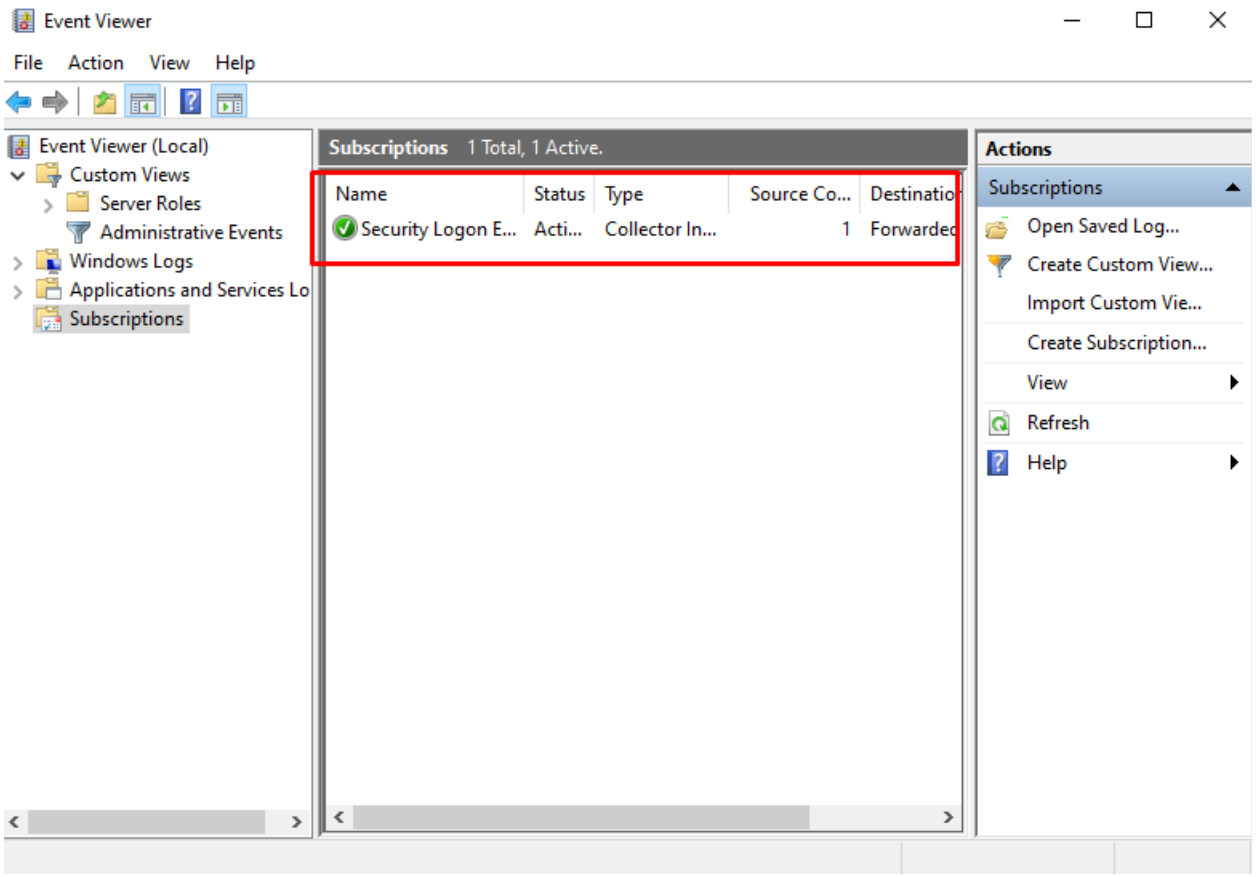

Select C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.
C:\Users\alice.hr>hostname
DESKTOP-HE0NJ48
C:\Users\alice.hr>


Subscription Properties - Security Logon Events
Subscription name:
Security Logon Events
Description:
Destination log:
Forwarded Events
Subscription type and source computers
Collector initiated
Select Computers...
This computer contacts the selected source computers and provides the subscription.
Source computer initiated
Select Computer Groups...
Source computers in the selected groups must be configured through policy or local configuration to contact this computer and receive the subscription.
Events to collect:
<filter not configured>
Select Events...
User account (the selected account must have read access to the source logs):
Machine Account
Change user account or configure advanced settings:
Advanced...
OK
Cancel


Query Filter
Filter
XML
Logged:
Any time
Event level:
Critical
Warning
Verbose
Error
Information
By log
Event logs:
Security
By source
Event sources:
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Logs
Includes/Excludes Event IDs: Ente
exclude criteria, type a minus sig
as. To
<All Event IDs>
Task category:
Keywords:
User:
<All Users>
Computer(s):
<All Computers
ear

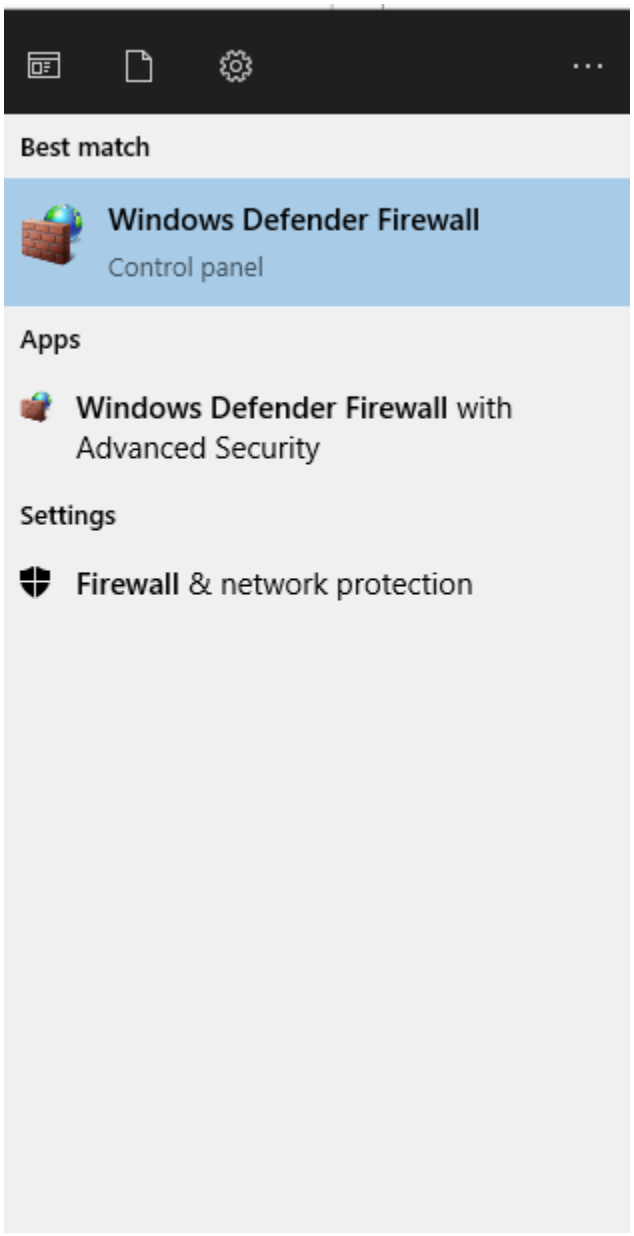

Computer name
WIN2022DC
Query Filter
Filter
XML
Logged:
Any time
Event level:
Critical
Warning
Verbose
Error
Information
By log
Event logs:
Security
By source
Event sources:
Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76
4624, 4625
Task category:
Keywords:
User:
<All Users>
Computer(s):
<All Computers>
Clear
OK
Cancel

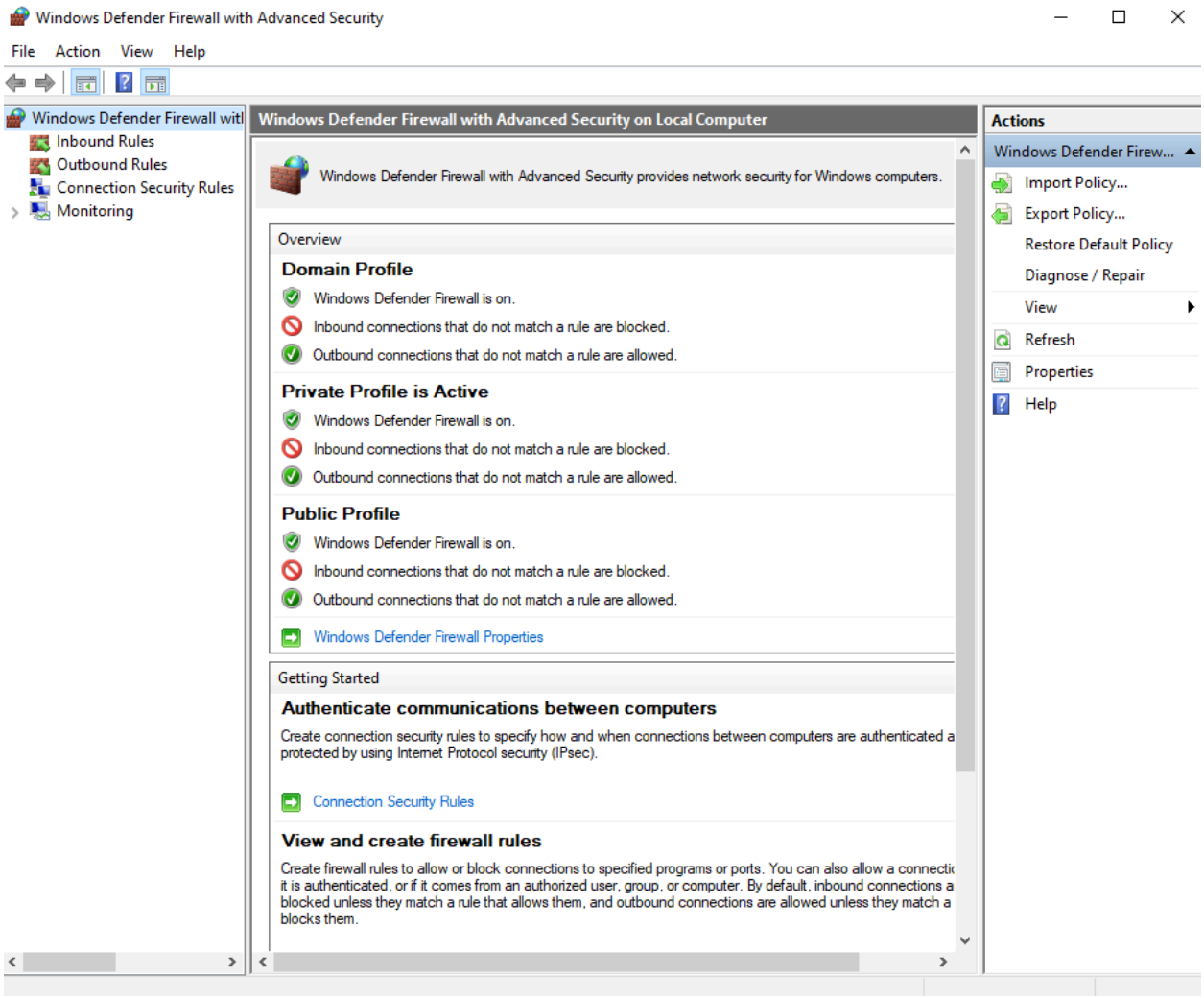

Subscription Properties - Security Logon Events
Subscription name:
Security Logon Events
Description:
Destination log:
Forwarded Events
Subscription type and source computers
Collector initiated
Select Computers...
This computer contacts the selected source computers and provides the subscription.
Source computer initiated
Select Computer Groups...
Source computers in the selected groups must be configured through policy or local configuration to contact this computer and receive the subscription.
Events to collect:
Select Events...
User account (the selected account must have read access to the source logs):
Machine Account
Change user account or configure advanced settings:
Advanced...
OK
Cancel

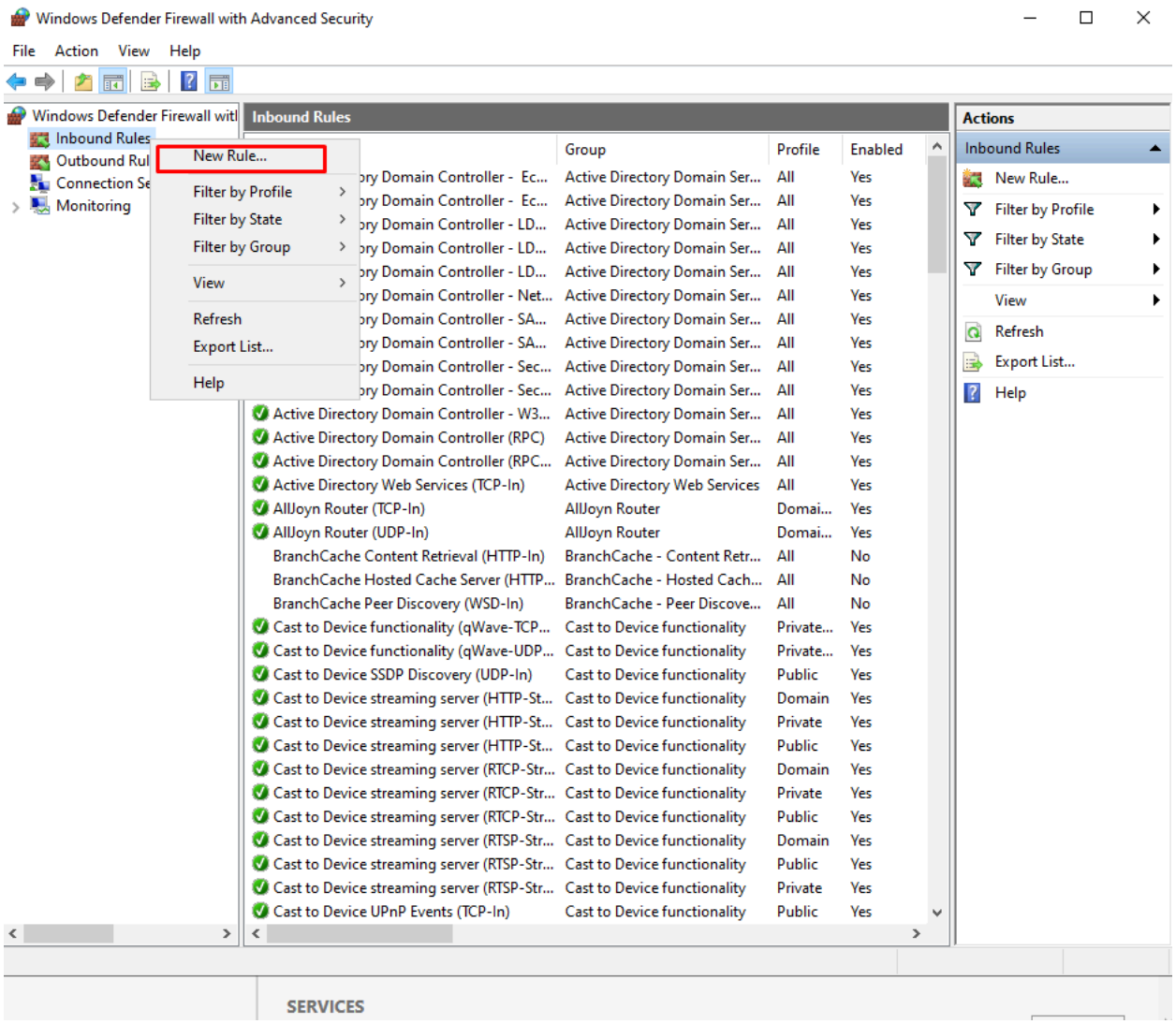


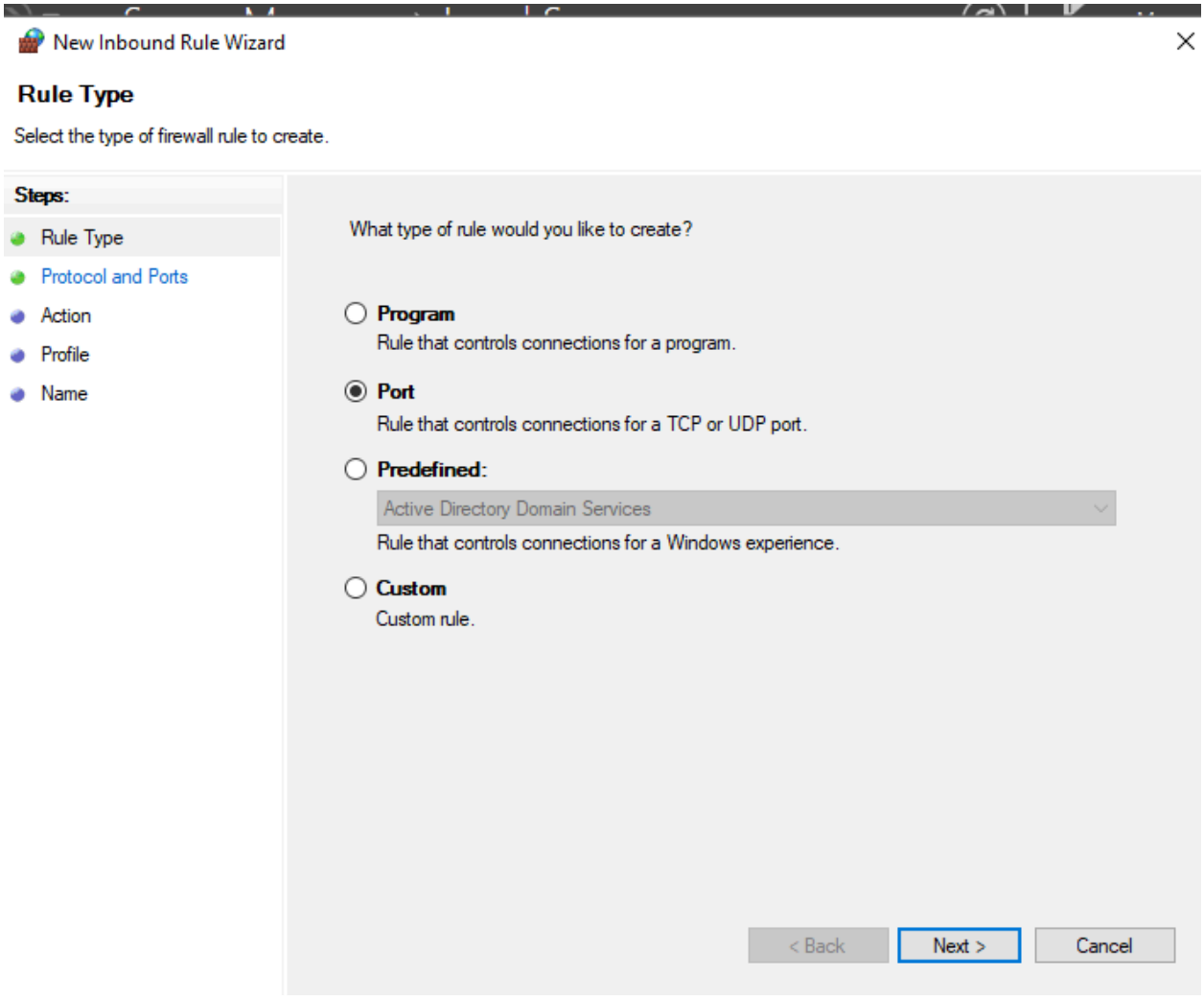
WEF Event Successfully Created

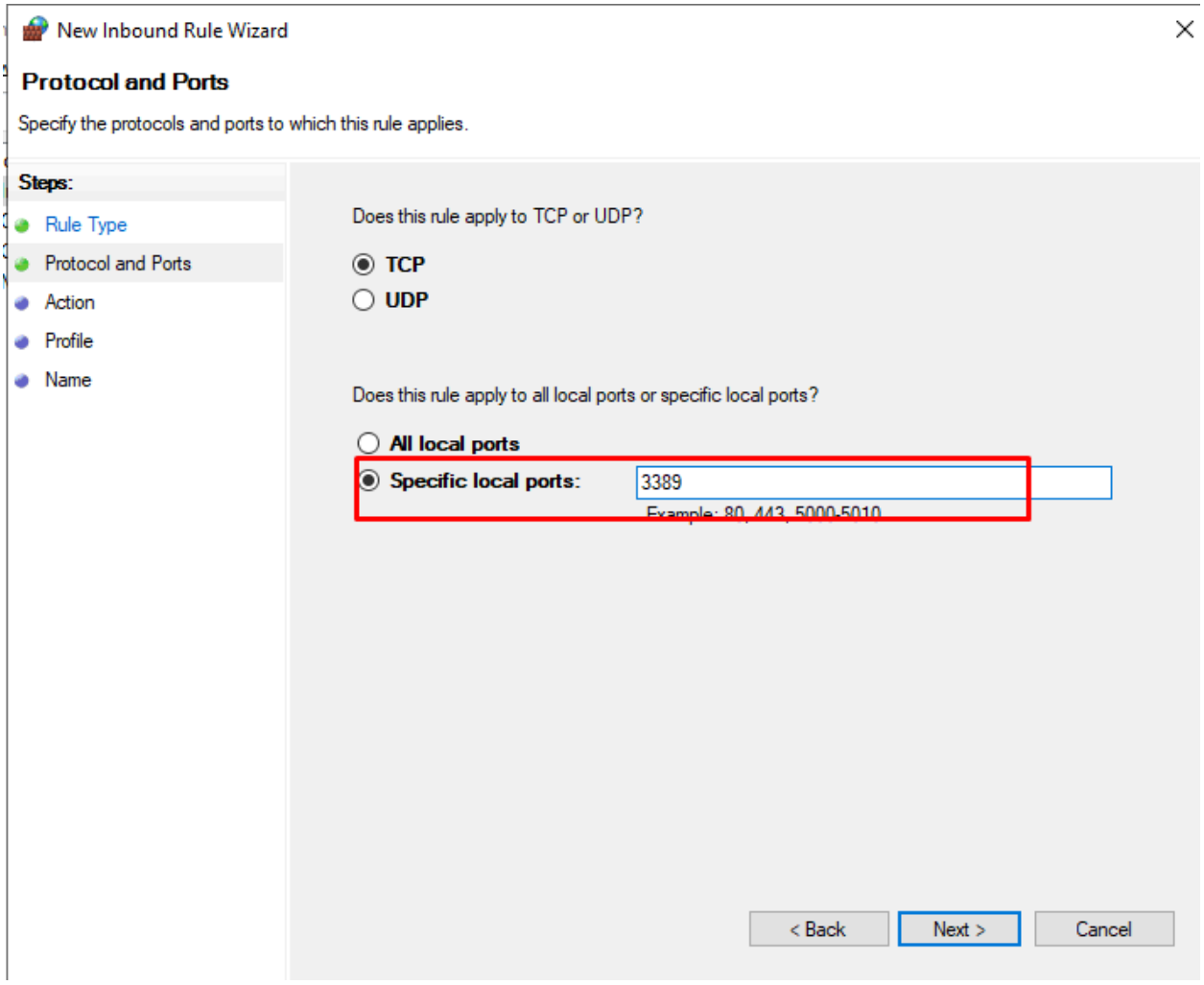
Windows Server 2022: Create Firewall

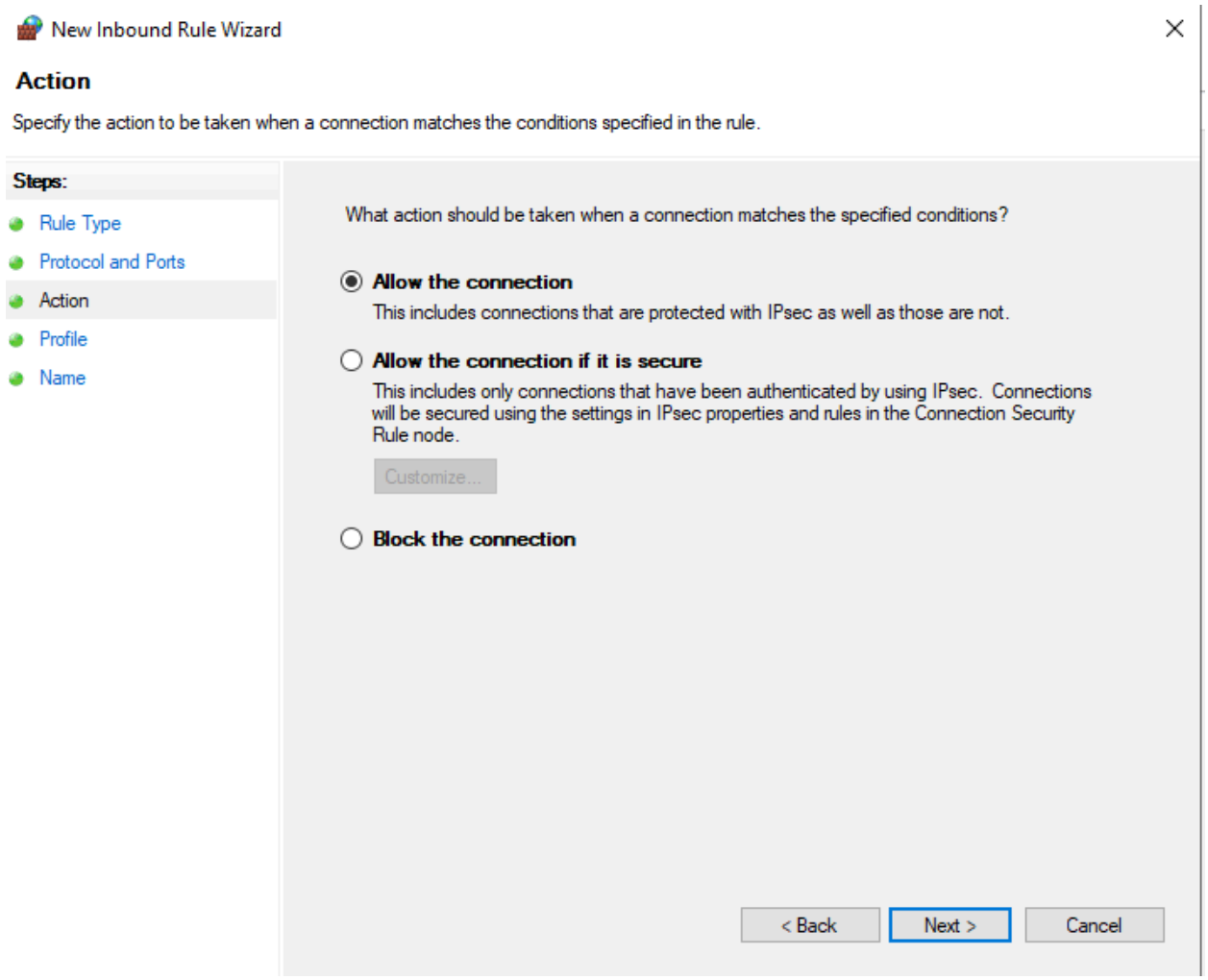


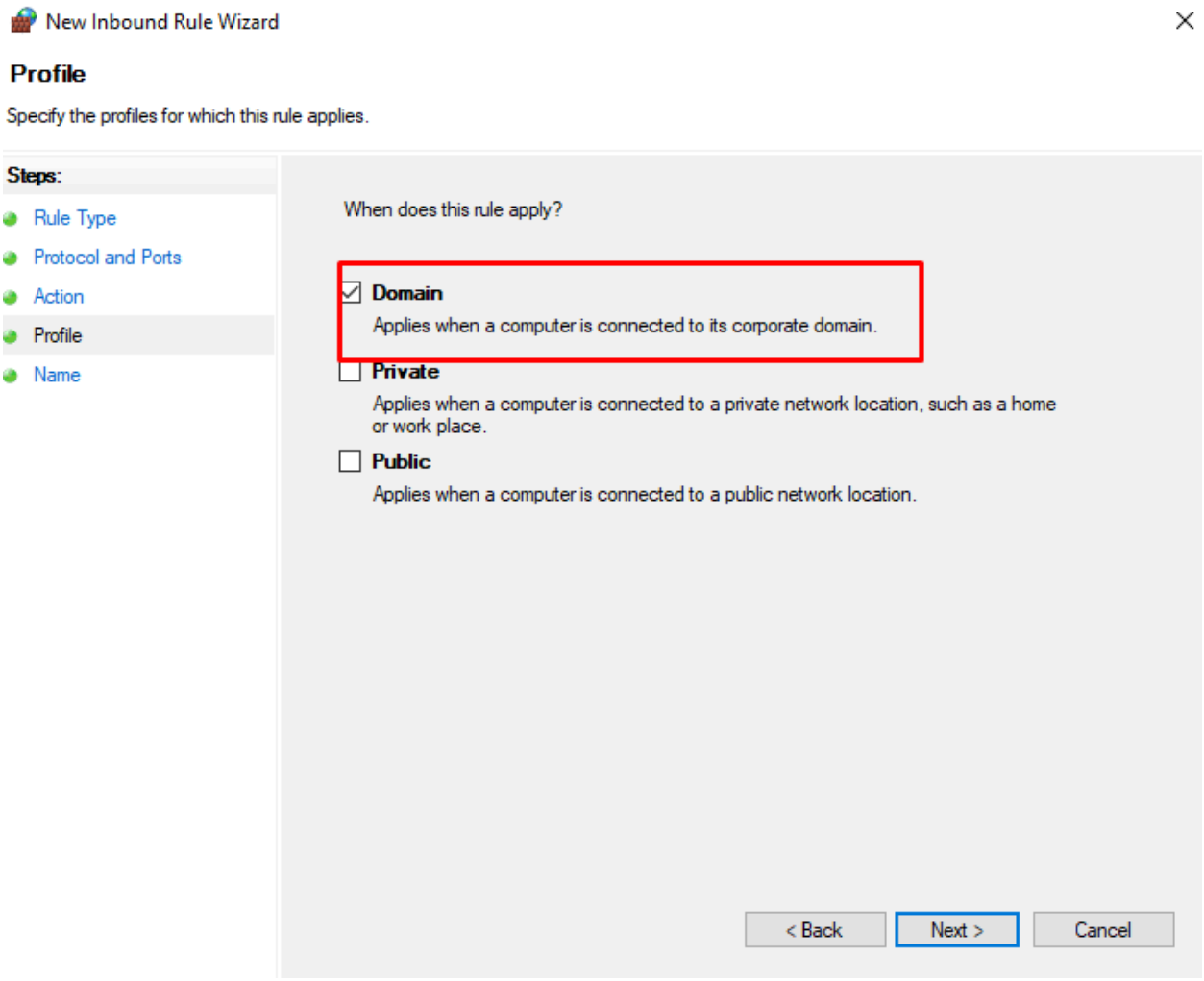

Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall witl
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Windows Defender Firewall with Advanced Security on Local Computer
Windows Defender Firewall with Advanced Security provides network security for Windows computers.
Overview
Domain Profile
Windows Defender Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Private Profile is Active
Windows Defender Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Public Profile
Windows Defender Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Windows Defender Firewall Properties
Getting Started
Authenticate communications between computers
Create connection security rules to specify how and when connections between computers are authenticated a
protected by using Internet Protocol security (IPsec).
Connection Security Rules
View and create firewall rules
Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connecti
it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connections a
blocked unless they match a rule that allows them, and outbound connections are allowed unless they match a
blocks them.
Actions
Windows Defender Firew...
Import Policy...
Export Policy...
Restore Default Policy
Diagnose / Repair
View
Refresh
Properties
Help

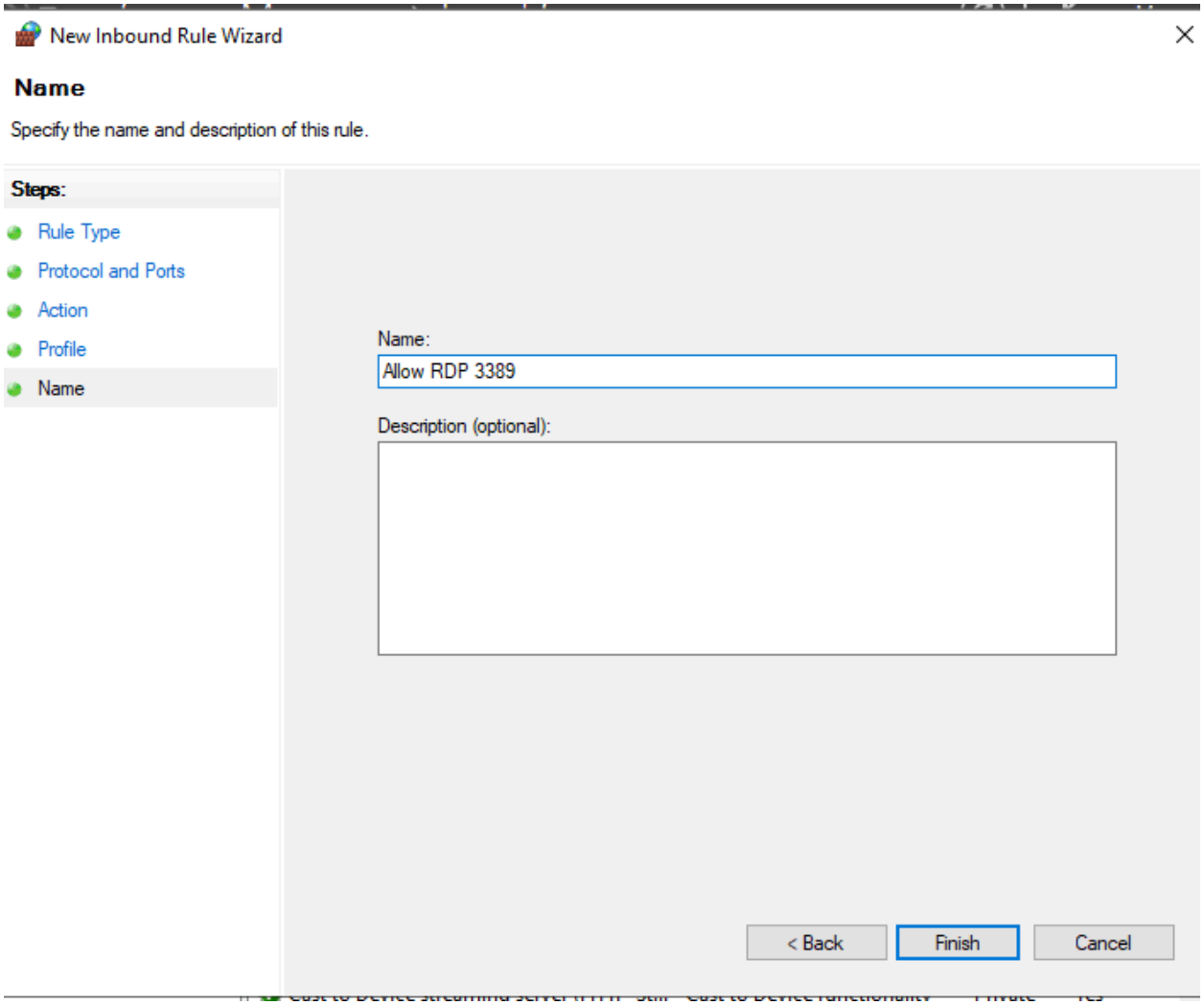

Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall witl
Inbound Rules
Outbound Rul
Connection Se
Monitoring
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
Inbound Rules
Group
Profile
Enabled
Active Directory Domain Controller (RPC)
Active Directory Domain Controller (RPC...
Active Directory Web Services (TCP-In)
AllJoyn Router (TCP-In)
AllJoyn Router (UDP-In)
BranchCache Content Retrieval (HTTP-In)
BranchCache Hosted Cache Server (HTTP...
BranchCache Peer Discovery (WSD-In)
Cast to Device functionality (qWave-TCP...
Cast to Device functionality (qWave-UDP...
Cast to Device SSDP Discovery (UDP-In)
Cast to Device streaming server (HTTP-St...
Cast to Device streaming server (RTCP-Str...
Cast to Device streaming server (RTSP-Str...
Cast to Device UPnP Events (TCP-In)
Cast to Device functionality
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
SERVICES

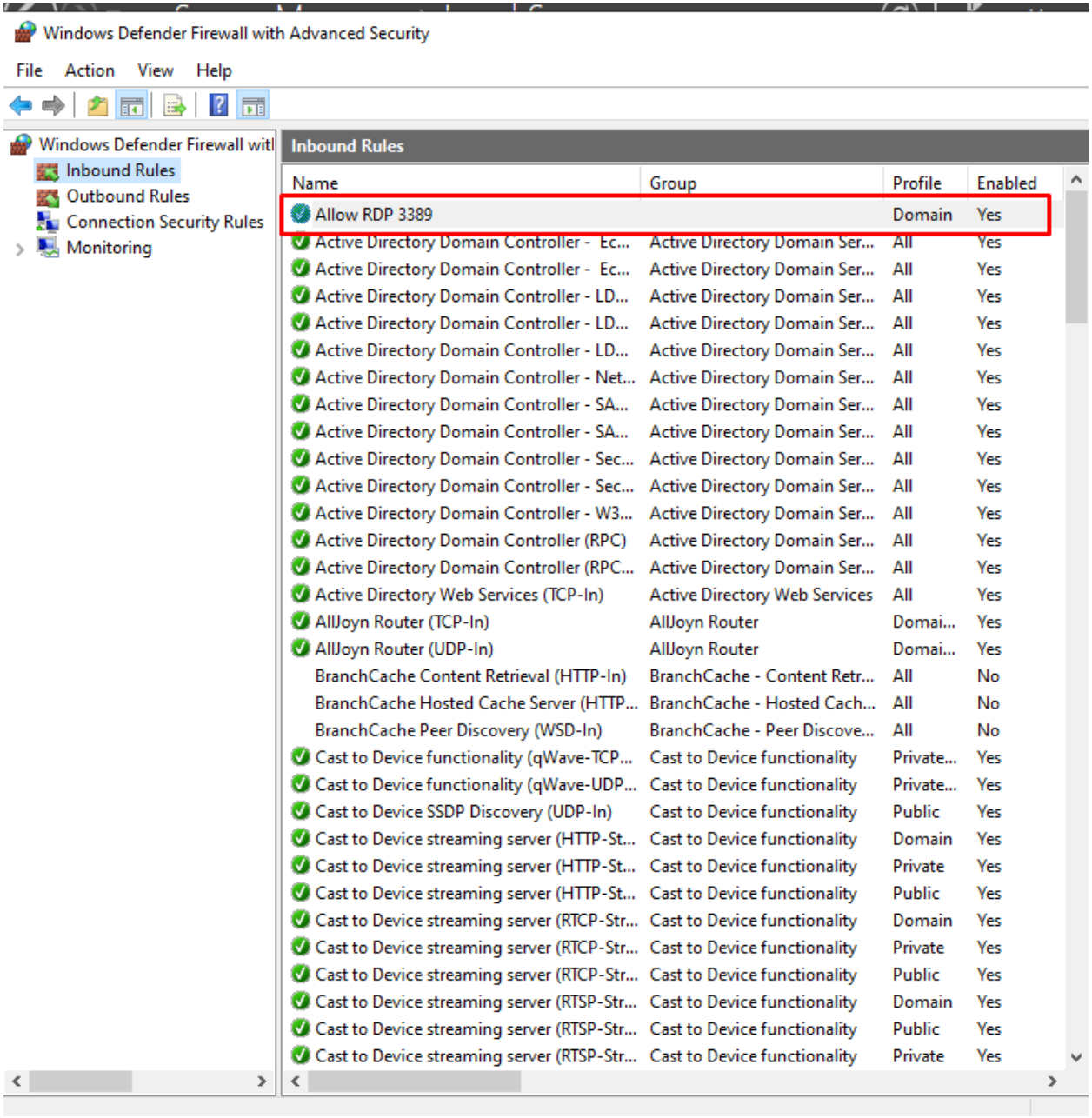

New Inbound Rule Wizard
Rule Type
Select the type of firewall rule to create.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
What type of rule would you like to create?
Program
Rule that controls connections for a program.
Port
Rule that controls connections for a TCP or UDP port.
Predefined:
Active Directory Domain Services
Rule that controls connections for a Windows experience.
Custom
Custom rule.
< Back
Next >
Cancel


New Inbound Rule Wizard
Protocol and Ports
Specify the protocols and ports to which this rule applies.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
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:
3389
Example: 80, 443, 5000-5010
< Back
Next >
Cancel

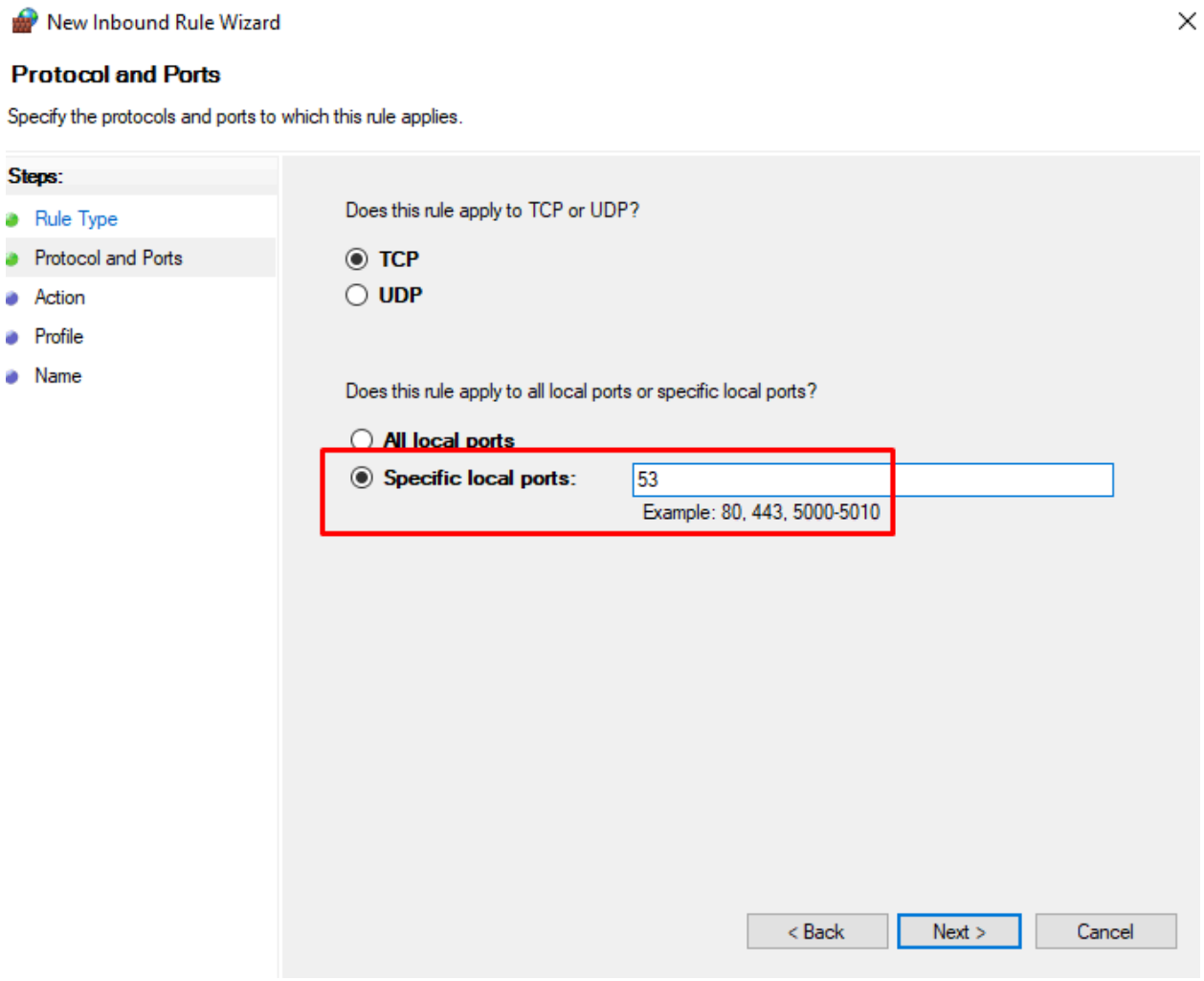

New Inbound Rule Wizard
Action
Specify the action to be taken when a connection matches the conditions specified in the rule.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
What action should be taken when a connection matches the specified conditions?
Allow the connection
This includes connections that are protected with IPsec as well as those are not.
Allow the connection if it is secure
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
Customize...
Block the connection
< Back
Next >
Cancel


New Inbound Rule Wizard
Profile
Specify the profiles for which this rule applies.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
When does this rule apply?
Domain
Applies when a computer is connected to its corporate domain.
Private
Applies when a computer is connected to a private network location, such as a home or work place.
Public
Applies when a computer is connected to a public network location.
< Back
Next >
Cancel


New Inbound Rule Wizard
Name
Specify the name and description of this rule.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
Name:
Allow RDP 3389
Description (optional):
< Back
Finish
Cancel

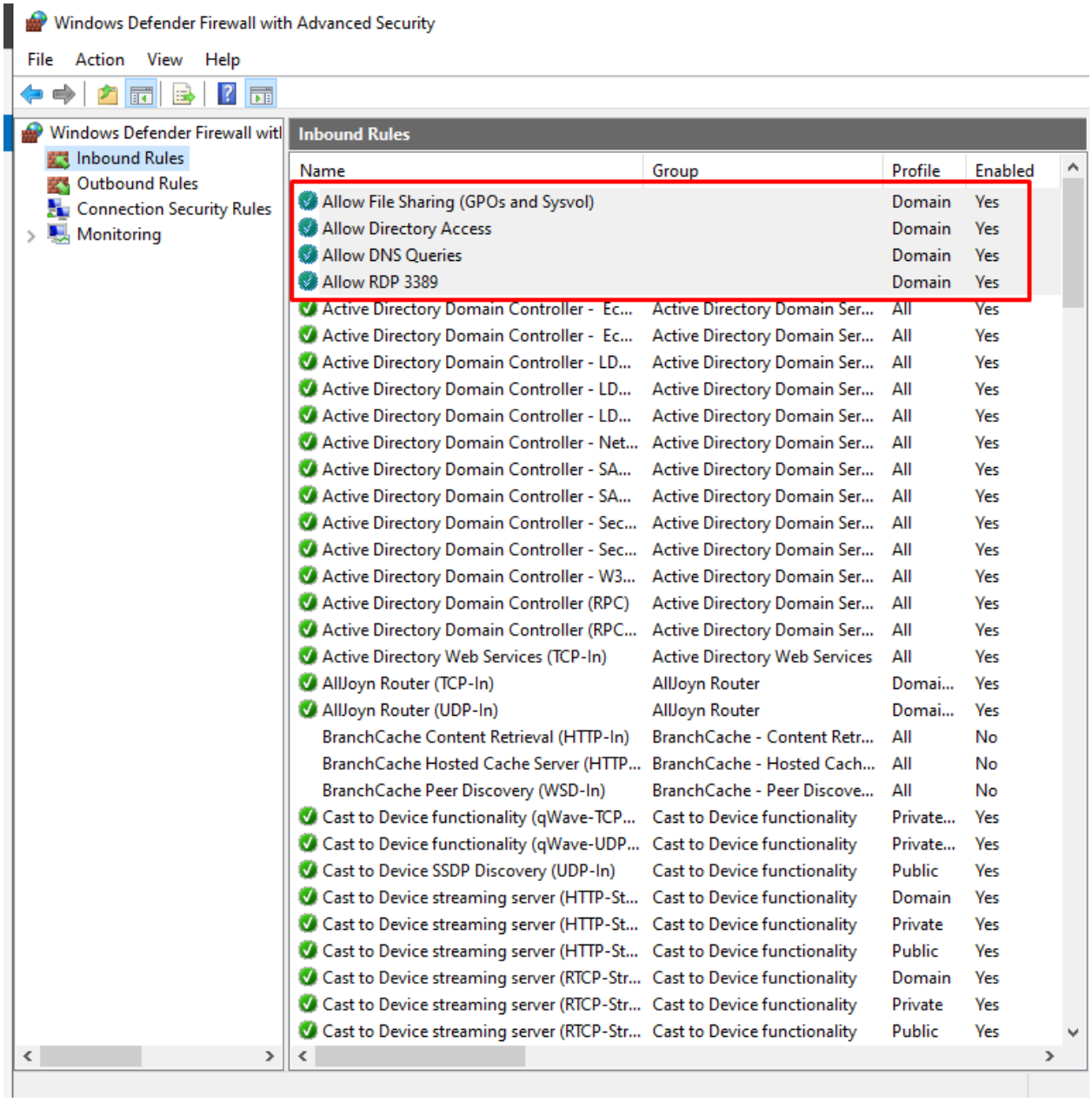


RDP 3389 successfully added to inbound rules

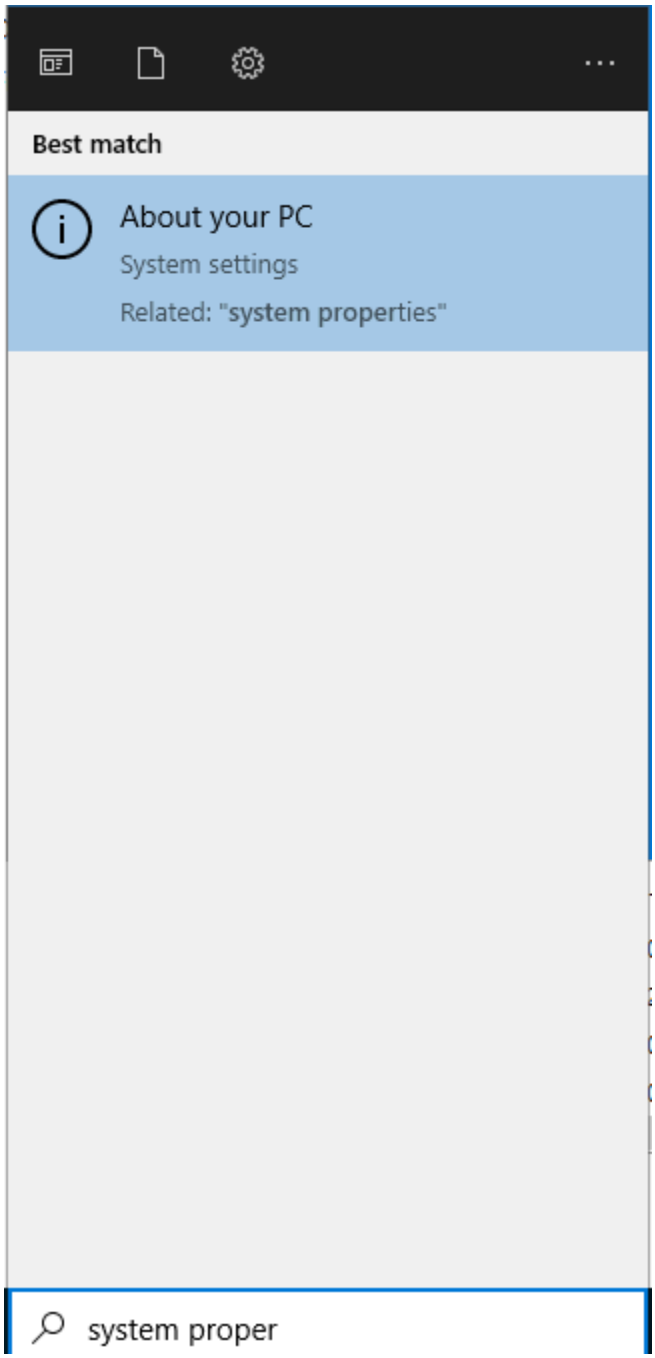


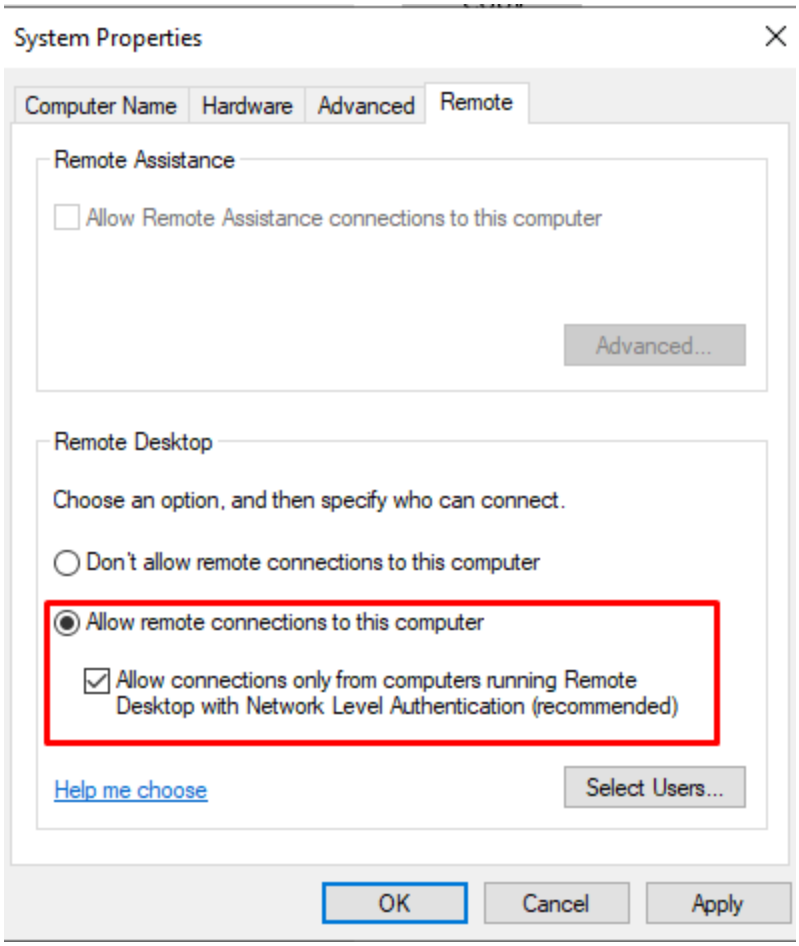
Repeat for other ports:

Rule	Port	Purpose
RDP	3389	Remote Desktop
DNS	53	DNS Queries
LDAP	389	Directory Access
SMB	445	File Sharing (GPOs and Sysvol use this)

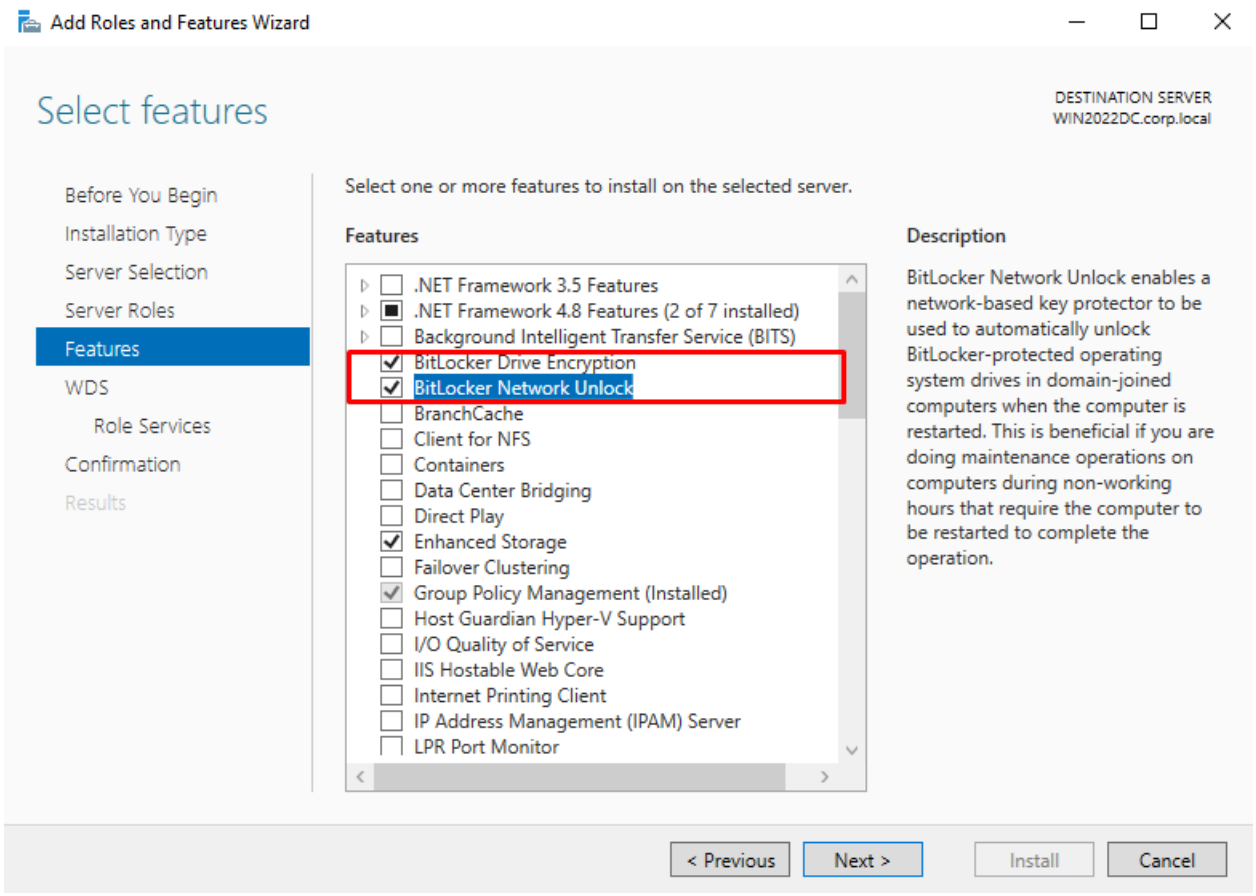

Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall witl
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name Group Profile Enabled
Allow File Sharing (GPOs and Sysvol) Domain Yes
Allow Directory Access Domain Yes
Allow DNS Queries Domain Yes
Allow RDP 3389 Domain Yes
Active Directory Domain Controller - Ec... Active Directory Domain Ser... All Yes
Active Directory Domain Controller - Ec... Active Directory Domain Ser... All Yes
Active Directory Domain Controller - LD... Active Directory Domain Ser... All Yes
Active Directory Domain Controller - LD... Active Directory Domain Ser... All Yes
Active Directory Domain Controller - LD... Active Directory Domain Ser... All Yes
Active Directory Domain Controller - Net... Active Directory Domain Ser... All Yes
Active Directory Domain Controller - SA... Active Directory Domain Ser... All Yes
Active Directory Domain Controller - SA... Active Directory Domain Ser... All Yes
Active Directory Domain Controller - Sec... Active Directory Domain Ser... All Yes
Active Directory Domain Controller - Sec... Active Directory Domain Ser... All Yes
Active Directory Domain Controller - W3... Active Directory Domain Ser... All Yes
Active Directory Domain Controller (RPC) Active Directory Domain Ser... All Yes
Active Directory Domain Controller (RPC... Active Directory Domain Ser... All Yes
Active Directory Web Services (TCP-In) Active Directory Web Services All Yes
AllJoyn Router (TCP-In) AllJoyn Router Domai... Yes
AllJoyn Router (UDP-In) AllJoyn Router Domai... Yes
BranchCache Content Retrieval (HTTP-In) BranchCache - Content Retr... All No
BranchCache Hosted Cache Server (HTTP... BranchCache - Hosted Cach... All No
BranchCache Peer Discovery (WSD-In) BranchCache - Peer Discove... All No
Cast to Device functionality (qWave-TCP... Cast to Device functionality Private... Yes
Cast to Device functionality (qWave-UDP... Cast to Device functionality Private... Yes
Cast to Device SSDP Discovery (UDP-In) Cast to Device functionality Public Yes
Cast to Device streaming server (HTTP-St... Cast to Device functionality Domain Yes
Cast to Device streaming server (HTTP-St... Cast to Device functionality Private Yes
Cast to Device streaming server (HTTP-St... Cast to Device functionality Public Yes
Cast to Device streaming server (RTCP-Str... Cast to Device functionality Domain Yes
Cast to Device streaming server (RTCP-Str... Cast to Device functionality Private Yes
Cast to Device streaming server (RTCP-Str... Cast to Device functionality Public Yes

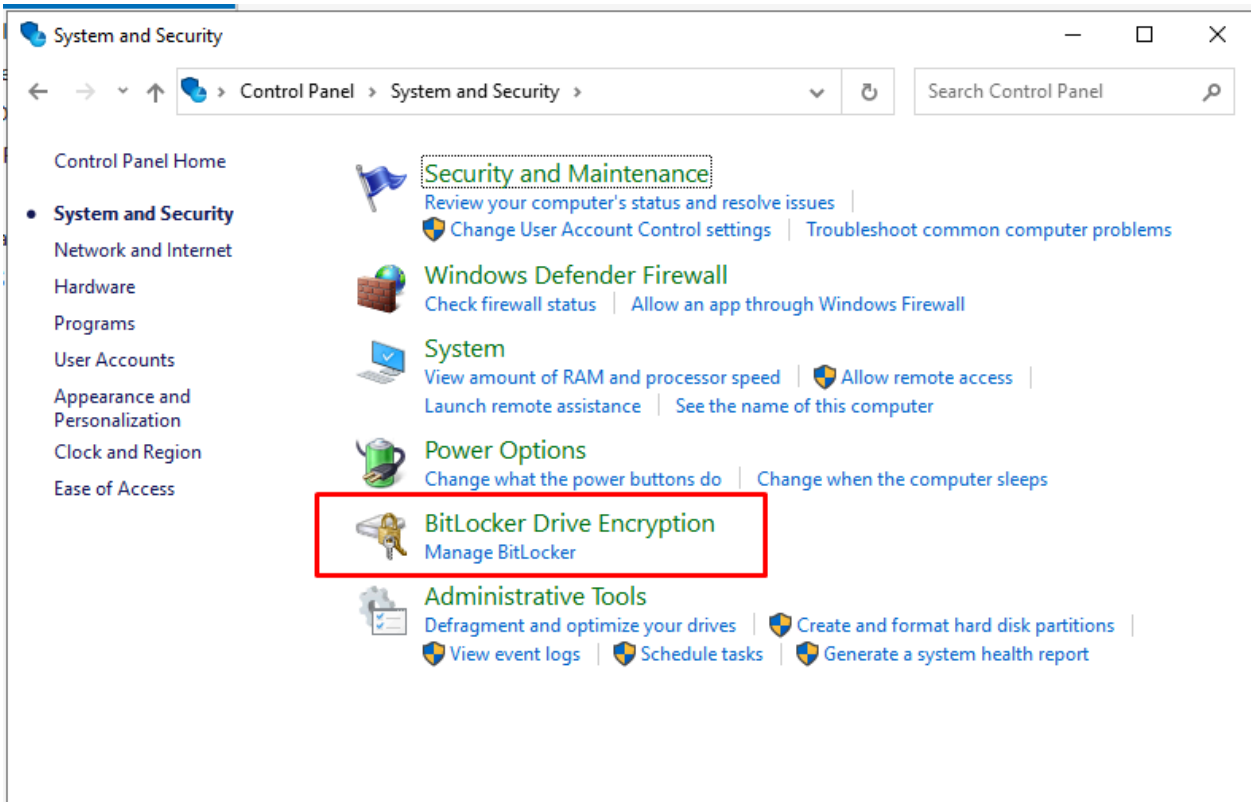
Windows Server 2022: Enable NLA (Network Level Authentication) for RDP

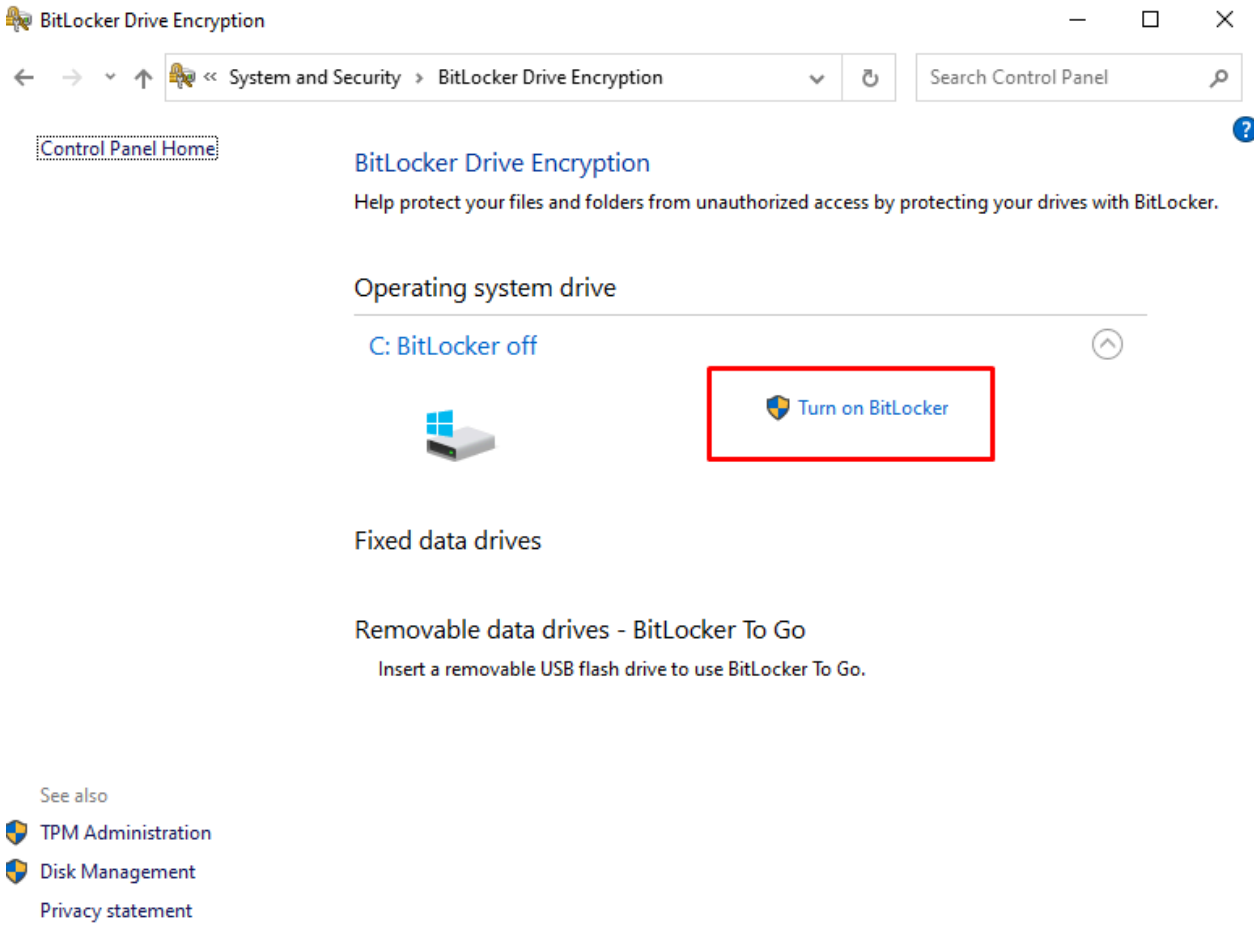


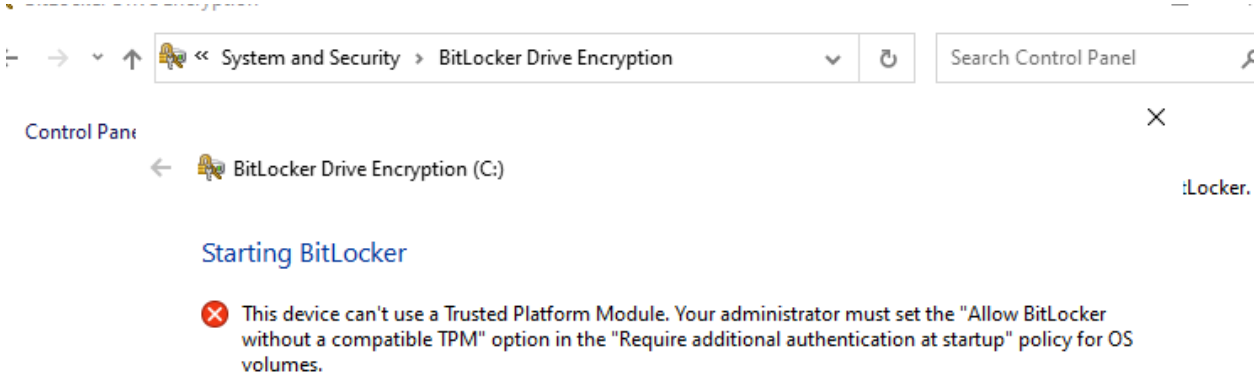

System Properties
Computer Name
Hardware
Advanced
Remote
Remote Assistance
Allow Remote Assistance connections to this computer
Advanced...
Remote Desktop
Choose an option, and then specify who can connect.
Don't allow remote connections to this computer
Allow remote connections to this computer
Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)
Help me choose
Select Users...
OK
Cancel
Apply

Windows Server 2022: Install and Enable BitLocker

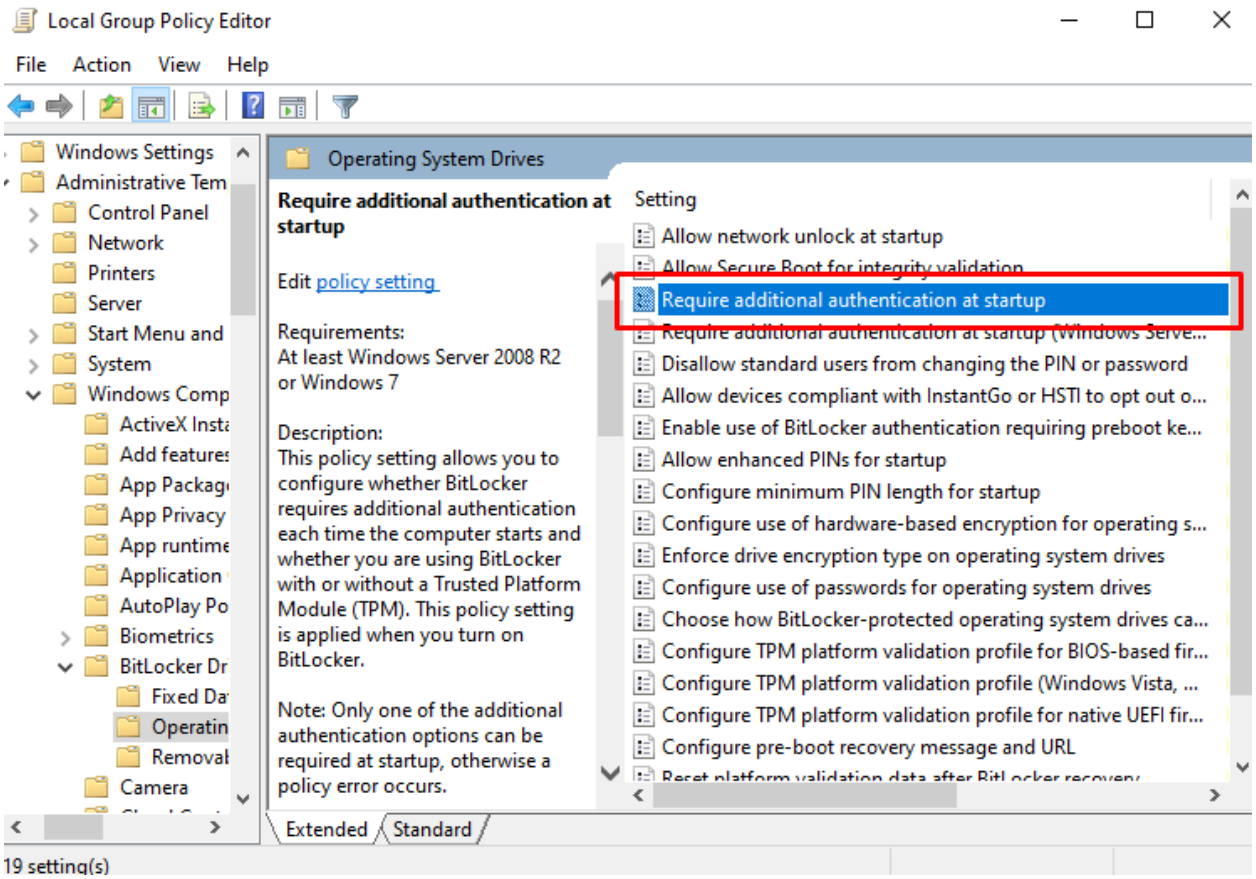


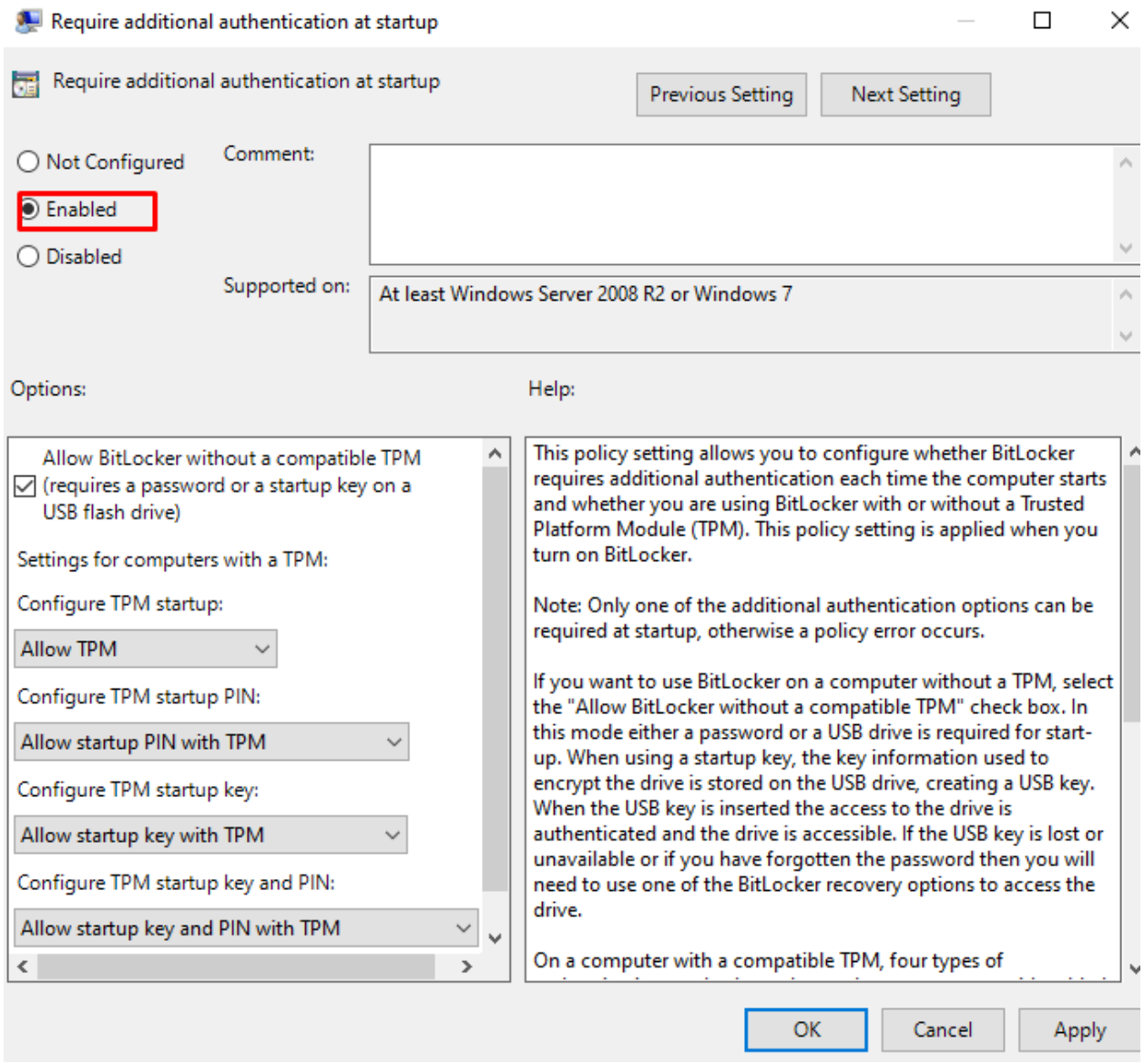

System and Security
Control Panel › System and Security ›
Search Control Panel
Control Panel Home
System and Security
Network and Internet
Hardware
Programs
User Accounts
Appearance and Personalization
Clock and Region
Ease of Access
Security and Maintenance
Review your computer's status and resolve issues
Change User Account Control settings
Troubleshoot common computer problems
Windows Defender Firewall
Check firewall status
Allow an app through Windows Firewall
System
View amount of RAM and processor speed
Allow remote access
Launch remote assistance
See the name of this computer
Power Options
Change what the power buttons do
Change when the computer sleeps
BitLocker Drive Encryption
Manage BitLocker
Administrative Tools
Defragment and optimize your drives
Create and format hard disk partitions
View event logs
Schedule tasks
Generate a system health report

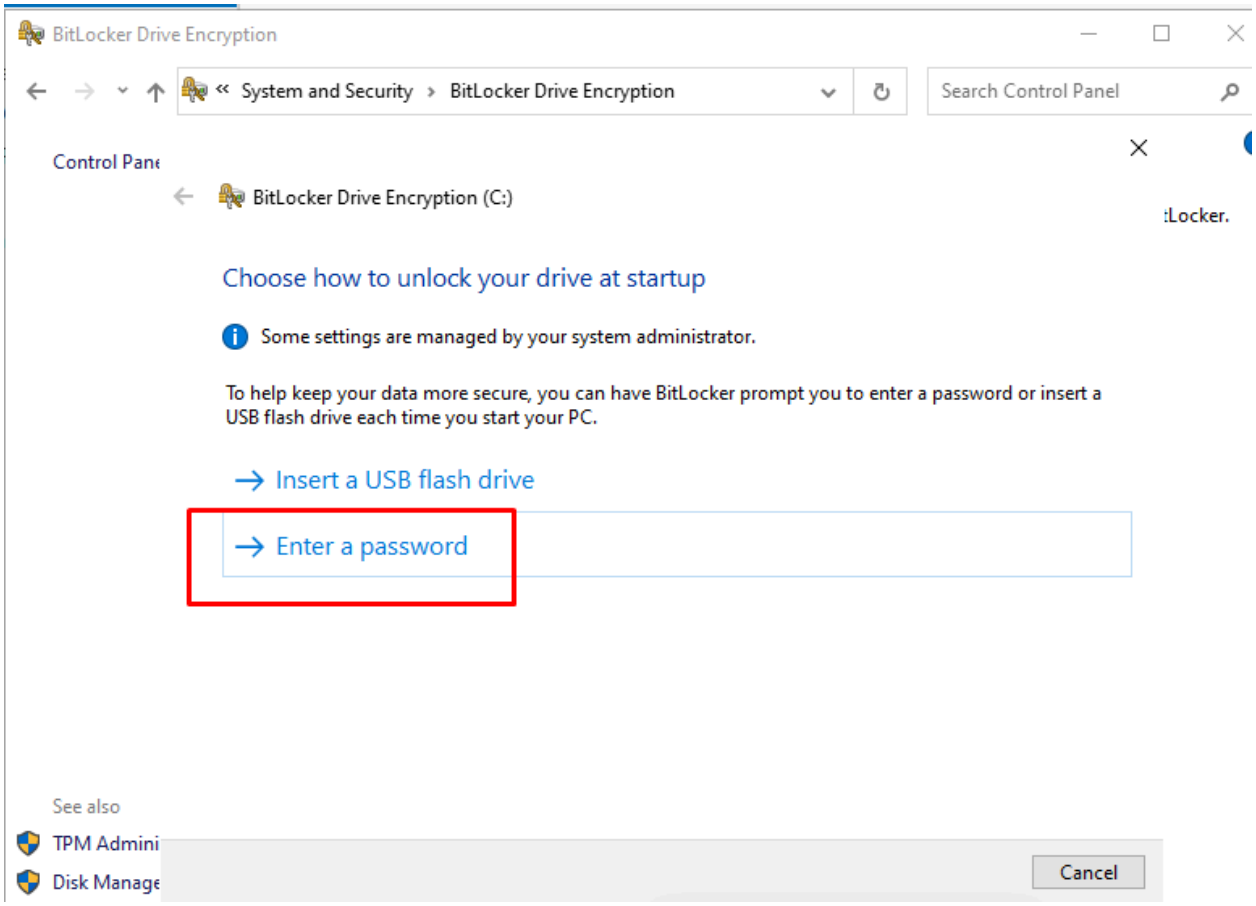

BitLocker Drive Encryption
System and Security › BitLocker Drive Encryption
Search Control Panel
Control Panel Home
BitLocker Drive Encryption
Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.
Operating system drive
C: BitLocker off
Turn on BitLocker
Fixed data drives
Removable data drives - BitLocker To Go
Insert a removable USB flash drive to use BitLocker To Go.
See also
TPM Administration
Disk Management
Privacy statement

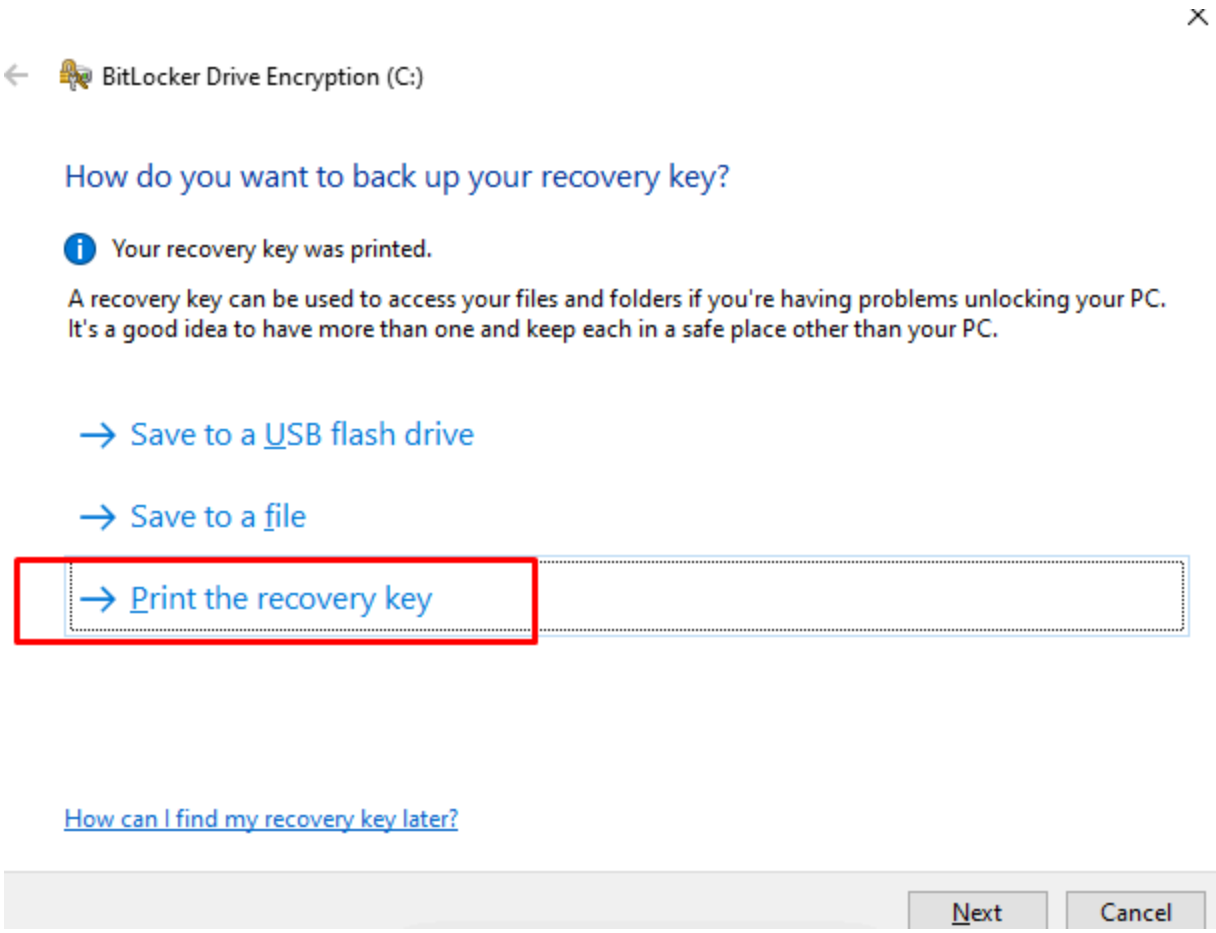

System and Security › BitLocker Drive Encryption
Search Control Panel
Control Pane
BitLocker Drive Encryption (C:)
:Locker.
Starting BitLocker
This device can't use a Trusted Platform Module. Your administrator must set the "Allow BitLocker without a compatible TPM" option in the "Require additional authentication at startup" policy for OS volumes.

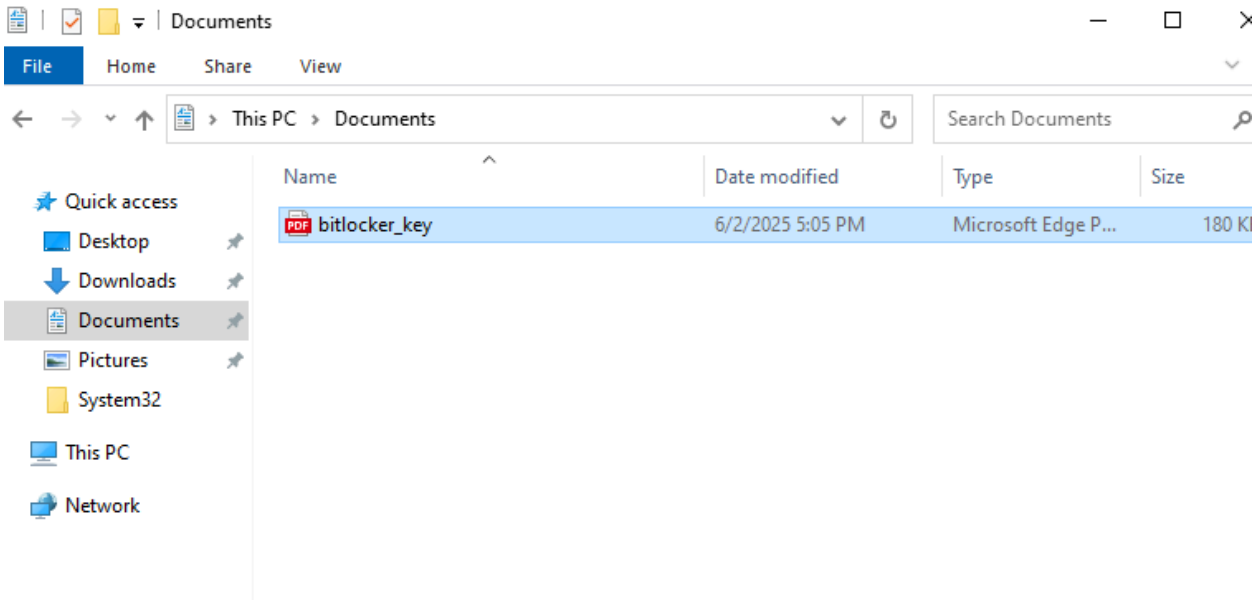
TO fix:


Local Group Policy Editor
File Action View Help
Windows Settings
Administrative Tem
Control Panel
Network
Printers
Server
Start Menu and
System
Windows Comp
ActiveX Insta
Add features
App Packag
App Privacy
App runtime
Application
AutoPlay Po
Biometrics
BitLocker Dr
Fixed Da
Operatin
Removal
Camera
Operating System Drives
Require additional authentication at startup
Edit policy setting
Requirements:
At least Windows Server 2008 R2 or Windows 7
Description:
This policy setting allows you to configure whether BitLocker requires additional authentication each time the computer starts and whether you are using BitLocker with or without a Trusted Platform Module (TPM). This policy setting is applied when you turn on BitLocker.
Note: Only one of the additional authentication options can be required at startup, otherwise a policy error occurs.
Setting
Allow network unlock at startup
Require additional authentication at startup
Disallow standard users from changing the PIN or password
Allow devices compliant with InstantGo or HSTI to opt out o...
Enable use of BitLocker authentication requiring preboot ke...
Allow enhanced PINs for startup
Configure minimum PIN length for startup
Configure use of hardware-based encryption for operating s...
Enforce drive encryption type on operating system drives
Configure use of passwords for operating system drives
Choose how BitLocker-protected operating system drives ca...
Configure TPM platform validation profile for BIOS-based fir...
Configure TPM platform validation profile (Windows Vista, ...
Configure TPM platform validation profile for native UEFI fir...
Configure pre-boot recovery message and URL
Extended
Standard
19 setting(s)


Require additional authentication at startup
Require additional authentication at startup
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Windows Server 2008 R2 or Windows 7
Options:
Help:
Allow BitLocker without a compatible TPM (requires a password or a startup key on a USB flash drive)
Settings for computers with a TPM:
Configure TPM startup:
Allow TPM
Configure TPM startup PIN:
Allow startup PIN with TPM
Configure TPM startup key:
Allow startup key with TPM
Configure TPM startup key and PIN:
Allow startup key and PIN with TPM
This policy setting allows you to configure whether BitLocker requires additional authentication each time the computer starts and whether you are using BitLocker with or without a Trusted Platform Module (TPM). This policy setting is applied when you turn on BitLocker.
Note: Only one of the additional authentication options can be required at startup, otherwise a policy error occurs.
If you want to use BitLocker on a computer without a TPM, select the "Allow BitLocker without a compatible TPM" check box. In this mode either a password or a USB drive is required for start-up. When using a startup key, the key information used to encrypt the drive is stored on the USB drive, creating a USB key. When the USB key is inserted the access to the drive is authenticated and the drive is accessible. If the USB key is lost or unavailable or if you have forgotten the password then you will need to use one of the BitLocker recovery options to access the drive.
On a computer with a compatible TPM, four types of
OK
Cancel
Apply

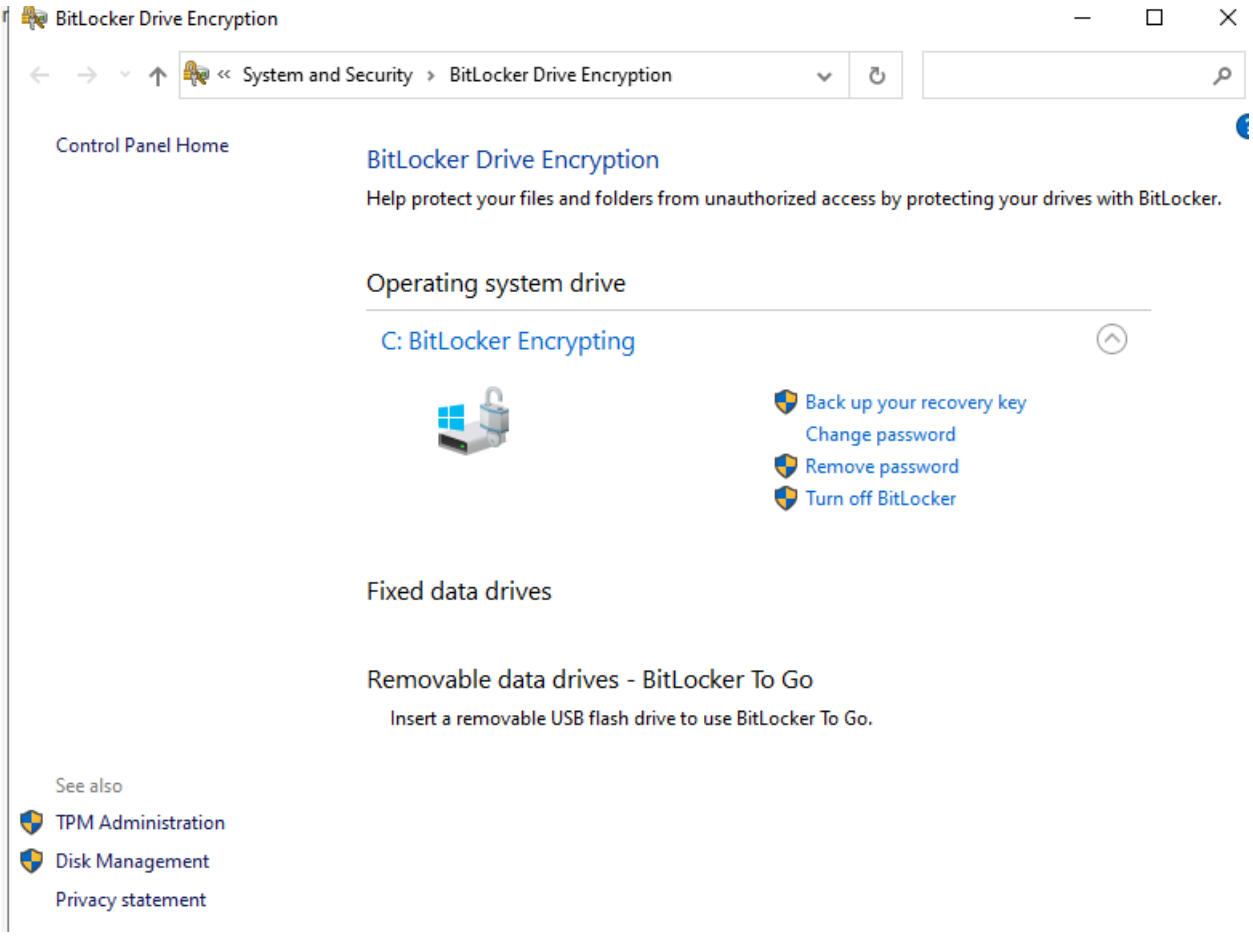

BitLocker Drive Encryption
System and Security › BitLocker Drive Encryption
Search Control Panel
Control Pane
BitLocker Drive Encryption (C:)
:Locker.
Choose how to unlock your drive at startup
Some settings are managed by your system administrator.
To help keep your data more secure, you can have BitLocker prompt you to enter a password or insert a USB flash drive each time you start your PC.
Insert a USB flash drive
Enter a password
See also
TPM Admini
Disk Manage
Cancel


BitLocker Drive Encryption (C:)
How do you want to back up your recovery key?
Your recovery key was printed.
A recovery key can be used to access your files and folders if you're having problems unlocking your PC. It's a good idea to have more than one and keep each in a safe place other than your PC.
Save to a USB flash drive
Save to a file
Print the recovery key
How can I find my recovery key later?
Next
Cancel


Documents
File
Home
Share
View
This PC
Documents
Search Documents
Quick access
Desktop
Downloads
Documents
Pictures
System32
This PC
Network
Name
Date modified
Type
Size
bitlocker_key
6/2/2025 5:05 PM
Microsoft Edge P...
180 KI

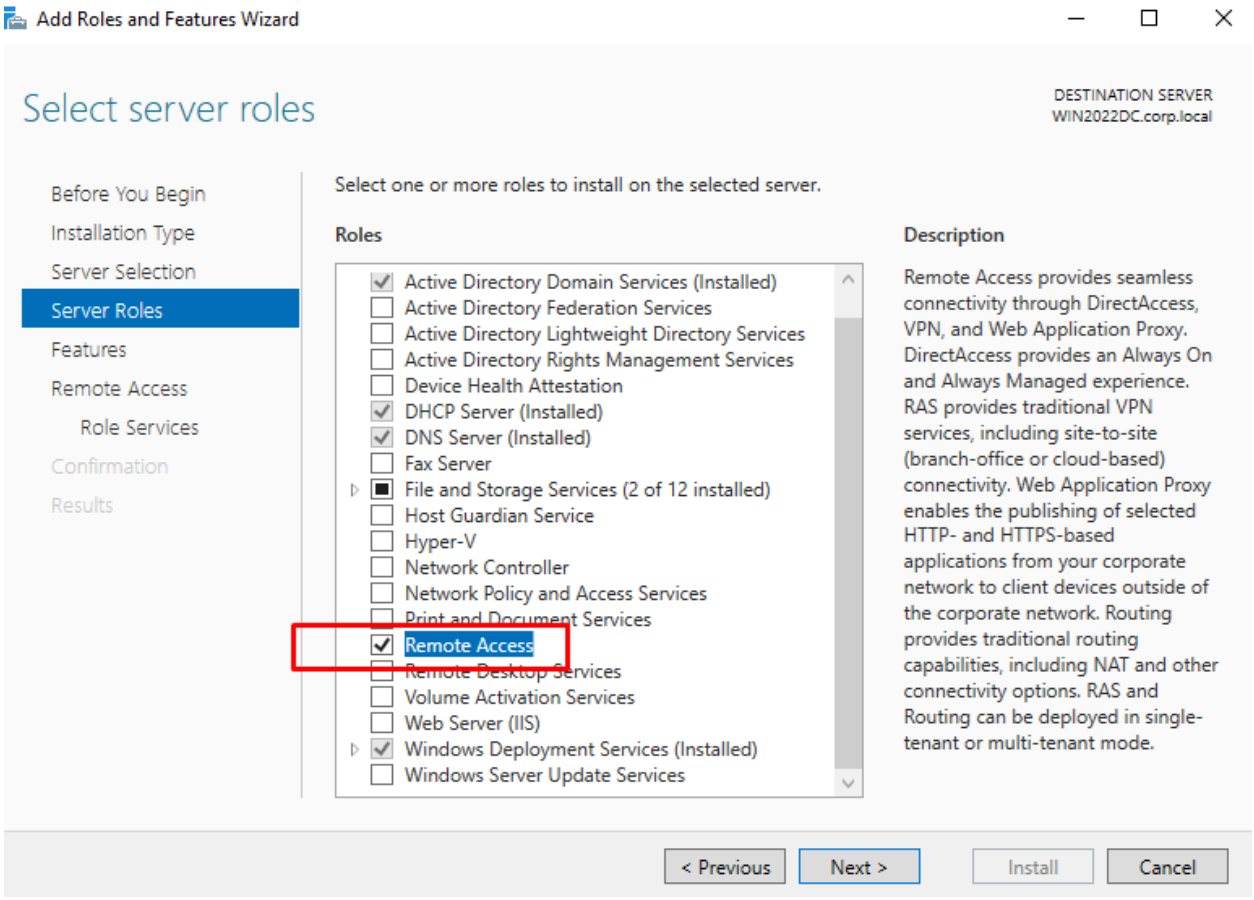

BitLocker Drive Encryption Notification Utility
Encryption will begin after computer restart
Encryption of C: by BitLocker Drive Encryption will begin after this computer is restarted. Click for more information and to restart Windows.

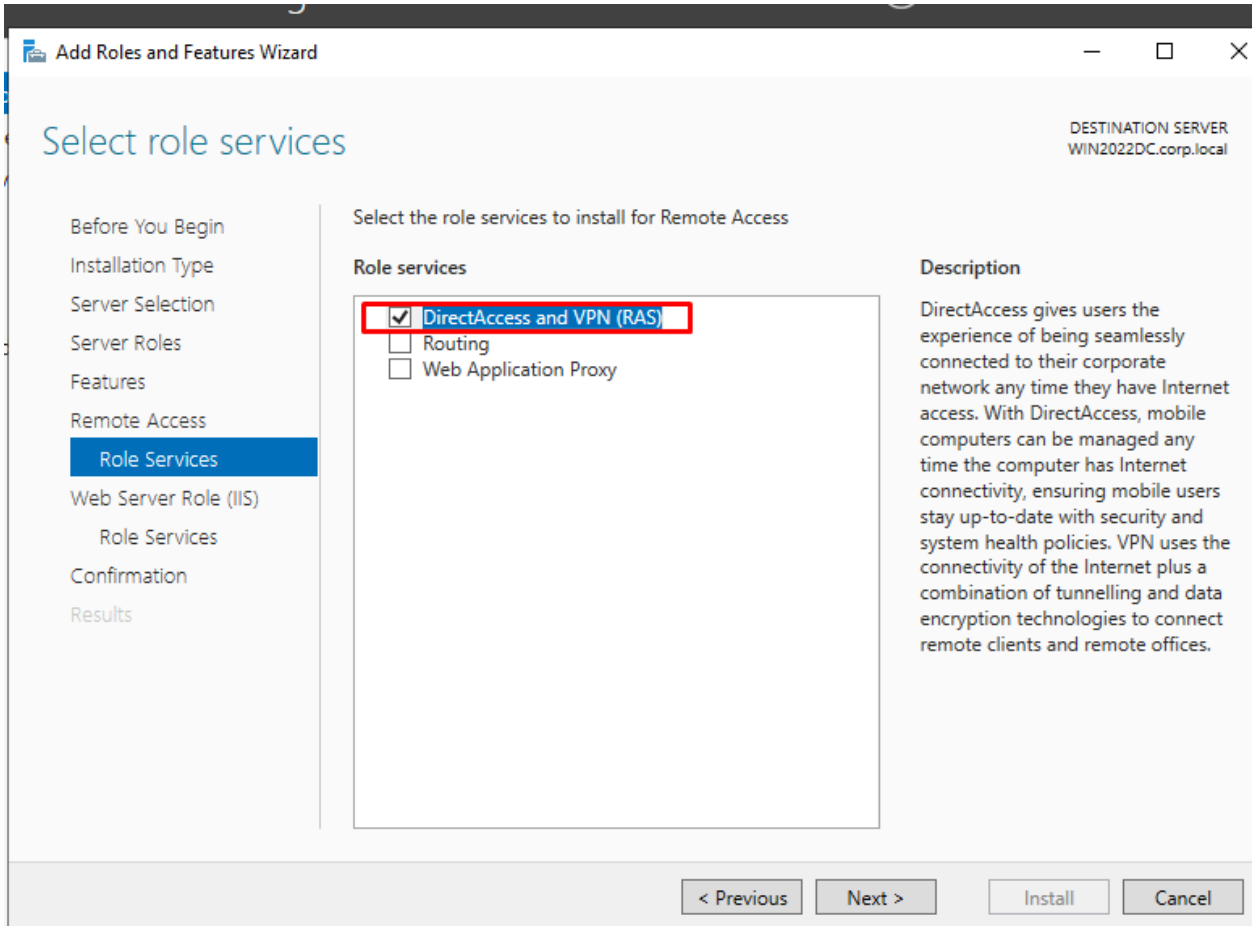

Home
Windows Server 2022
BitLocker drive encryption
Enter the password to unlock this drive
[********
]
Press the Insert key to see the password as you type.

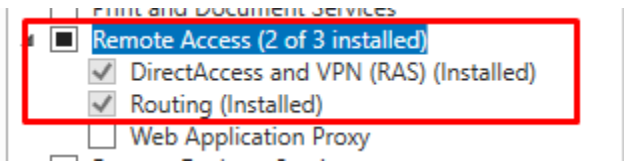


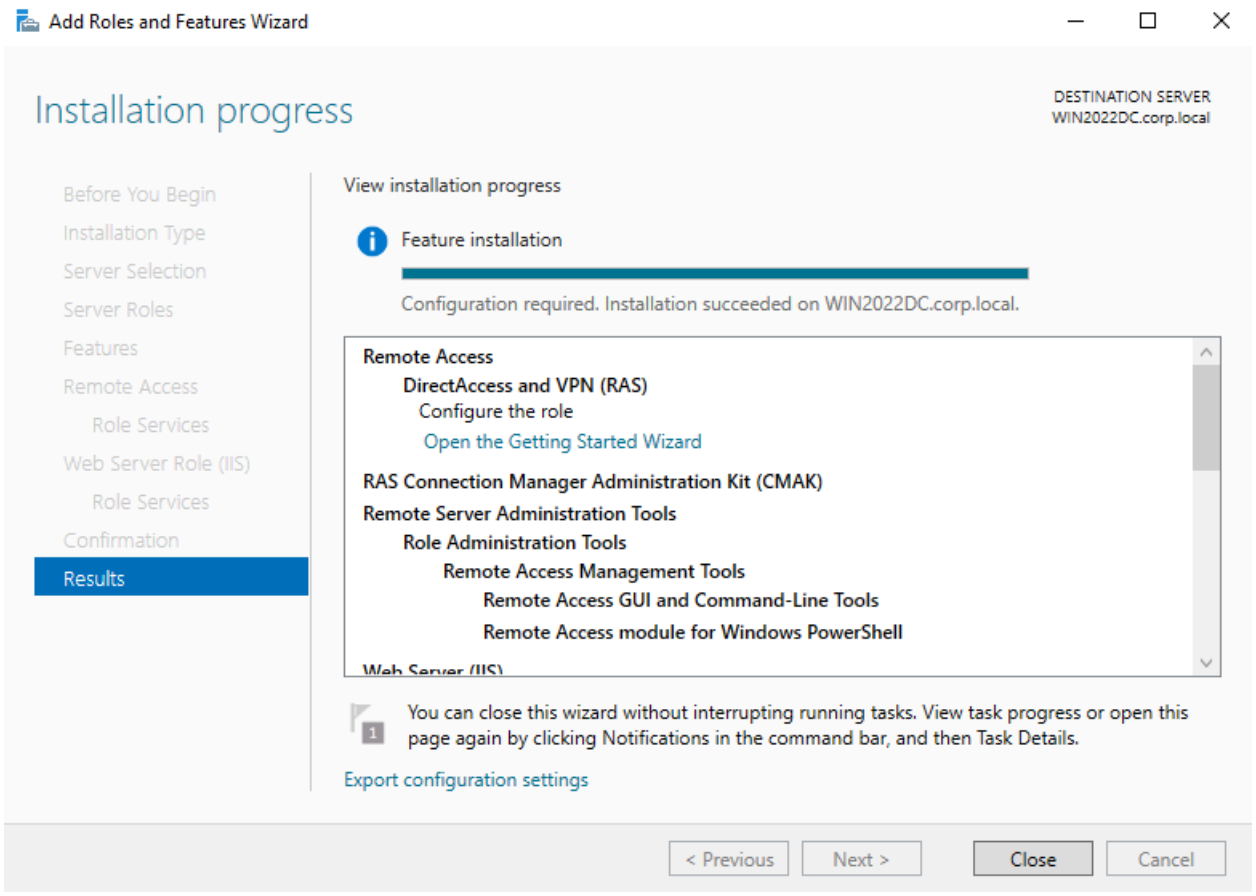
Bitlocker successfully enabled

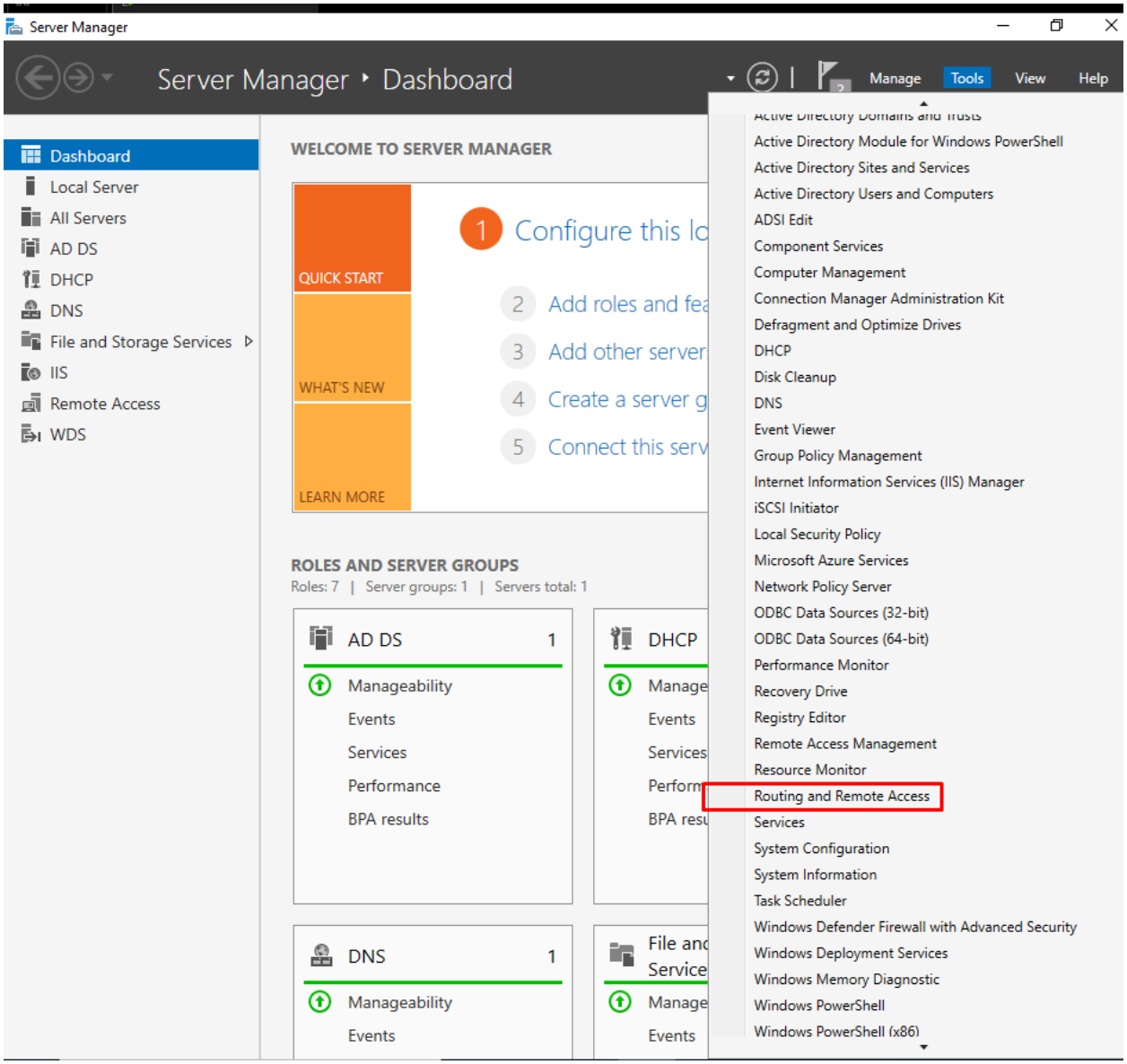
Windows Server 2022: Install and use Remote Access

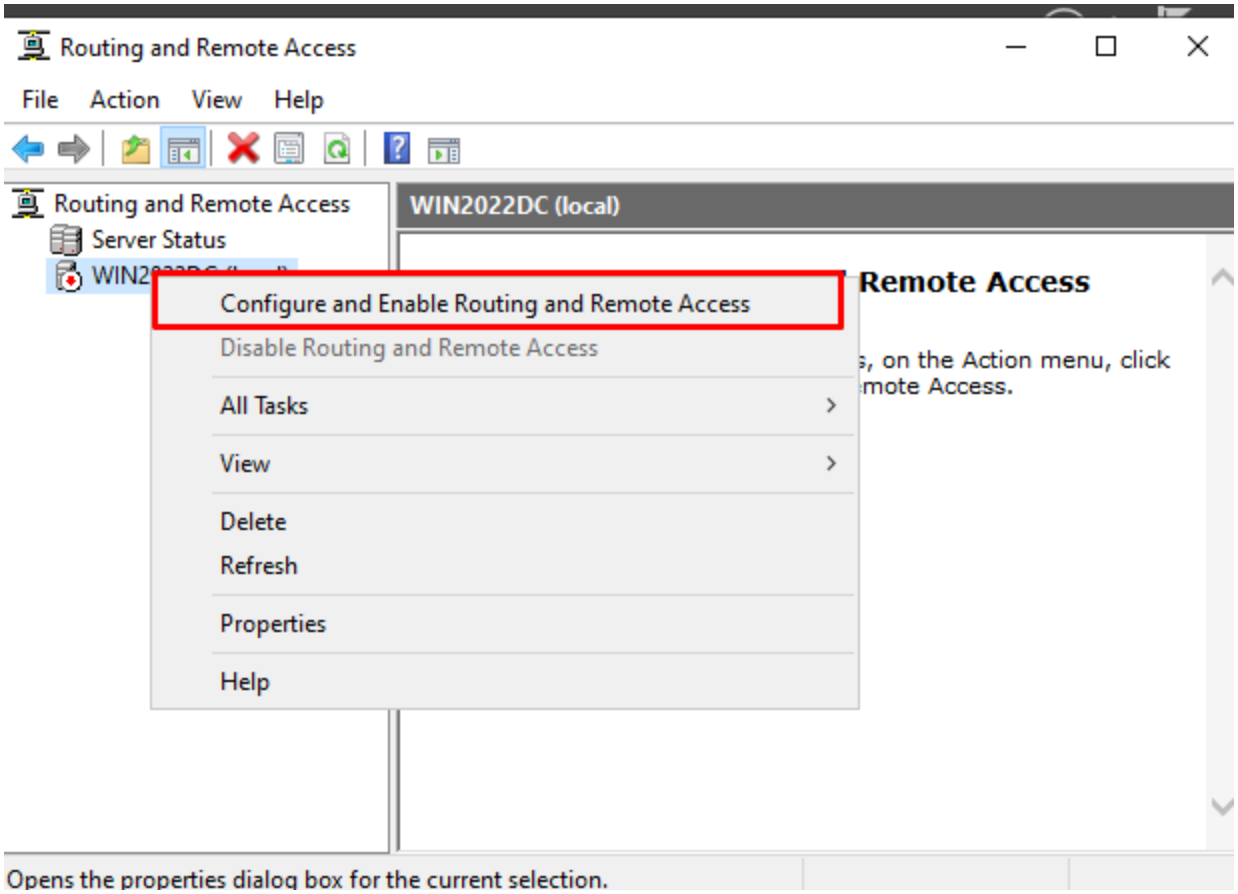


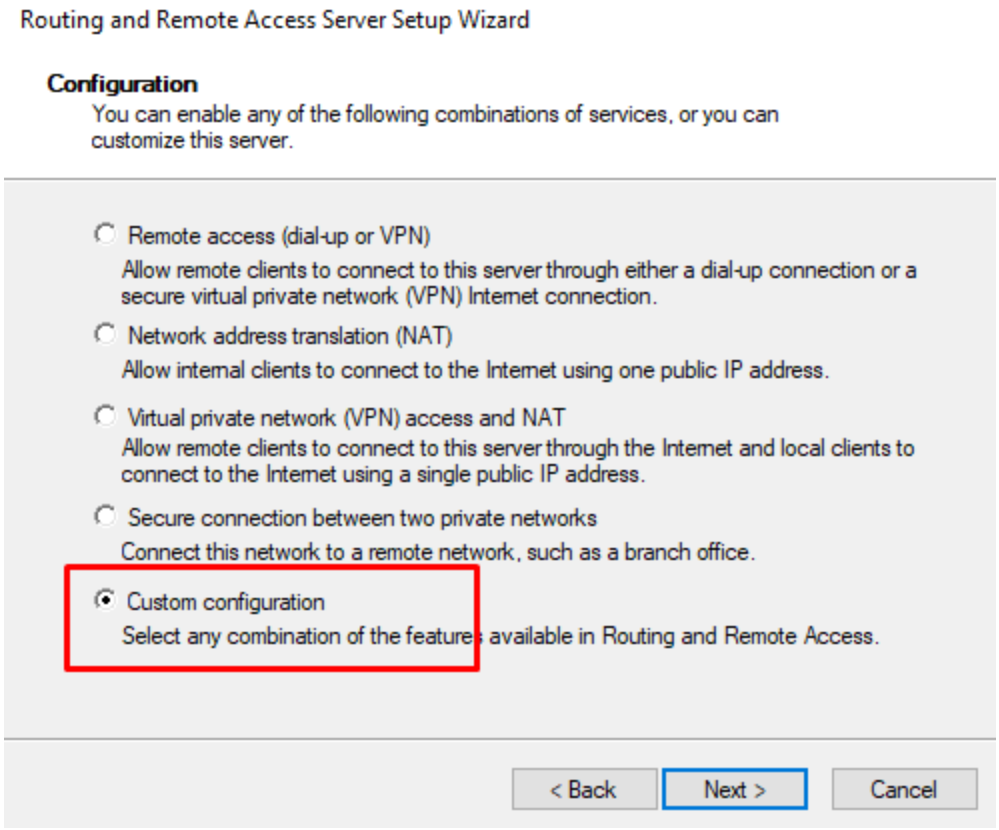

Add Roles and Features Wizard
Select role services
DESTINATION SERVER
WIN2022DC.corp.local
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Remote Access
Role Services
Web Server Role (IIS)
Role Services
Confirmation
Results
Select the role services to install for Remote Access
Role services
DirectAccess and VPN (RAS)
Routing
Web Application Proxy
Description
DirectAccess gives users the experience of being seamlessly connected to their corporate network any time they have Internet access. With DirectAccess, mobile computers can be managed any time the computer has Internet connectivity, ensuring mobile users stay up-to-date with security and system health policies. VPN uses the connectivity of the Internet plus a combination of tunnelling and data encryption technologies to connect remote clients and remote offices.
< Previous
Next >
Install
Cancel

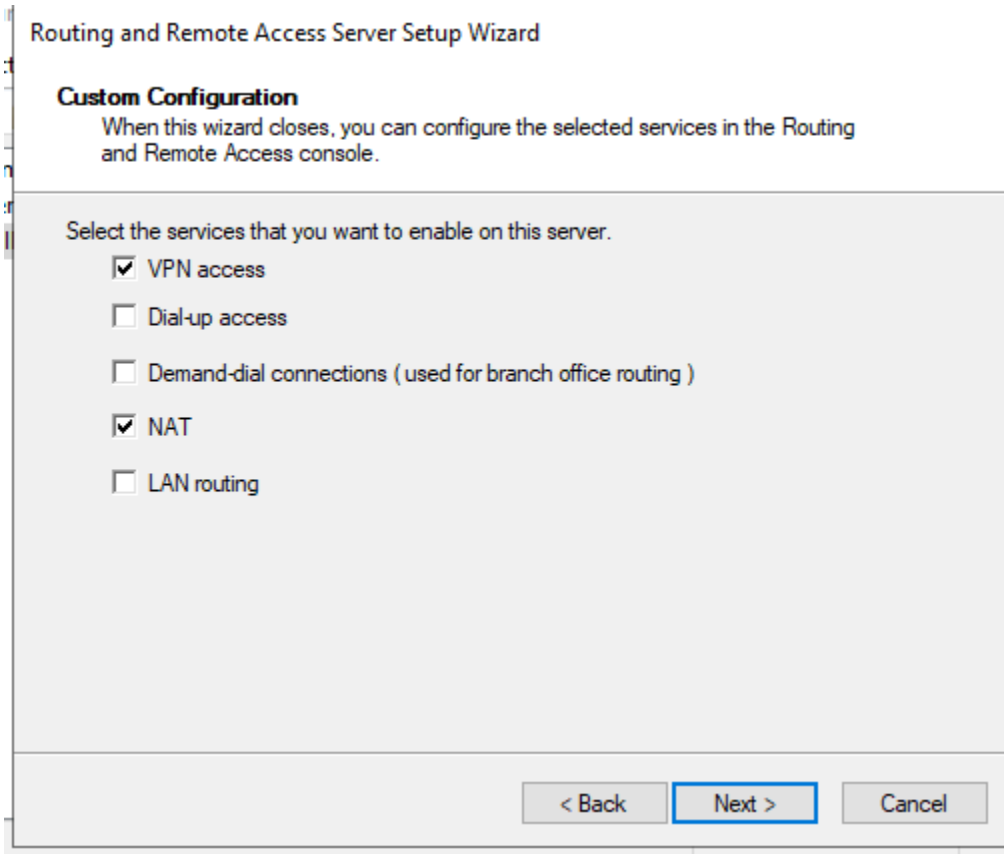

Remote Access (2 of 3 installed)
DirectAccess and VPN (RAS) (Installed)
Routing (Installed)
Web Application Proxy


Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
WIN2022DC.corp.local
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Remote Access
Role Services
Web Server Role (IIS)
Role Services
Confirmation
Results
View installation progress
Feature installation
Configuration required. Installation succeeded on WIN2022DC.corp.local.
Remote Access
DirectAccess and VPN (RAS)
Configure the role
Open the Getting Started Wizard
RAS Connection Manager Administration Kit (CMAK)
Remote Server Administration Tools
Role Administration Tools
Remote Access Management Tools
Remote Access GUI and Command-Line Tools
Remote Access module for Windows PowerShell
Web Server (IIS)
You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.
Export configuration settings
< Previous
Next >
Close
Cancel

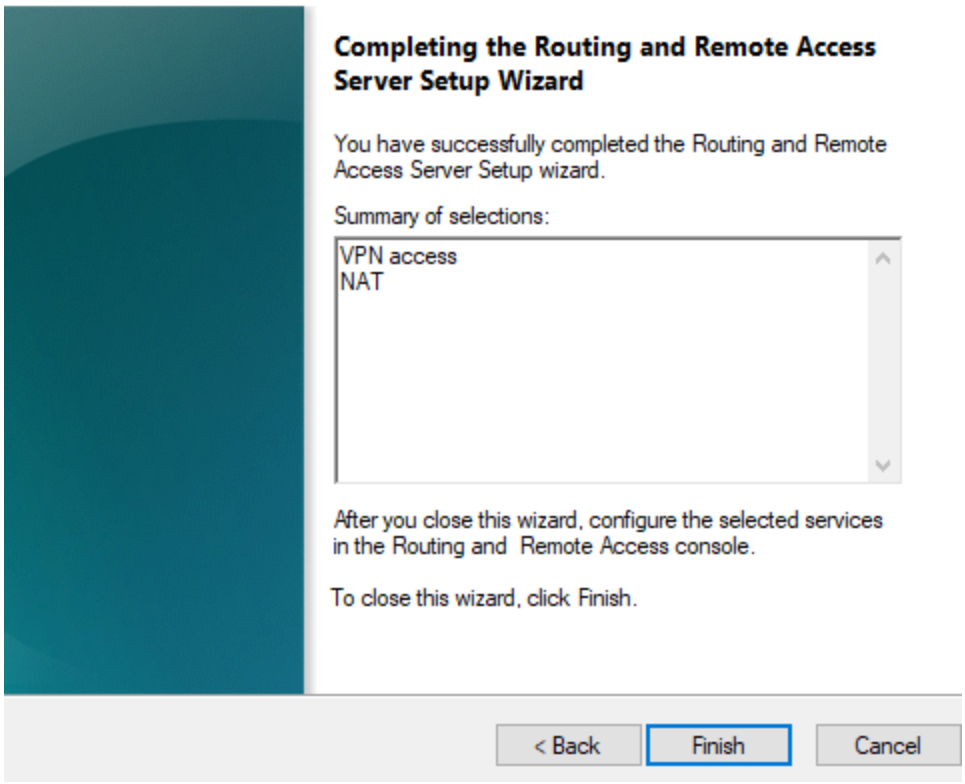

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
DHCP
DNS
File and Storage Services
IIS
Remote Access
WDS
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this lo
2 Add roles and fea
3 Add other server
4 Create a server g
5 Connect this serv
ROLES AND SERVER GROUPS
Roles: 7 | Server groups: 1 | Servers total: 1
AD DS 1
Manageability
Events
Services
Performance
BPA results
DHCP
Manage
Events
Services
Perform
BPA resu
DNS 1
Manageability
Events
File and
Service
Manage
Events
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Connection Manager Administration Kit
Defragment and Optimize Drives
DHCP
Disk Cleanup
DNS
Event Viewer
Group Policy Management
Internet Information Services (IIS) Manager
iSCSI Initiator
Local Security Policy
Microsoft Azure Services
Network Policy Server
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Recovery Drive
Registry Editor
Remote Access Management
Resource Monitor
Routing and Remote Access
Services
System Configuration
System Information
Task Scheduler
Windows Defender Firewall with Advanced Security
Windows Deployment Services
Windows Memory Diagnostic
Windows PowerShell
Windows PowerShell (x86)


Routing and Remote Access
File
Action
View
Help
Routing and Remote Access
Server Status
WIN2022DC (local)
Remote Access
Configure and Enable Routing and Remote Access
Disable Routing and Remote Access
All Tasks
View
Delete
Refresh
Properties
Help
Opens the properties dialog box for the current selection.

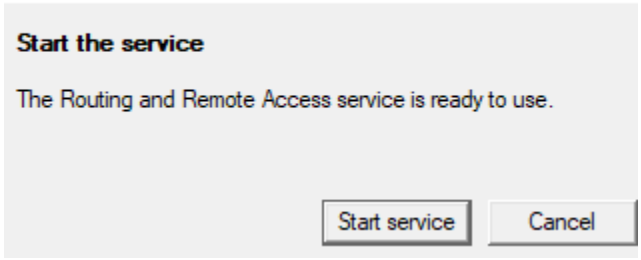

Routing and Remote Access Server Setup Wizard
Configuration
You can enable any of the following combinations of services, or you can customize this server.
Remote access (dial-up or VPN)
Allow remote clients to connect to this server through either a dial-up connection or a secure virtual private network (VPN) Internet connection.
Network address translation (NAT)
Allow internal clients to connect to the Internet using one public IP address.
Virtual private network (VPN) access and NAT
Allow remote clients to connect to this server through the Internet and local clients to connect to the Internet using a single public IP address.
Secure connection between two private networks
Connect this network to a remote network, such as a branch office.
Custom configuration
Select any combination of the features available in Routing and Remote Access.
< Back
Next >
Cancel

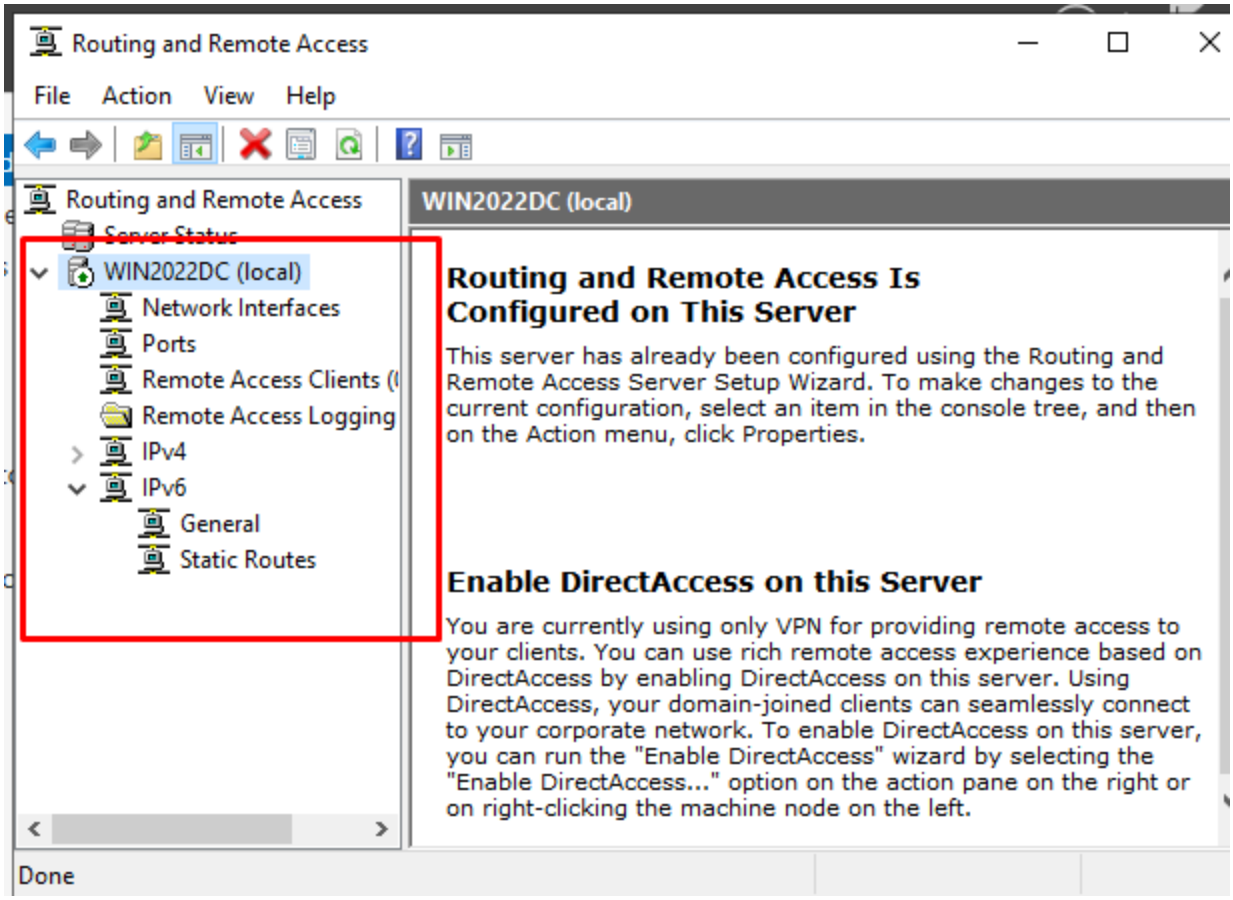

Routing and Remote Access Server Setup Wizard
Custom Configuration
When this wizard closes, you can configure the selected services in the Routing and Remote Access console.
Select the services that you want to enable on this server.
VPN access
Dial-up access
Demand-dial connections (used for branch office routing)
NAT
LAN routing
< Back
Next >
Cancel

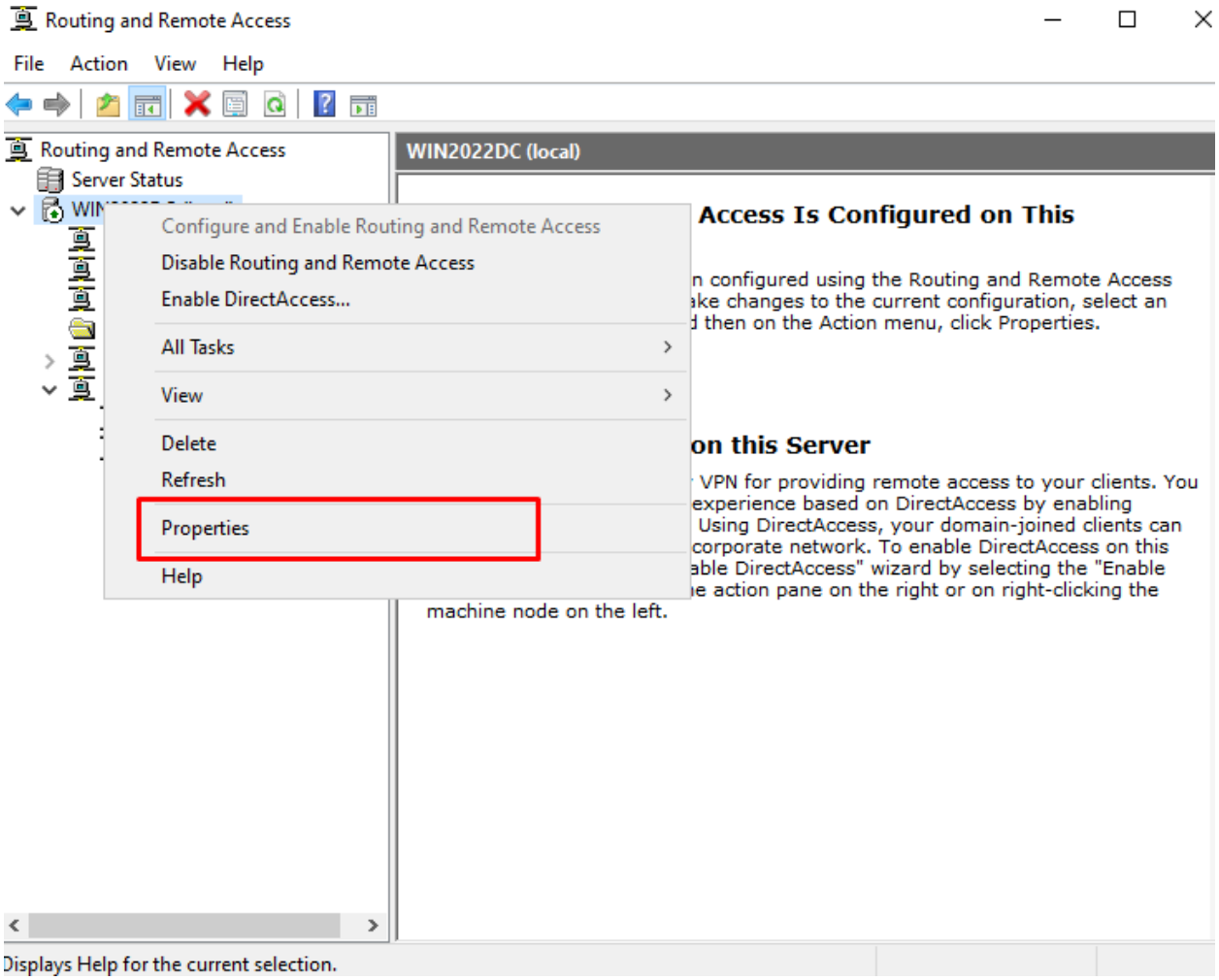
Routing and Remote Access Server Setup Wizard

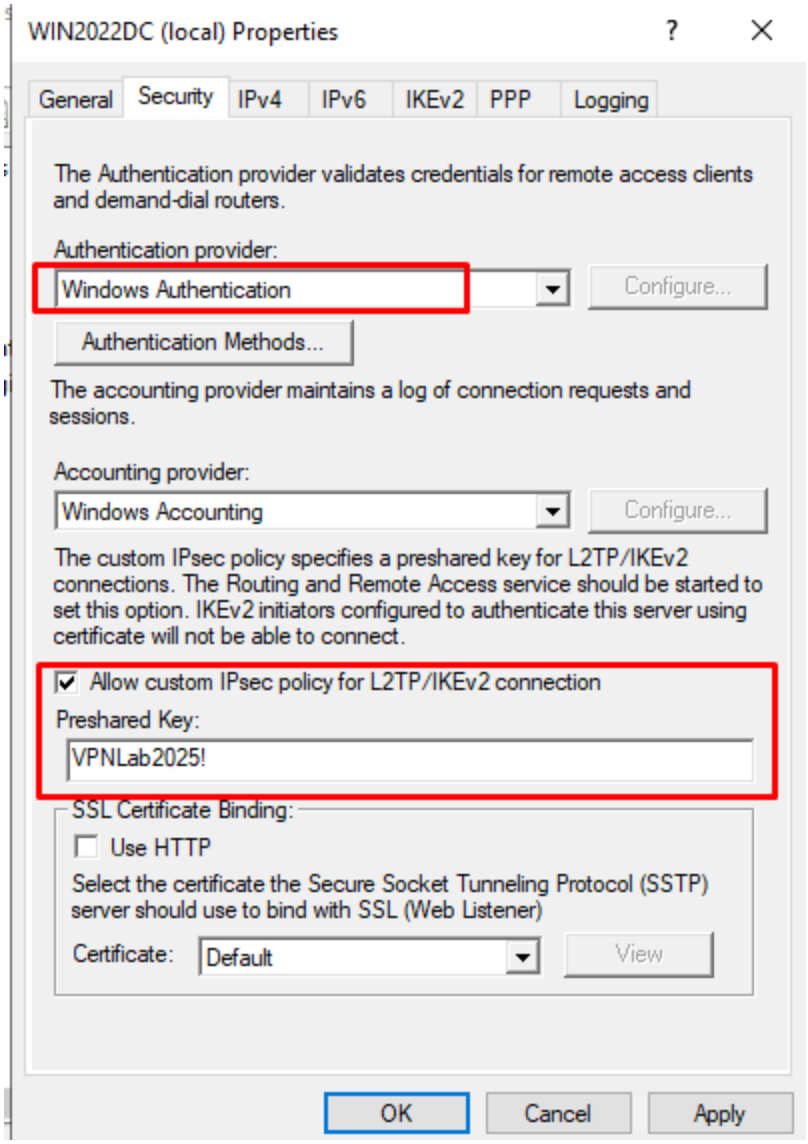


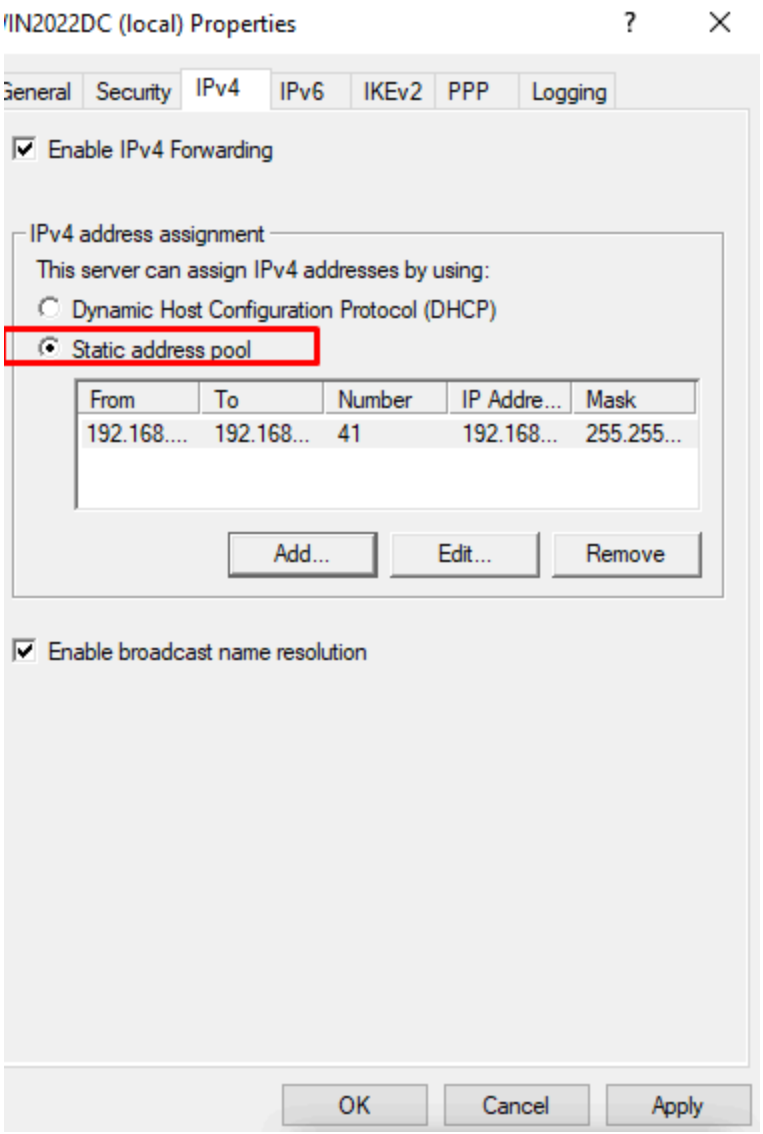
Routing and Remote Access

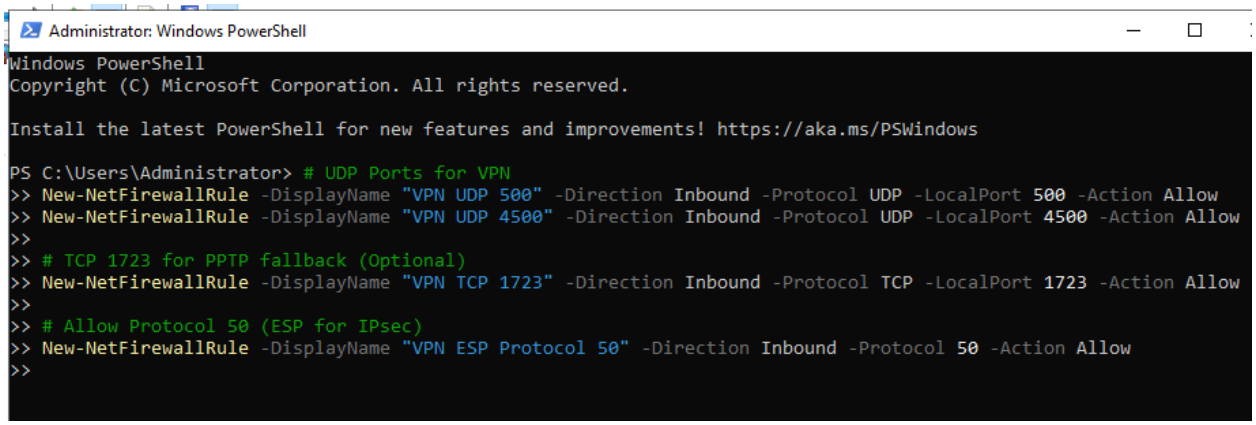



Routing and Remote Access
File Action View Help
Routing and Remote Access
Server Status
WIN2022DC (local)
Network Interfaces
Ports
Remote Access Clients (
Remote Access Logging
IPv4
IPv6
General
Static Routes
WIN2022DC (local)
Routing and Remote Access Is Configured on This Server
This server has already been configured using the Routing and Remote Access Server Setup Wizard. To make changes to the current configuration, select an item in the console tree, and then on the Action menu, click Properties.
Enable DirectAccess on this Server
You are currently using only VPN for providing remote access to your clients. You can use rich remote access experience based on DirectAccess by enabling DirectAccess on this server. Using DirectAccess, your domain-joined clients can seamlessly connect to your corporate network. To enable DirectAccess on this server, you can run the "Enable DirectAccess" wizard by selecting the "Enable DirectAccess..." option on the action pane on the right or on right-clicking the machine node on the left.
Done

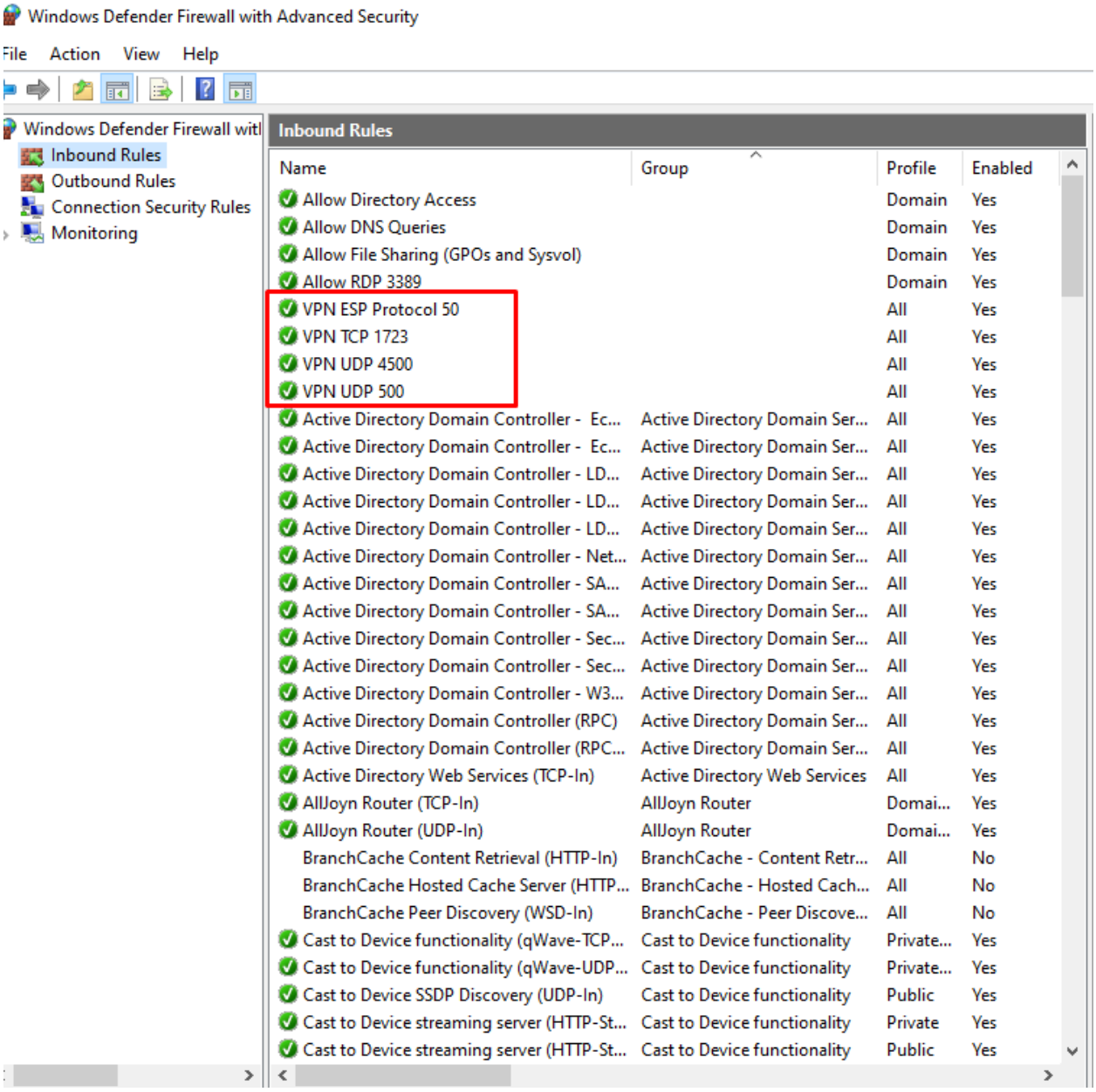

Routing and Remote Access
File Action View Help
Routing and Remote Access
Server Status
WIN2022DC (local)
Configure and Enable Routing and Remote Access
Disable Routing and Remote Access
Enable DirectAccess...
All Tasks
View
Delete
Refresh
Properties
Help
Access Is Configured on This
n configured using the Routing and Remote Access
ake changes to the current configuration, select an
d then on the Action menu, click Properties.
on this Server
VPN for providing remote access to your clients. You
experience based on DirectAccess by enabling
Using DirectAccess, your domain-joined clients can
corporate network. To enable DirectAccess on this
able DirectAccess" wizard by selecting the "Enable
e action pane on the right or on right-clicking the
machine node on the left.
Displays Help for the current selection.


WIN2022DC (local) Properties
General
Security
IPv4
IPv6
IKEv2
PPP
Logging
The Authentication provider validates credentials for remote access clients and demand-dial routers.
Authentication provider:
Windows Authentication
Configure...
Authentication Methods...
The accounting provider maintains a log of connection requests and sessions.
Accounting provider:
Windows Accounting
Configure...
The custom IPsec policy specifies a preshared key for L2TP/IKEv2 connections. The Routing and Remote Access service should be started to set this option. IKEv2 initiators configured to authenticate this server using certificate will not be able to connect.
Allow custom IPsec policy for L2TP/IKEv2 connection
Preshared Key:
VPNLab2025!
SSL Certificate Binding:
Use HTTP
Select the certificate the Secure Socket Tunneling Protocol (SSTP) server should use to bind with SSL (Web Listener)
Certificate:
Default
View
OK
Cancel
Apply

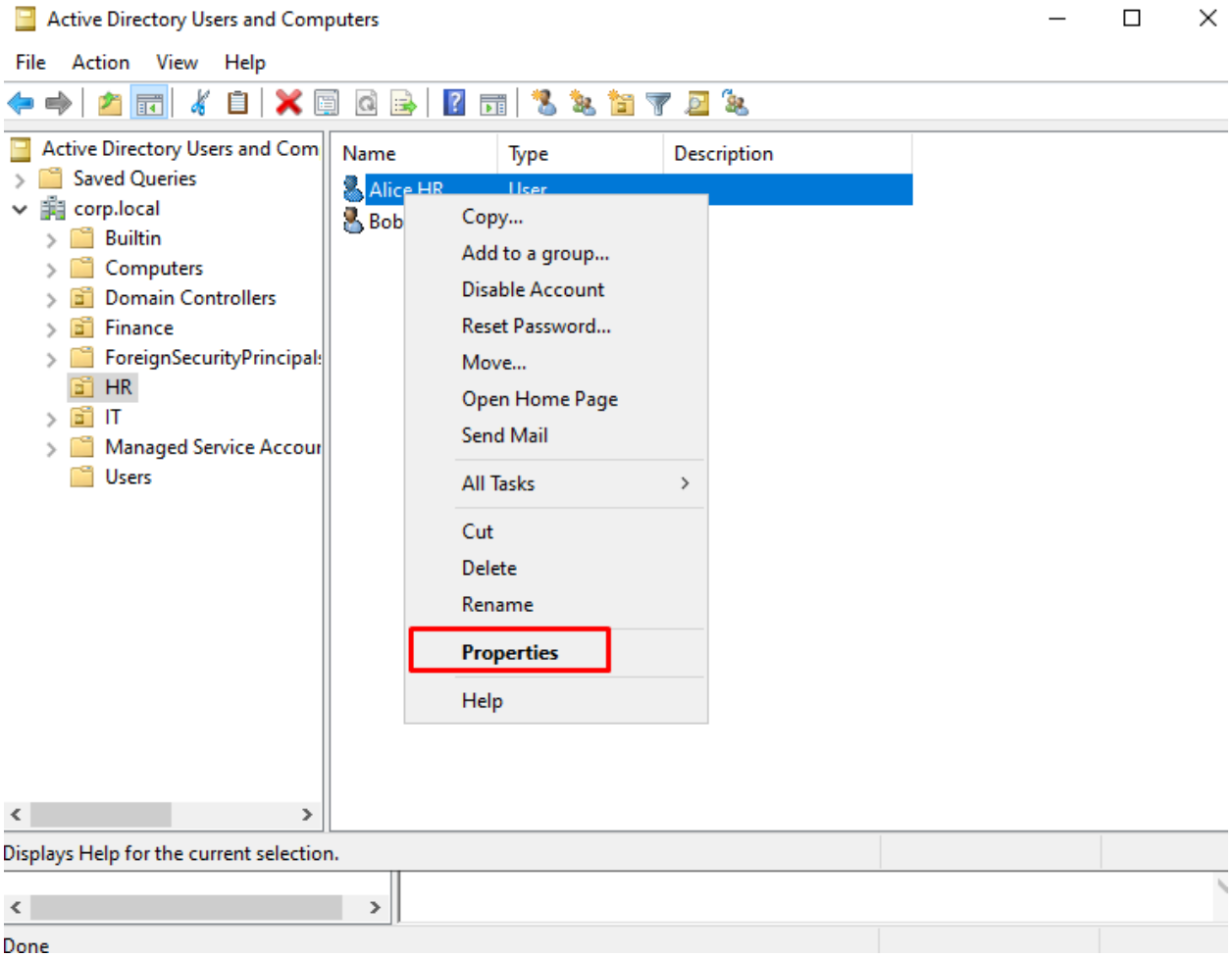

IN2022DC (local) Properties
General
Security
IPv4
IPv6
IKEv2
PPP
Logging
Enable IPv4 Forwarding
IPv4 address assignment
This server can assign IPv4 addresses by using:
Dynamic Host Configuration Protocol (DHCP)
Static address pool
From
To
Number
IP Addre...
Mask
192.168....
192.168...
41
192.168...
255.255...
Add...
Edit...
Remove
Enable broadcast name resolution
OK
Cancel
Apply

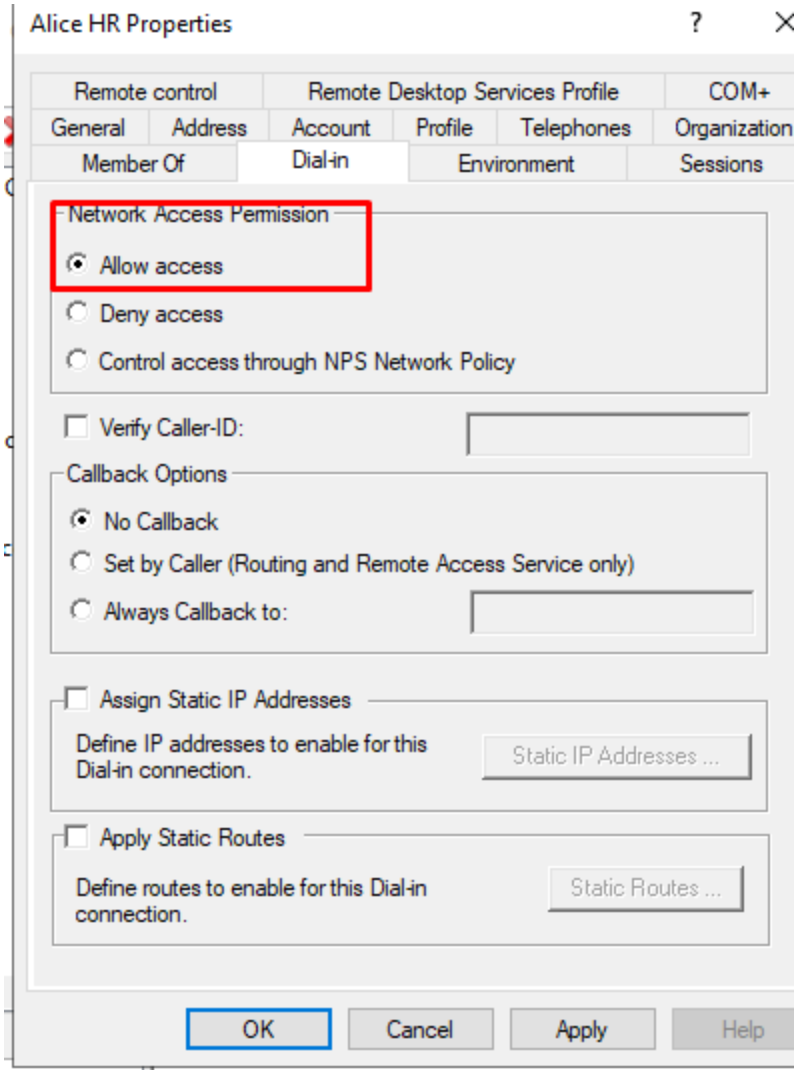

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS C:\Users\Administrator> # UDP Ports for VPN
>> New-NetFirewallRule -DisplayName "VPN UDP 500" -Direction Inbound -Protocol UDP -LocalPort 500 -Action Allow
>> New-NetFirewallRule -DisplayName "VPN UDP 4500" -Direction Inbound -Protocol UDP -LocalPort 4500 -Action Allow
>>
>> # TCP 1723 for PPTP fallback (Optional)
>> New-NetFirewallRule -DisplayName "VPN TCP 1723" -Direction Inbound -Protocol TCP -LocalPort 1723 -Action Allow
>>
>> # Allow Protocol 50 (ESP for IPsec)
>> New-NetFirewallRule -DisplayName "VPN ESP Protocol 50" -Direction Inbound -Protocol 50 -Action Allow
>>

```
Name                            : {c5985086-e4d6-45e0-bd45-8d0a4d23f6d7}
DisplayName                     : VPN UDP 500
Description                     :
DisplayGroup                    :
Group                           :
Enabled                         : True
Profile                         : Any
Platform                        : {}
Direction                       : Inbound
Action                          : Allow
EdgeTraversalPolicy             : Block
LooseSourceMapping              : False
LocalOnlyMapping                : False
Owner                           :
PrimaryStatus                   : OK
Status                          : The rule was parsed successfully from the store. (65536)
EnforcementStatus               : NotApplicable
PolicyStoreSource               : PersistentStore
PolicyStoreSourceType           : Local
RemoteDynamicKeywordAddresses : {}

Name                            : {22651a48-7725-40bd-b5ef-f3f4051967ad}
```

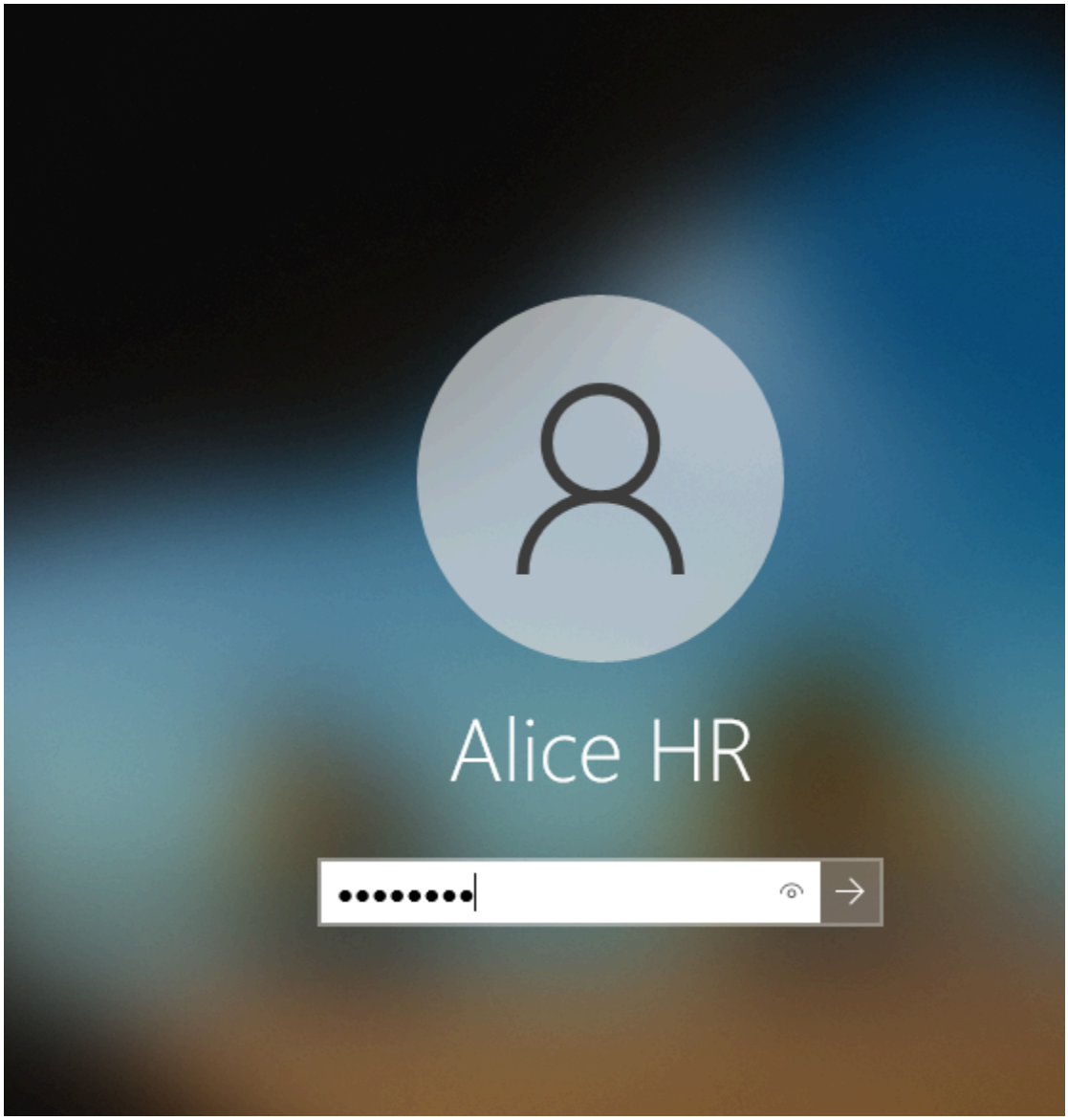

Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall witl
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name Group Profile Enabled
Allow Directory Access Domain Yes
Allow DNS Queries Domain Yes
Allow File Sharing (GPOs and Sysvol) Domain Yes
Allow RDP 3389 Domain Yes
VPN ESP Protocol 50 All Yes
VPN TCP 1723 All Yes
VPN UDP 4500 All Yes
VPN UDP 500 All Yes
Active Directory Domain Controller - Ec... Active Directory Domain Ser... All Yes
Active Directory Domain Controller - Ec... Active Directory Domain Ser... All Yes
Active Directory Domain Controller - LD... Active Directory Domain Ser... All Yes
Active Directory Domain Controller - LD... Active Directory Domain Ser... All Yes
Active Directory Domain Controller - LD... Active Directory Domain Ser... All Yes
Active Directory Domain Controller - Net... Active Directory Domain Ser... All Yes
Active Directory Domain Controller - SA... Active Directory Domain Ser... All Yes
Active Directory Domain Controller - SA... Active Directory Domain Ser... All Yes
Active Directory Domain Controller - Sec... Active Directory Domain Ser... All Yes
Active Directory Domain Controller - Sec... Active Directory Domain Ser... All Yes
Active Directory Domain Controller - W3... Active Directory Domain Ser... All Yes
Active Directory Domain Controller (RPC) Active Directory Domain Ser... All Yes
Active Directory Domain Controller (RPC... Active Directory Domain Ser... All Yes
Active Directory Web Services (TCP-In) Active Directory Web Services All Yes
AllJoyn Router (TCP-In) AllJoyn Router Domai... Yes
AllJoyn Router (UDP-In) AllJoyn Router Domai... Yes
BranchCache Content Retrieval (HTTP-In) BranchCache - Content Retr... All No
BranchCache Hosted Cache Server (HTTP... BranchCache - Hosted Cach... All No
BranchCache Peer Discovery (WSD-In) BranchCache - Peer Discove... All No
Cast to Device functionality (qWave-TCP... Cast to Device functionality Private... Yes
Cast to Device functionality (qWave-UDP... Cast to Device functionality Private... Yes
Cast to Device SSDP Discovery (UDP-In) Cast to Device functionality Public Yes
Cast to Device streaming server (HTTP-St... Cast to Device functionality Private Yes
Cast to Device streaming server (HTTP-St... Cast to Device functionality Public Yes

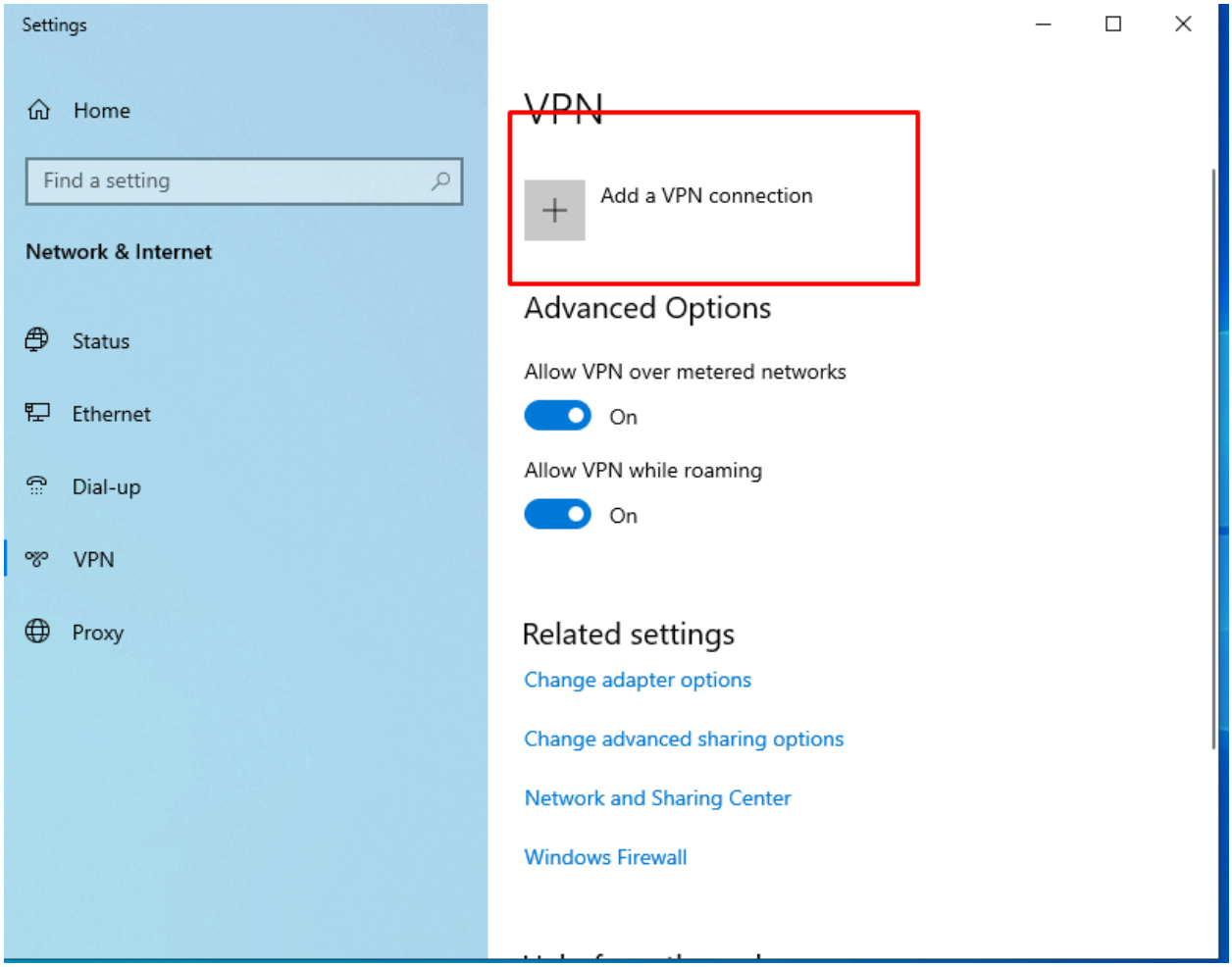
Enable VPN Access for a User

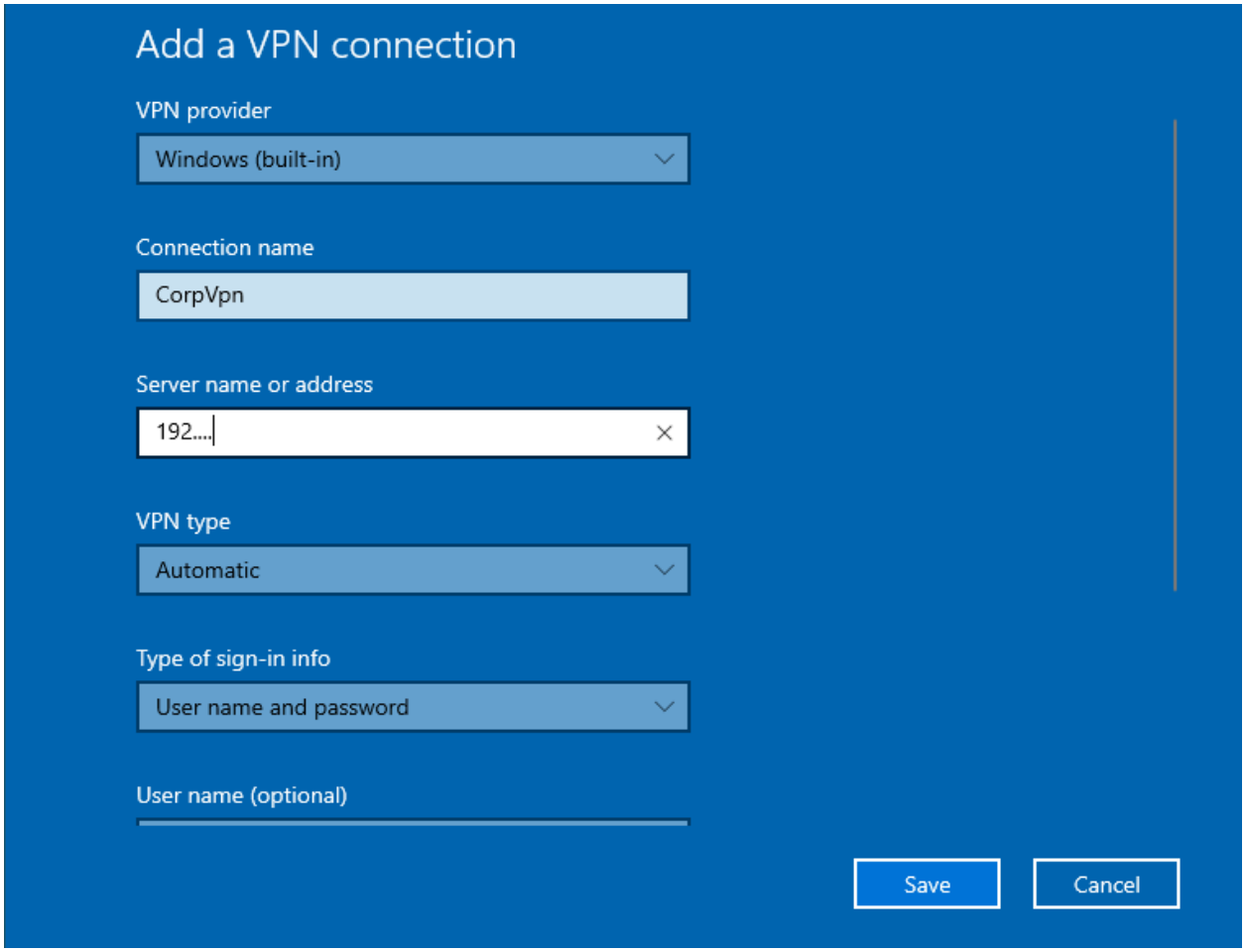


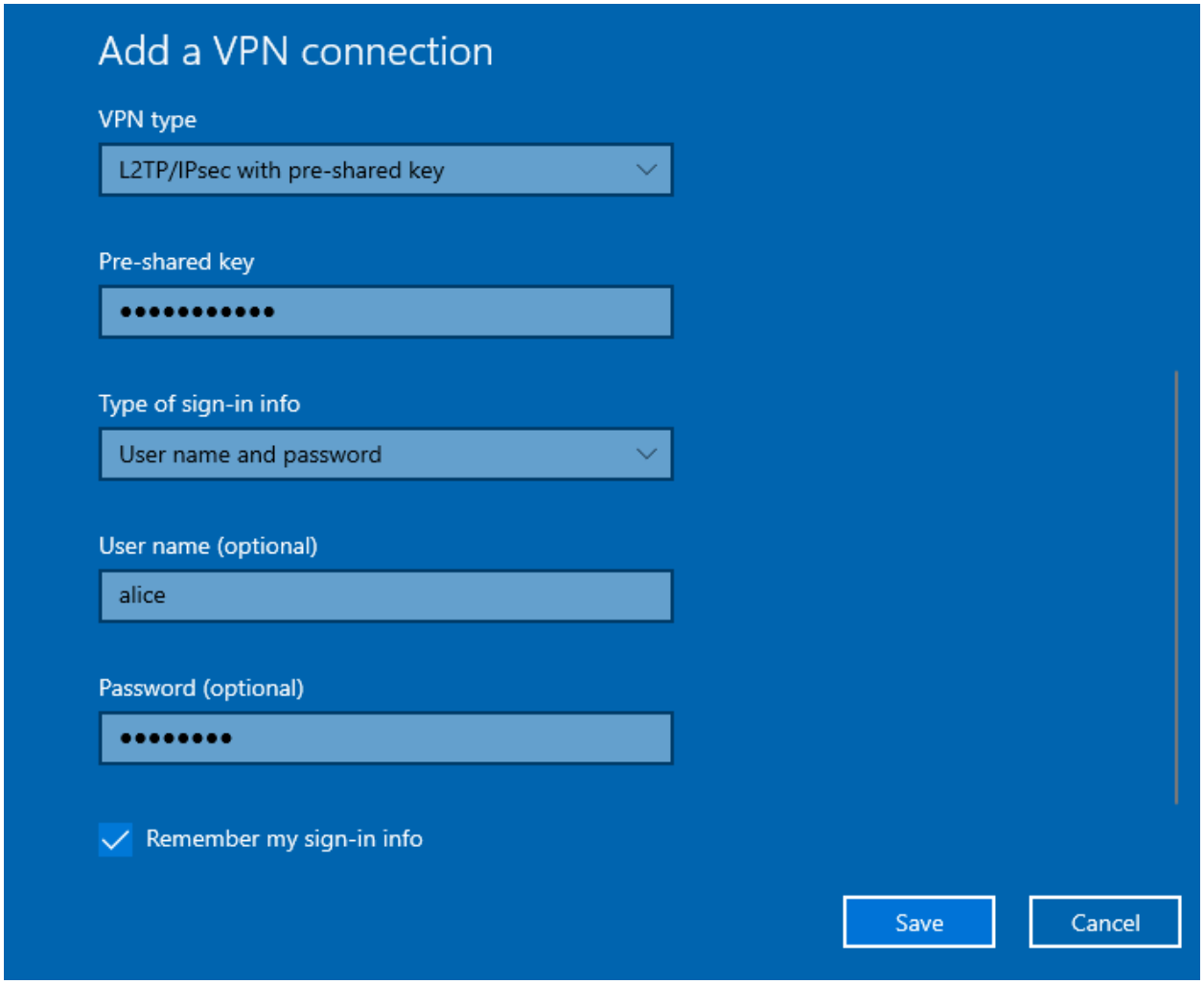

Alice HR Properties
Remote control
Remote Desktop Services Profile
COM+
General
Address
Account
Profile
Telephones
Organization
Member Of
Dial-in
Environment
Sessions
Network Access Permission
Allow access
Deny access
Control access through NPS Network Policy
Verify Caller-ID:
Callback Options
No Callback
Set by Caller (Routing and Remote Access Service only)
Always Callback to:
Assign Static IP Addresses
Define IP addresses to enable for this Dial-in connection.
Static IP Addresses ...
Apply Static Routes
Define routes to enable for this Dial-in connection.
Static Routes ...
OK
Cancel
Apply
Help

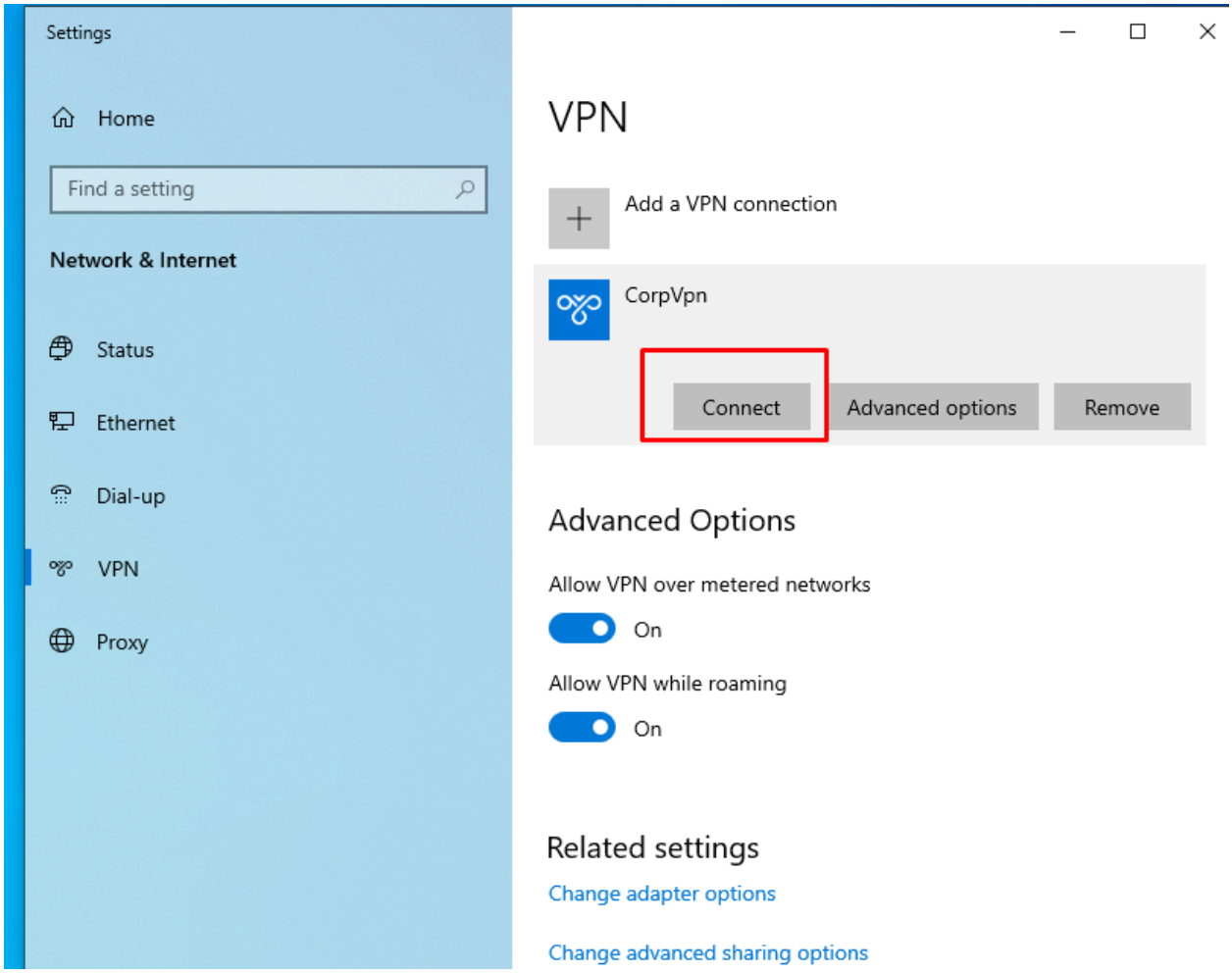
Login Windows 10 VM: Connect to created VPN

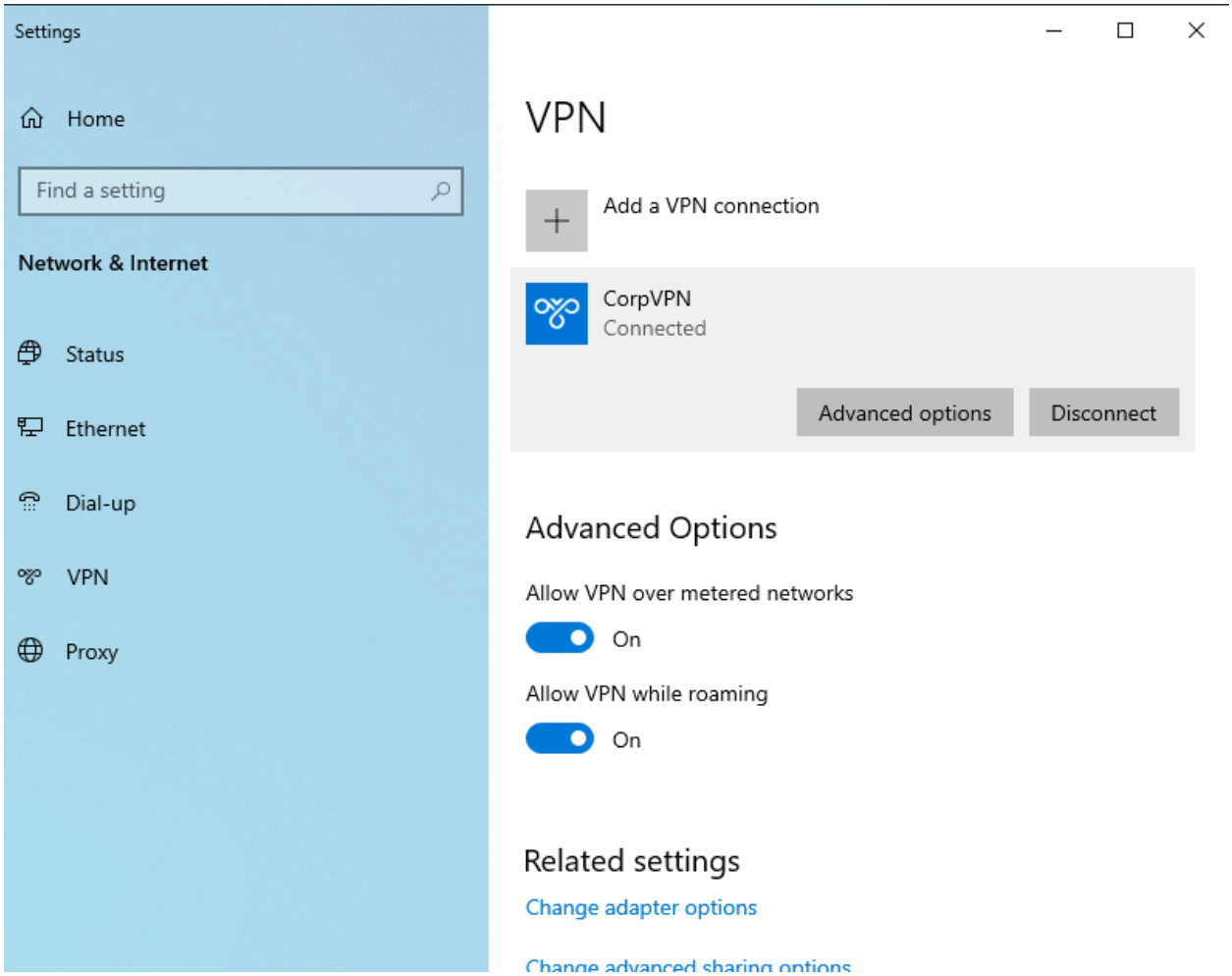



Settings
Home
Find a setting
Network & Internet
Status
Ethernet
Dial-up
VPN
Proxy
VPN
Add a VPN connection
Advanced Options
Allow VPN over metered networks
On
Allow VPN while roaming
On
Related settings
Change adapter options
Change advanced sharing options
Network and Sharing Center
Windows Firewall


Add a VPN connection
VPN provider
Windows (built-in)
Connection name
CorpVpn
Server name or address
192....
VPN type
Automatic
Type of sign-in info
User name and password
User name (optional)
Save
Cancel

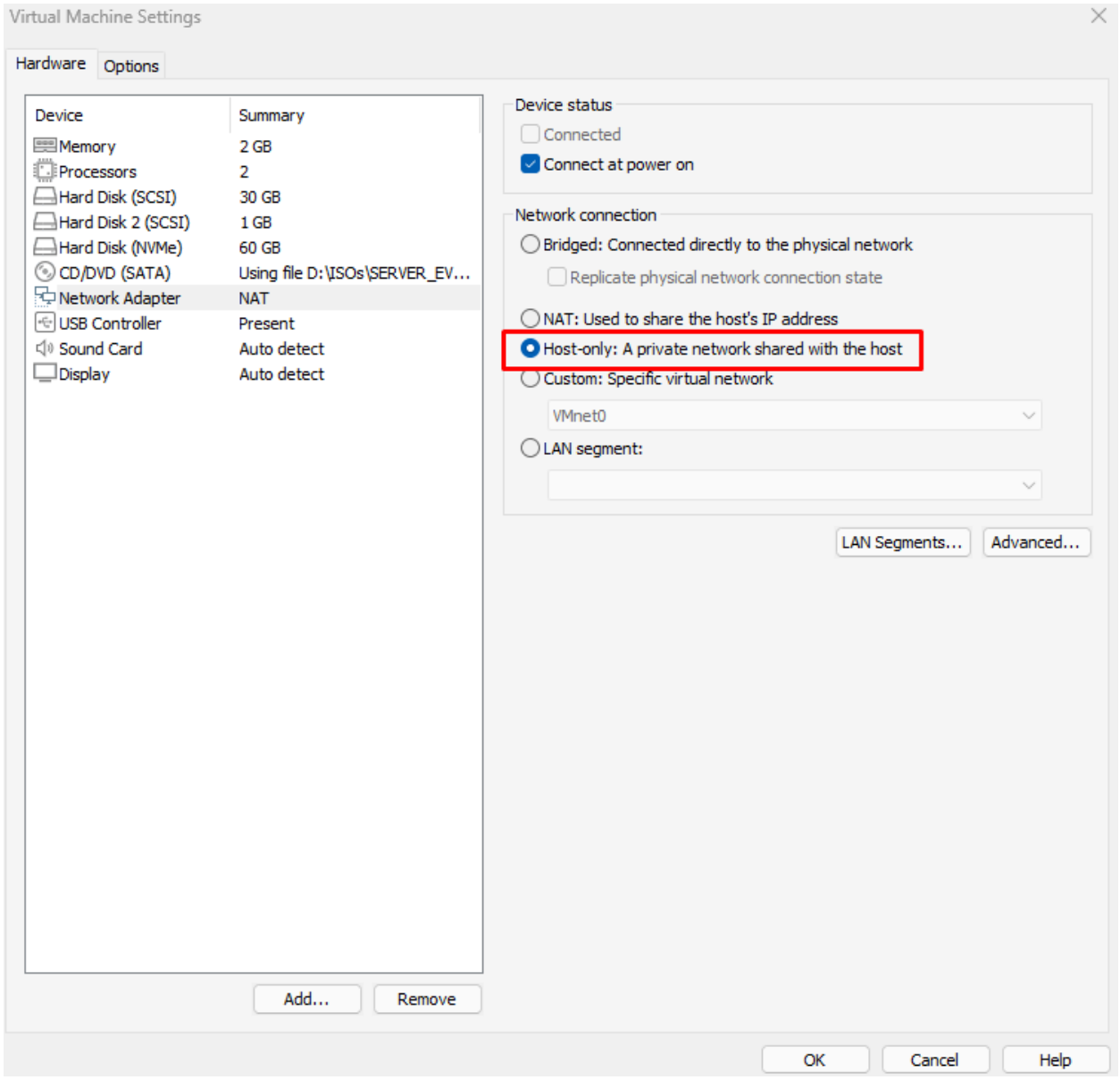

Add a VPN connection
VPN type
L2TP/IPsec with pre-shared key
Pre-shared key
Type of sign-in info
User name and password
User name (optional)
alice
Password (optional)
Remember my sign-in info
Save
Cancel

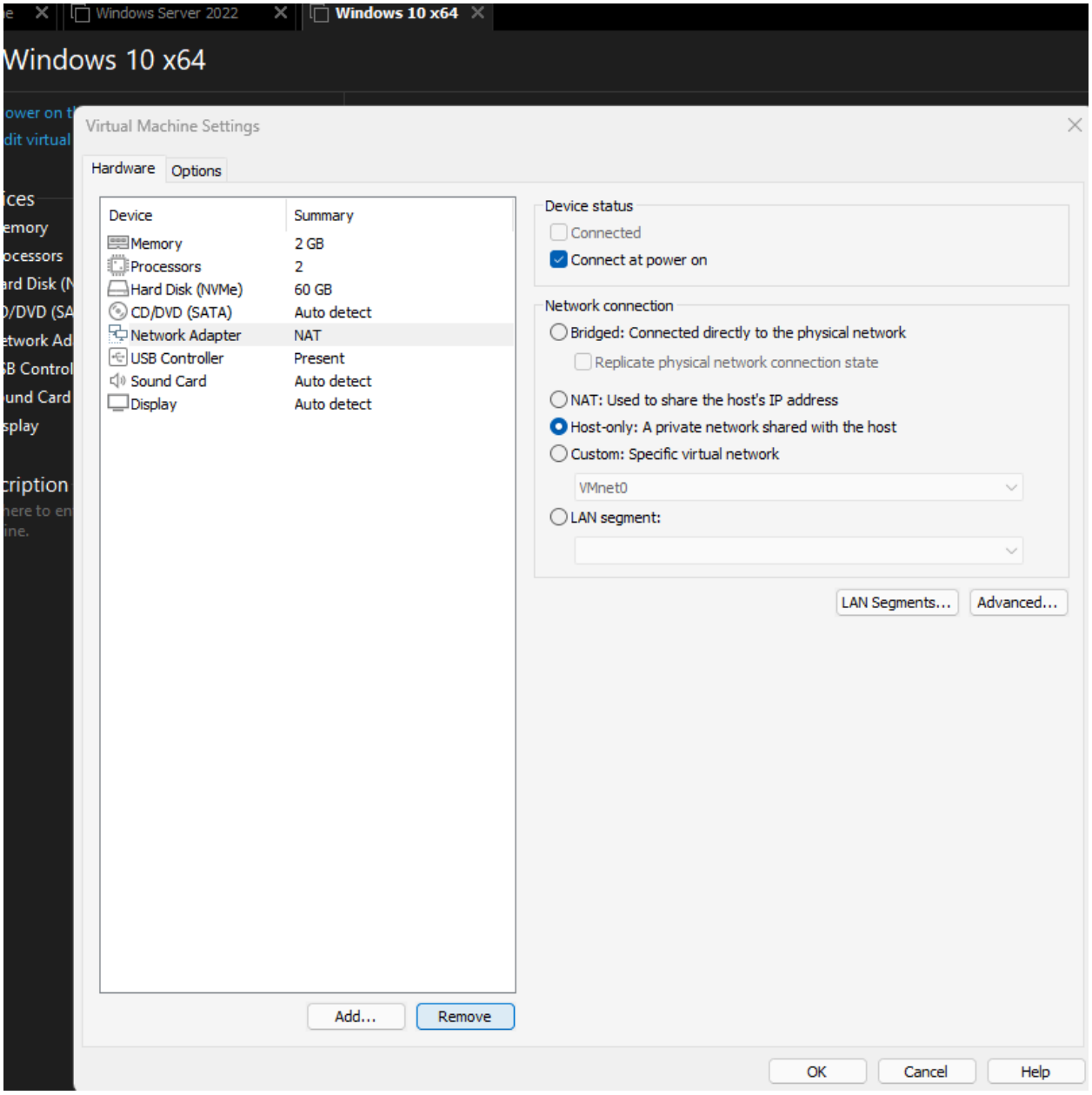

Settings
Home
Find a setting
Network & Internet
Status
Ethernet
Dial-up
VPN
Proxy
VPN
Add a VPN connection
CorpVpn
Connect
Advanced options
Remove
Advanced Options
Allow VPN over metered networks
On
Allow VPN while roaming
On
Related settings
Change adapter options
Change advanced sharing options



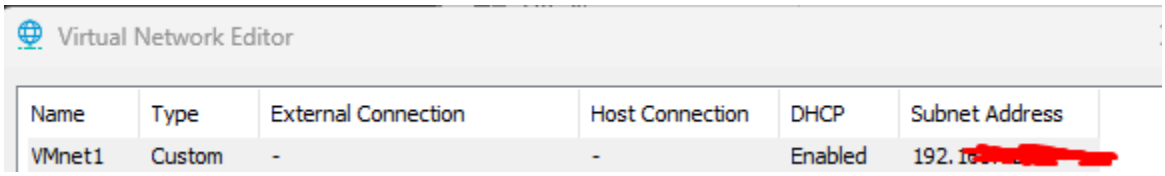
VPN successfully connected

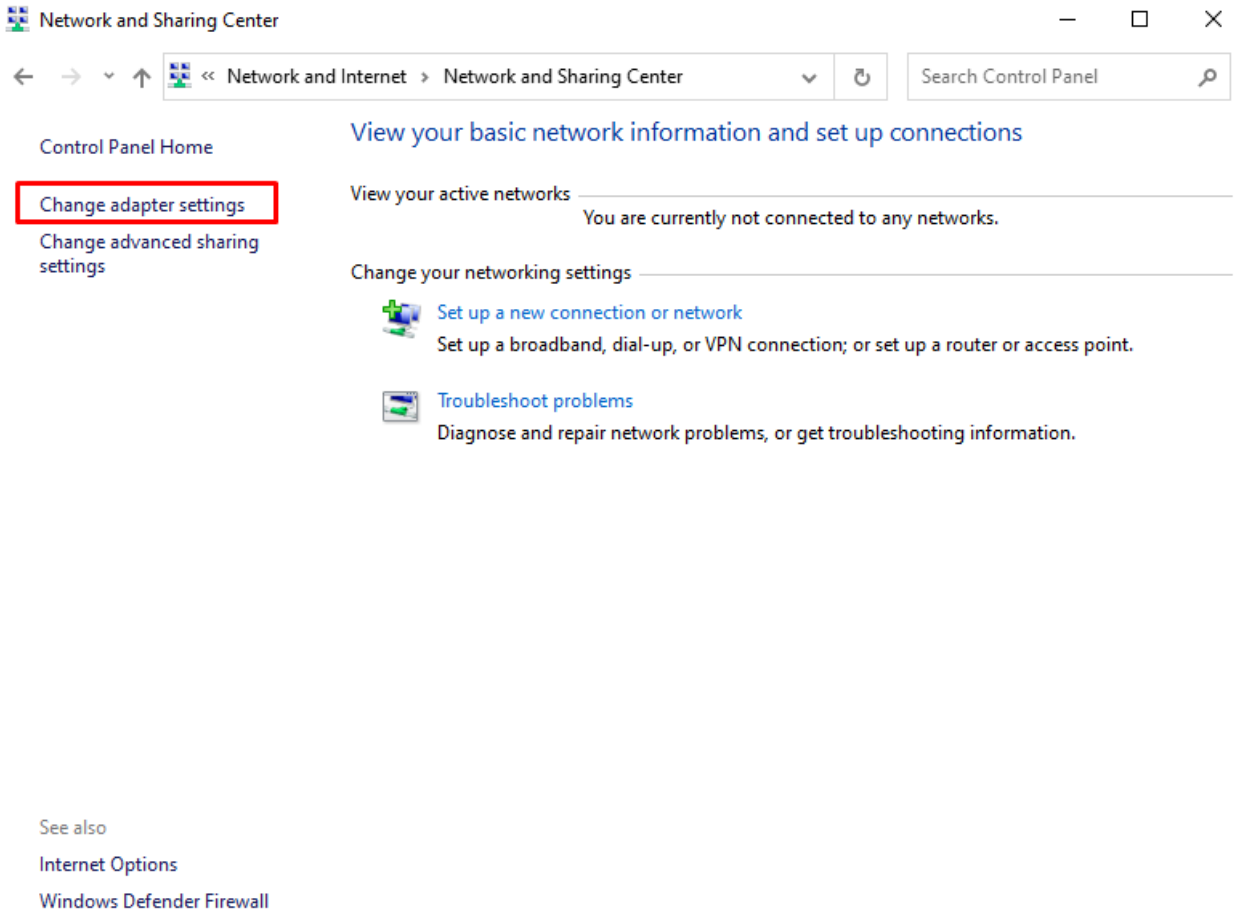
Windows Server 2022 & Windows 10 VM: Switch from NAT to Host-only network

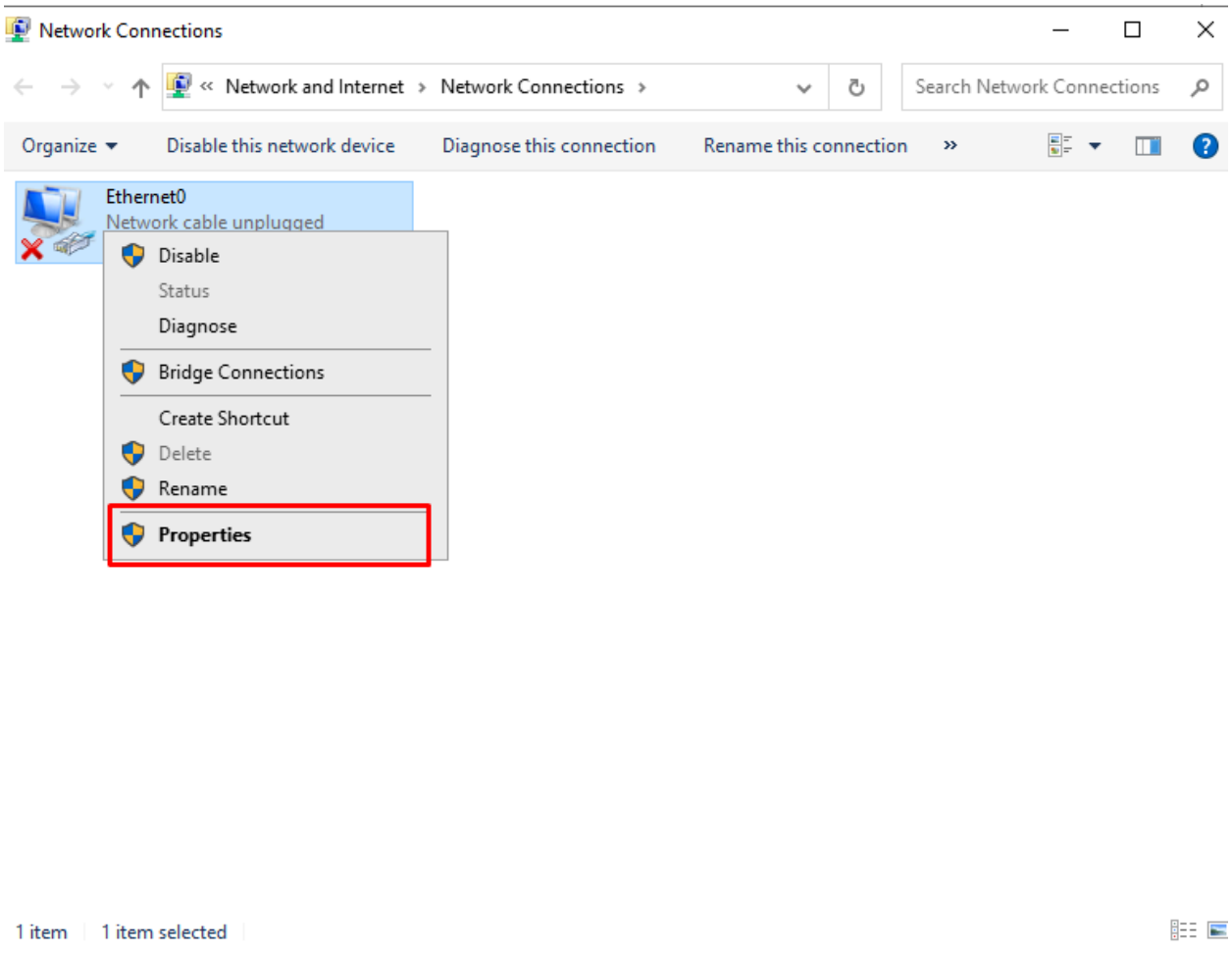


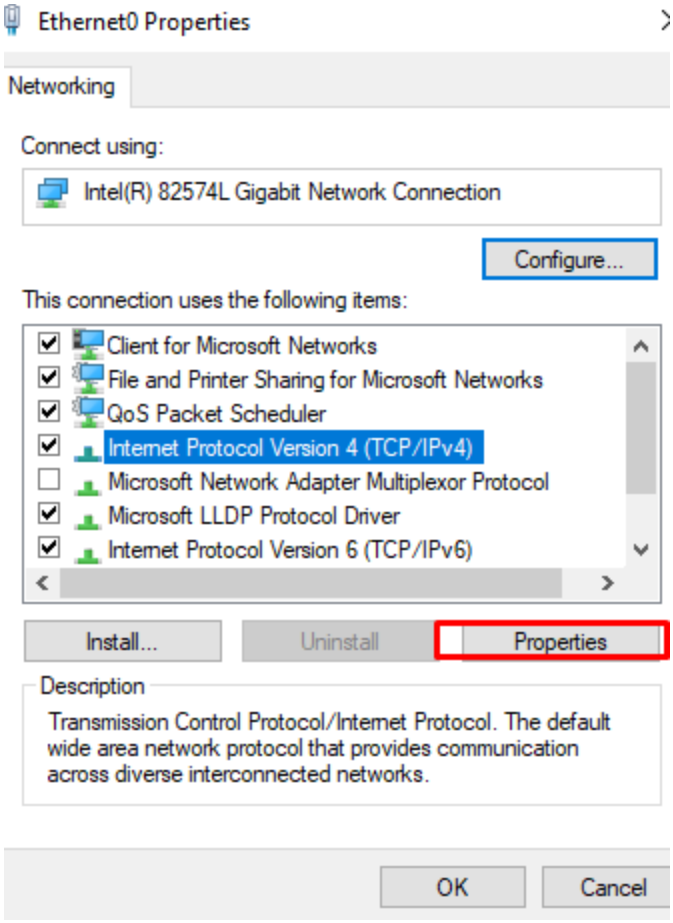


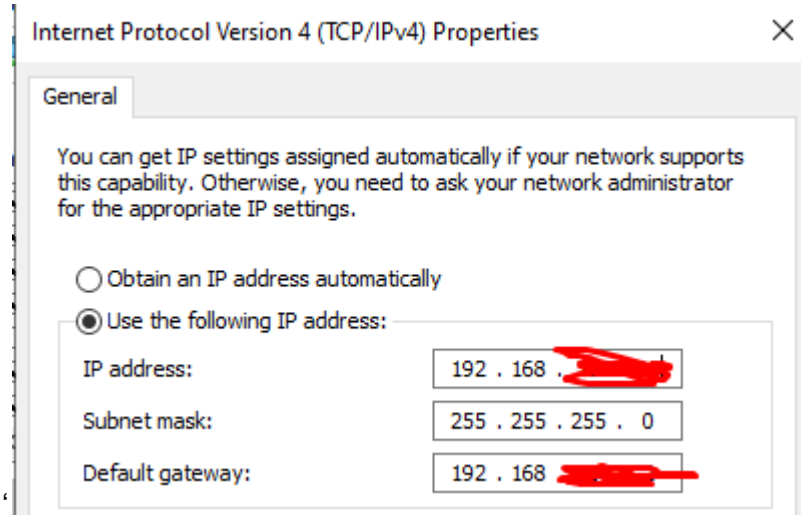
Complete steps above for both machines

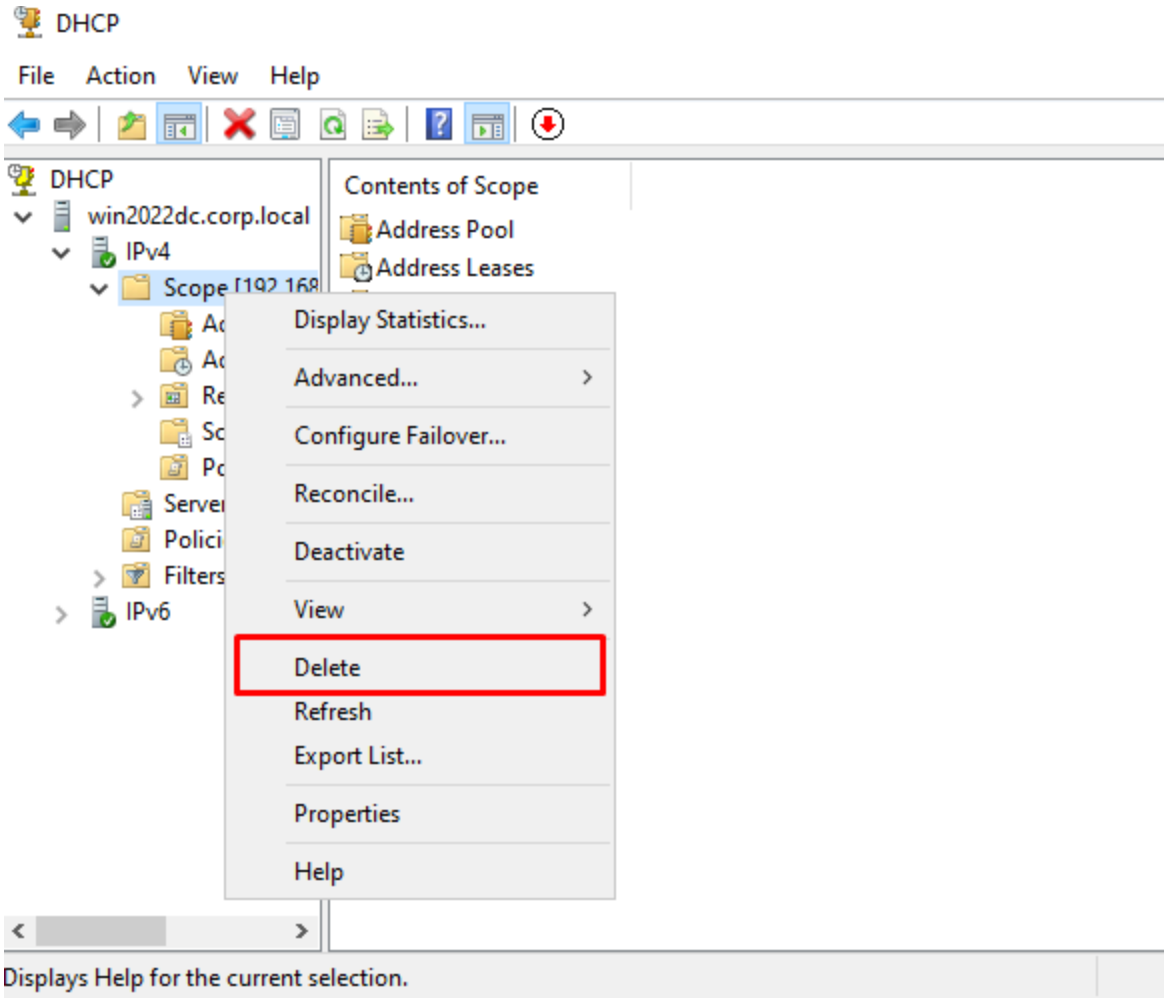


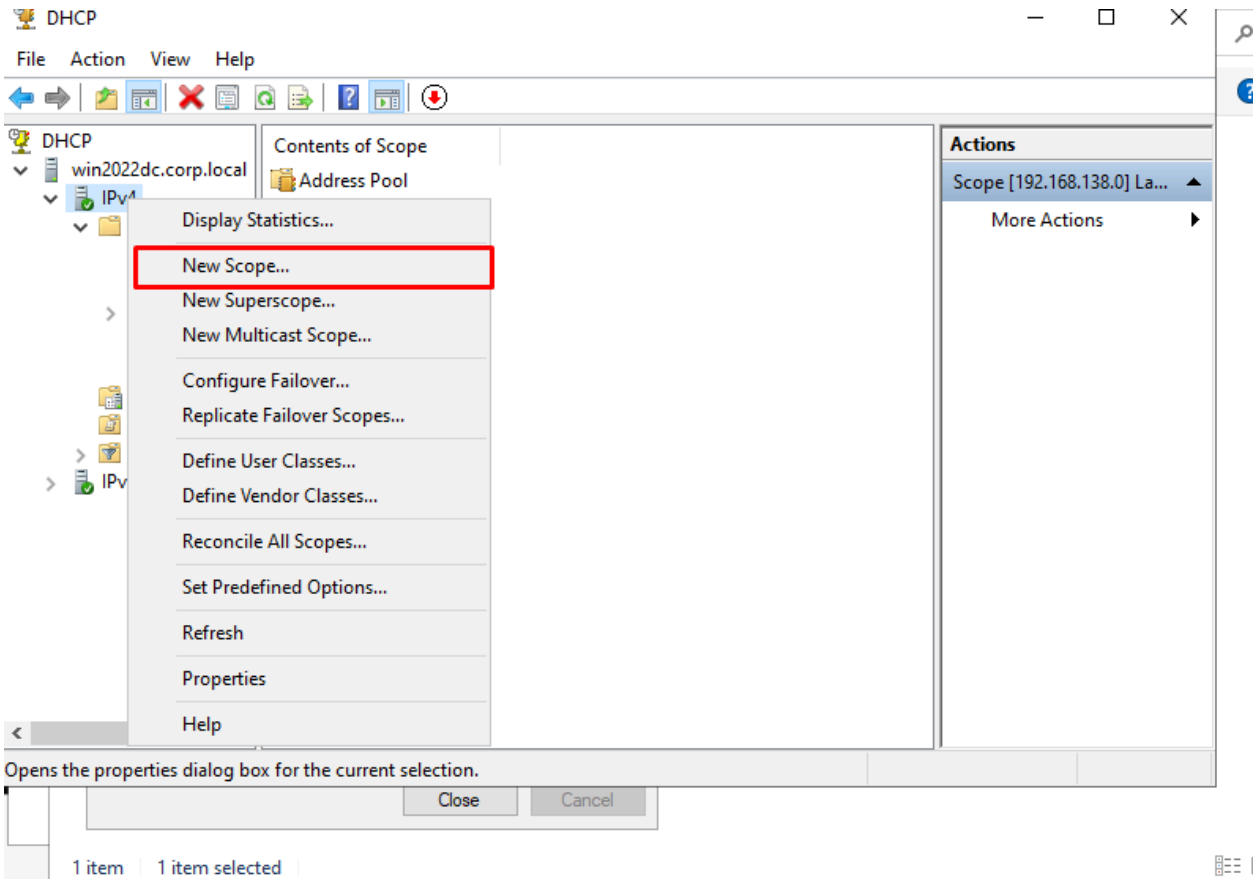

Network and Sharing Center
Network and Internet › Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
View your active networks
You are currently not connected to any networks.
Change your networking settings
Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.
Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.
See also
Internet Options
Windows Defender Firewall


Network Connections
Network and Internet
Network Connections
Search Network Connections
Organize
Disable this network device
Diagnose this connection
Rename this connection
Ethernet0
Network cable unplugged
Disable
Status
Diagnose
Bridge Connections
Create Shortcut
Delete
Rename
Properties
1 item
1 item selected


Ethernet0 Properties
Networking
Connect using:
Intel(R) 82574L Gigabit Network Connection
Configure...
This connection uses the following items:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
QoS Packet Scheduler
Internet Protocol Version 4 (TCP/IPv4)
Microsoft Network Adapter Multiplexor Protocol
Microsoft LLDP Protocol Driver
Internet Protocol Version 6 (TCP/IPv6)
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
OK
Cancel


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 .
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
192 . 168


DHCP
File
Action
View
Help
DHCP
win2022dc.corp.local
IPv4
Scope [192.168
IPv6
Contents of Scope
Address Pool
Address Leases
Display Statistics...
Advanced...
Configure Failover...
Reconcile...
Deactivate
View
Delete
Refresh
Export List...
Properties
Help
Displays Help for the current selection.


DHCP
File
Action
View
Help
DHCP
win2022dc.corp.local
IPv4
Contents of Scope
Address Pool
Actions
Scope [192.168.138.0] La...
More Actions
Display Statistics...
New Scope...
New Superscope...
New Multicast Scope...
Configure Failover...
Replicate Failover Scopes...
Define User Classes...
Define Vendor Classes...
Reconcile All Scopes...
Set Predefined Options...
Refresh
Properties
Help
Opens the properties dialog box for the current selection.
Close
Cancel
1 item
1 item selected

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: HostOnlyScope

Description: Host scope

< Back | Next > | Cancel

New Scope Wizard

IP Address Range

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

Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address: 192 [redacted]

End IP address: 192 [redacted]

Configuration settings that propagate to DHCP Client

Length: 24

Subnet mask: 255 . 255 . 255 . 0

< Back | Next > | Cancel

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

< Back | Next > | Cancel

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:

. . .

Add

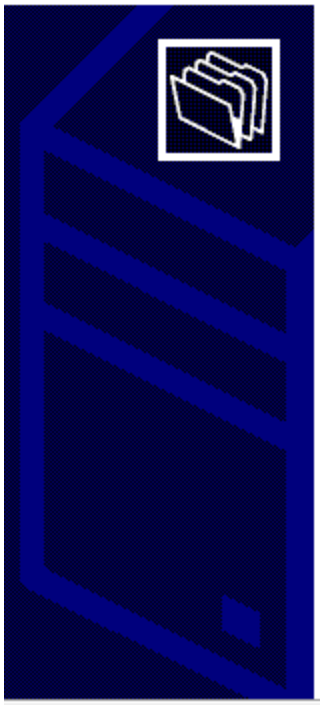
Remove

Up

Down

< Back | Next > | Cancel

New Scope Wizard



Completing the New Scope Wizard

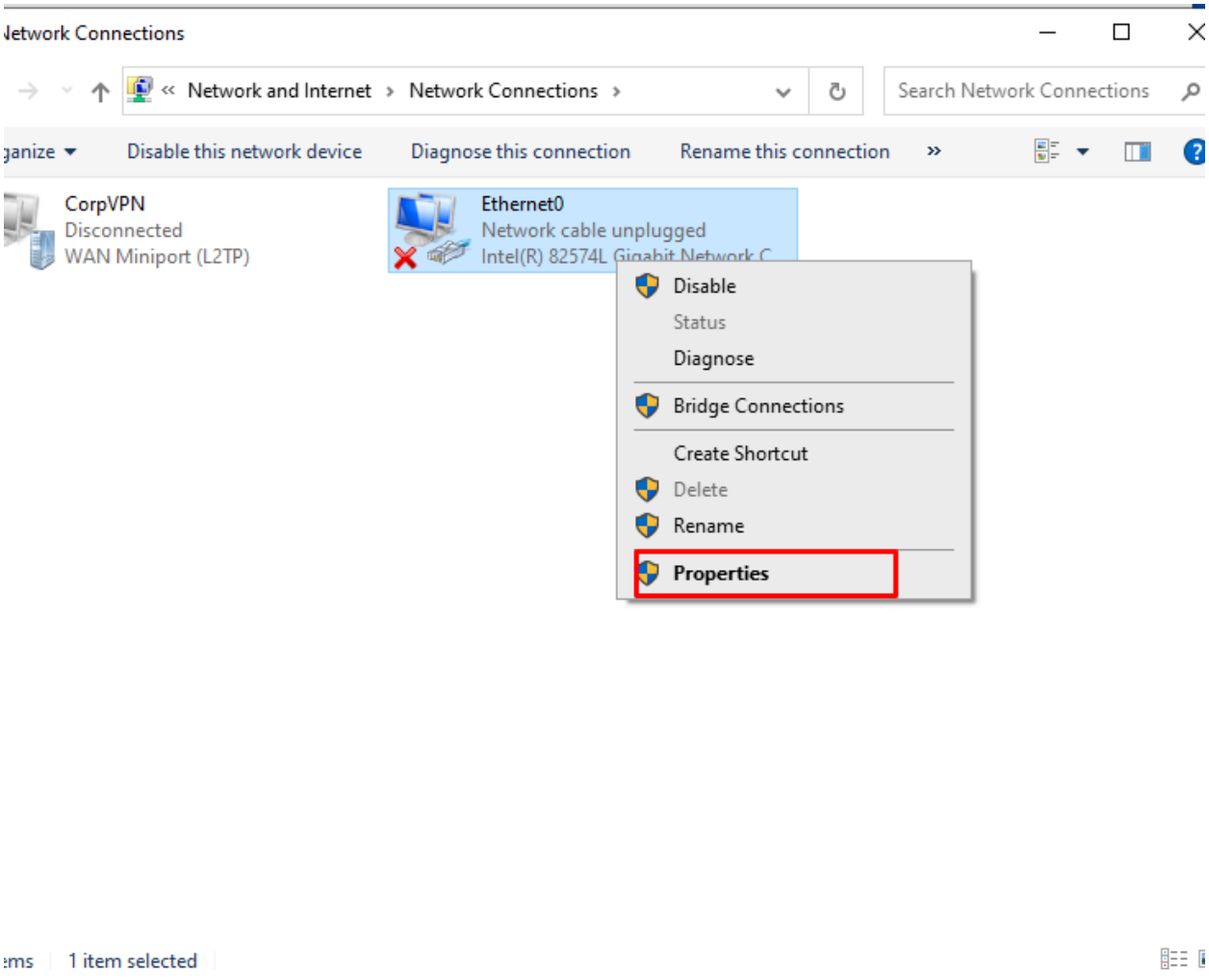
You have successfully completed the New Scope wizard.

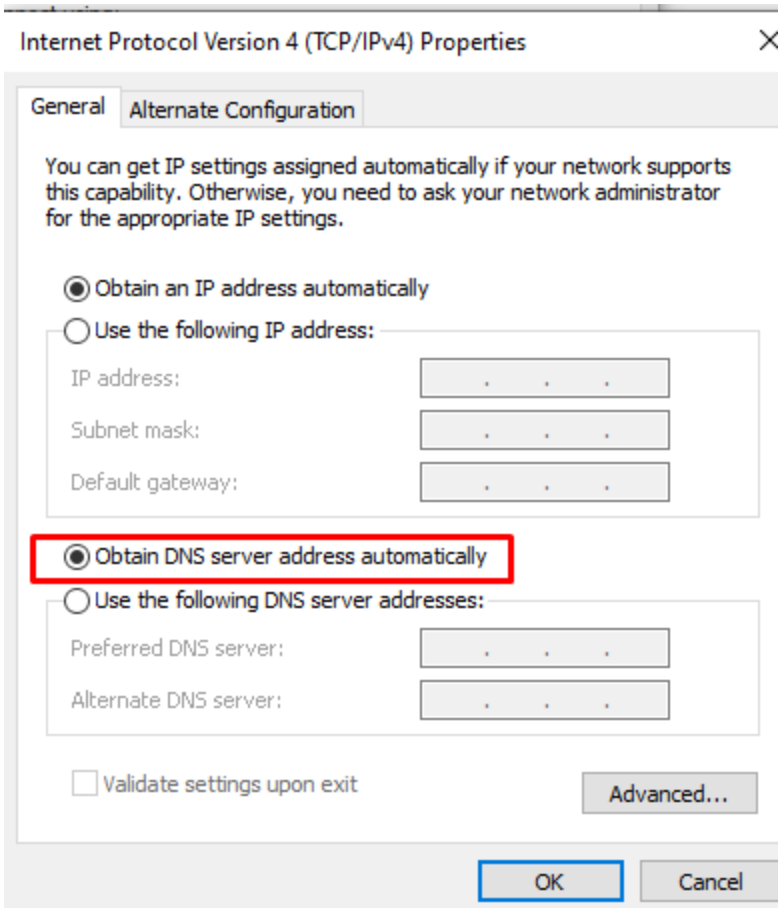
To provide high availability for this scope, configure failover for the newly added scope by right clicking on the scope and clicking on configure failover.

To close this wizard, click Finish.

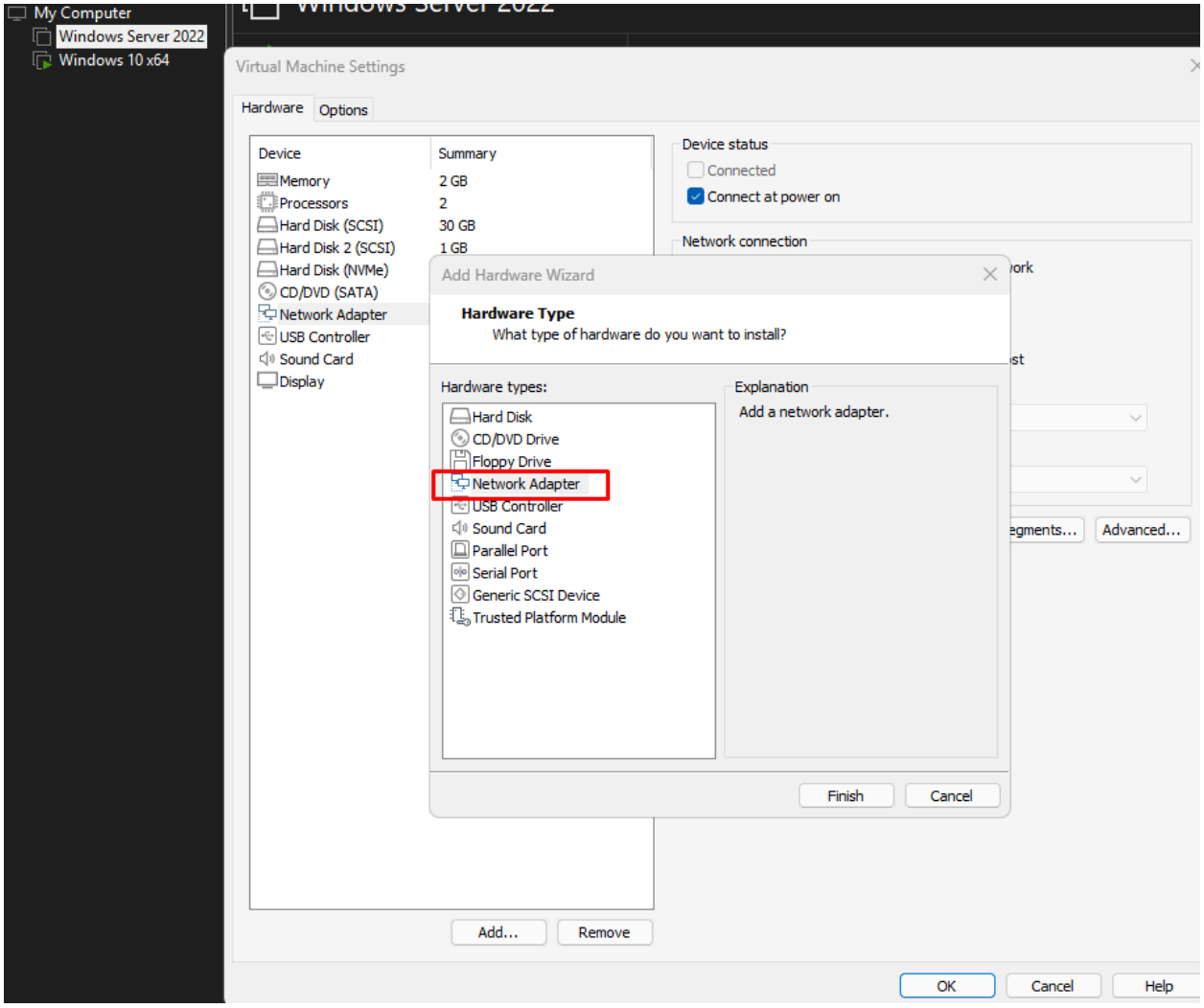
< Back | Finish | Cancel

Windows 10 VM: Change to Host Network



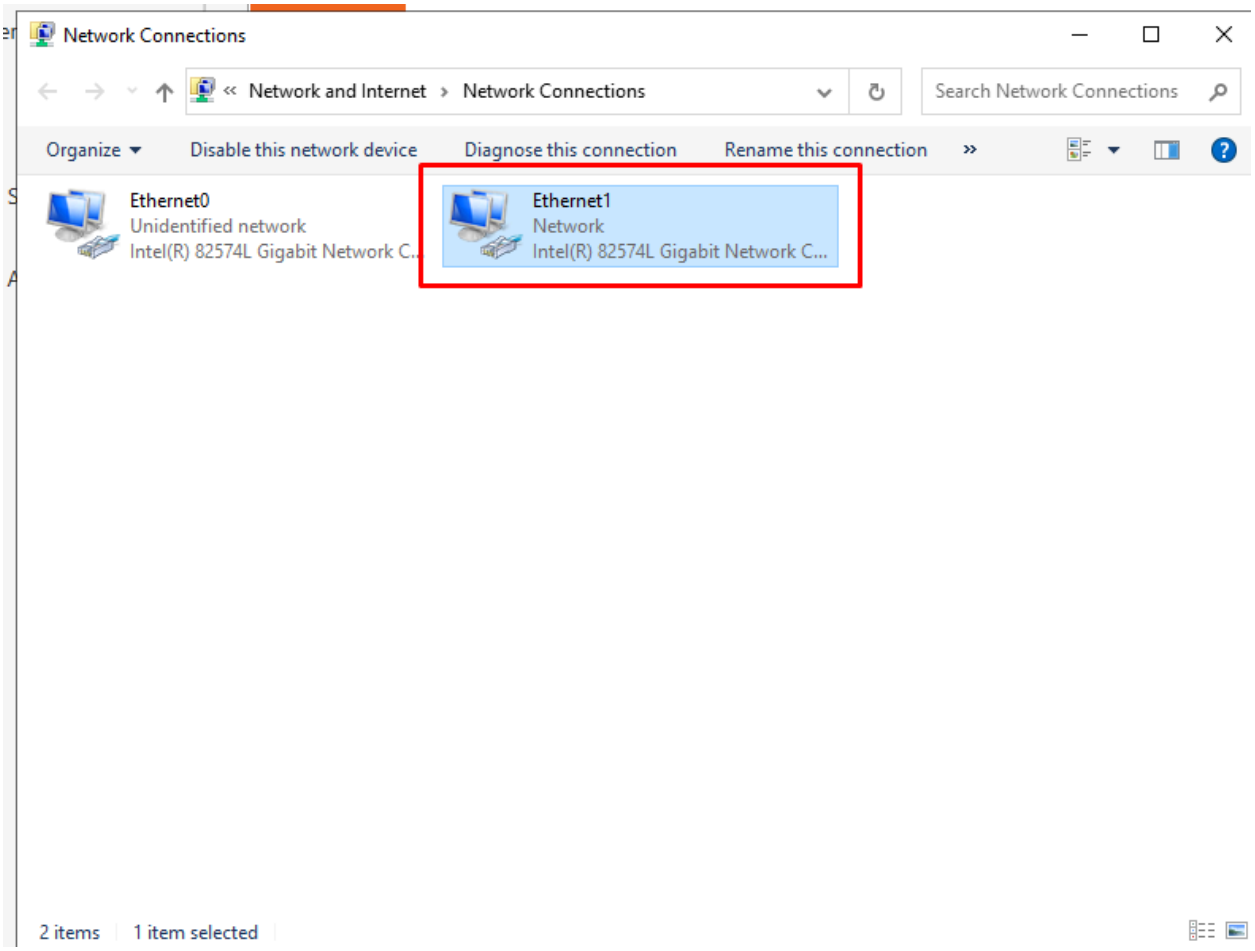

Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

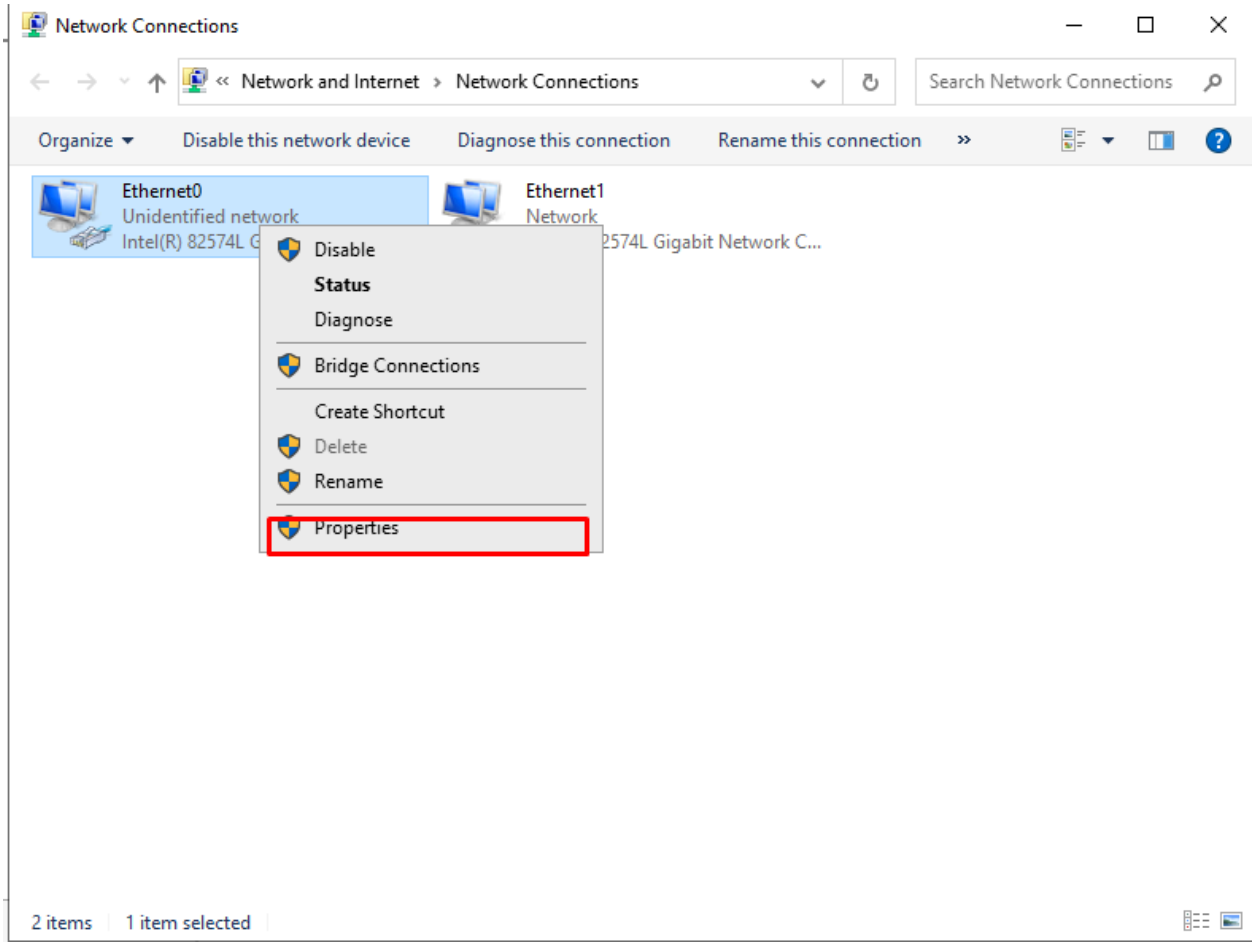
Windows Server 2022 & Windows 10 VM: Add new network adapter 2 for internet connection, Using both NAT & Host:

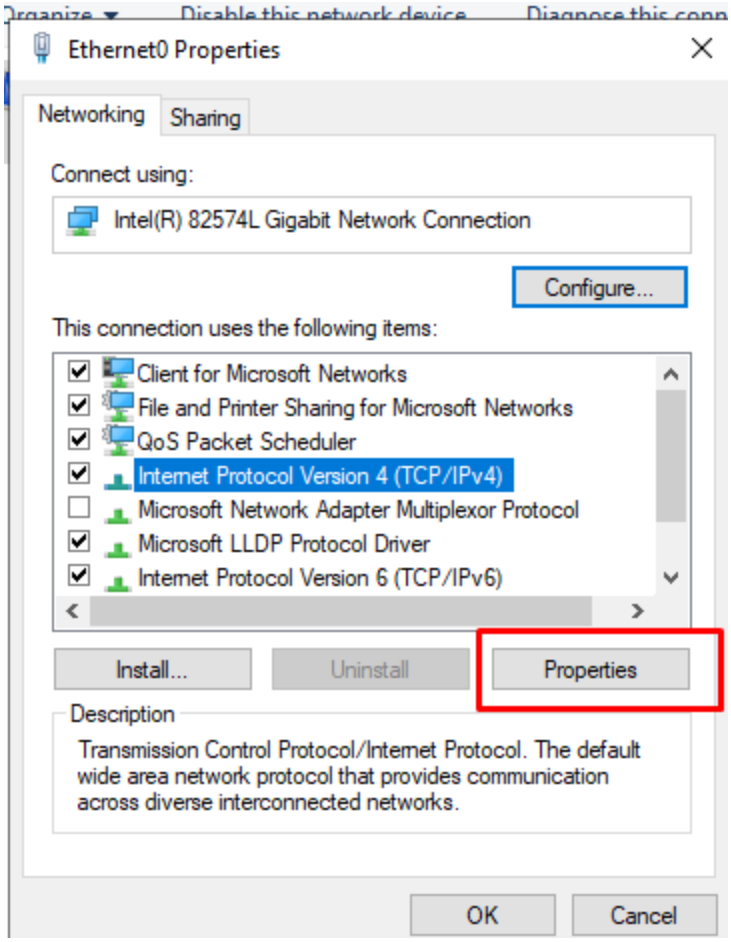


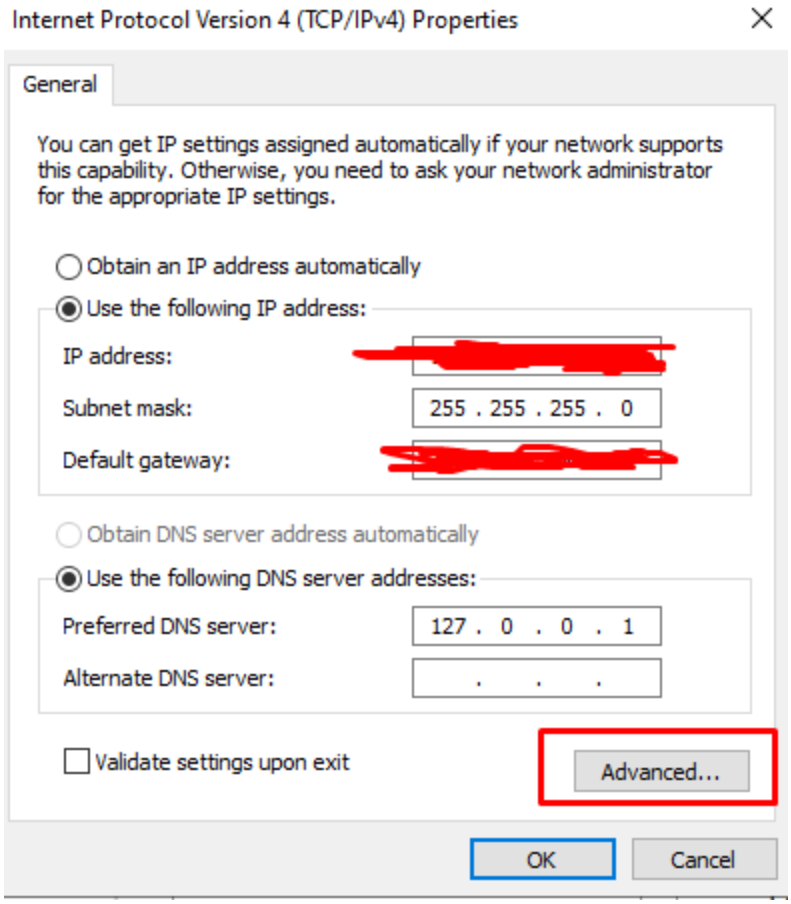
Repeat Above Step for Windows 10 VM

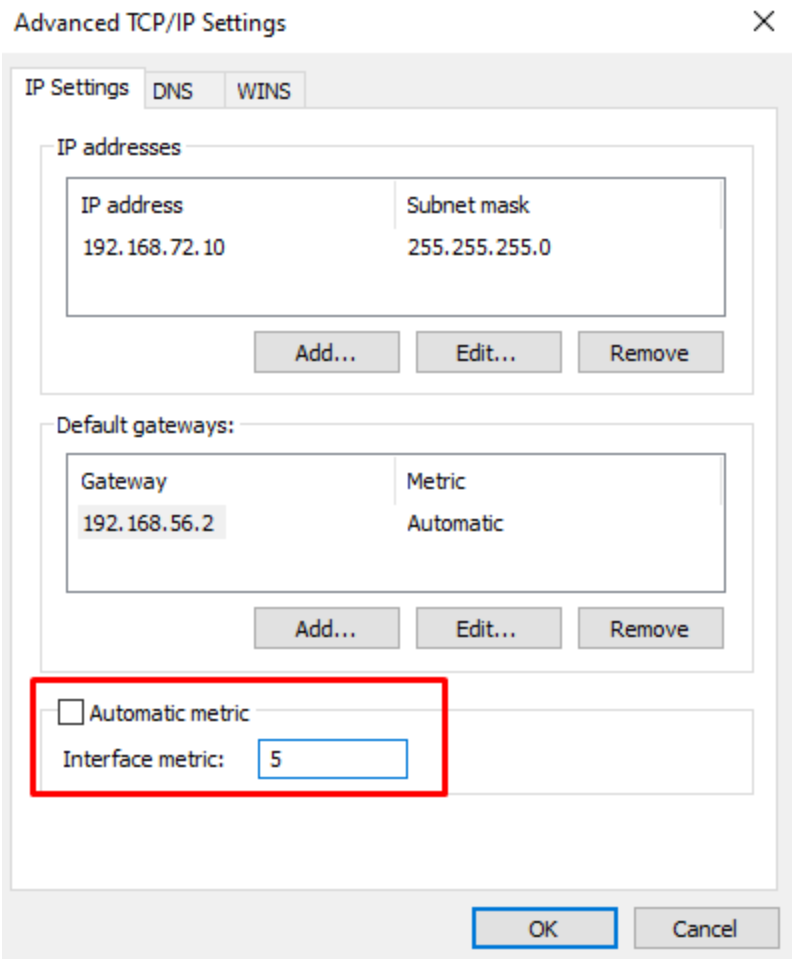
Windows Server 2022: Configure Both NAT and Host Networks

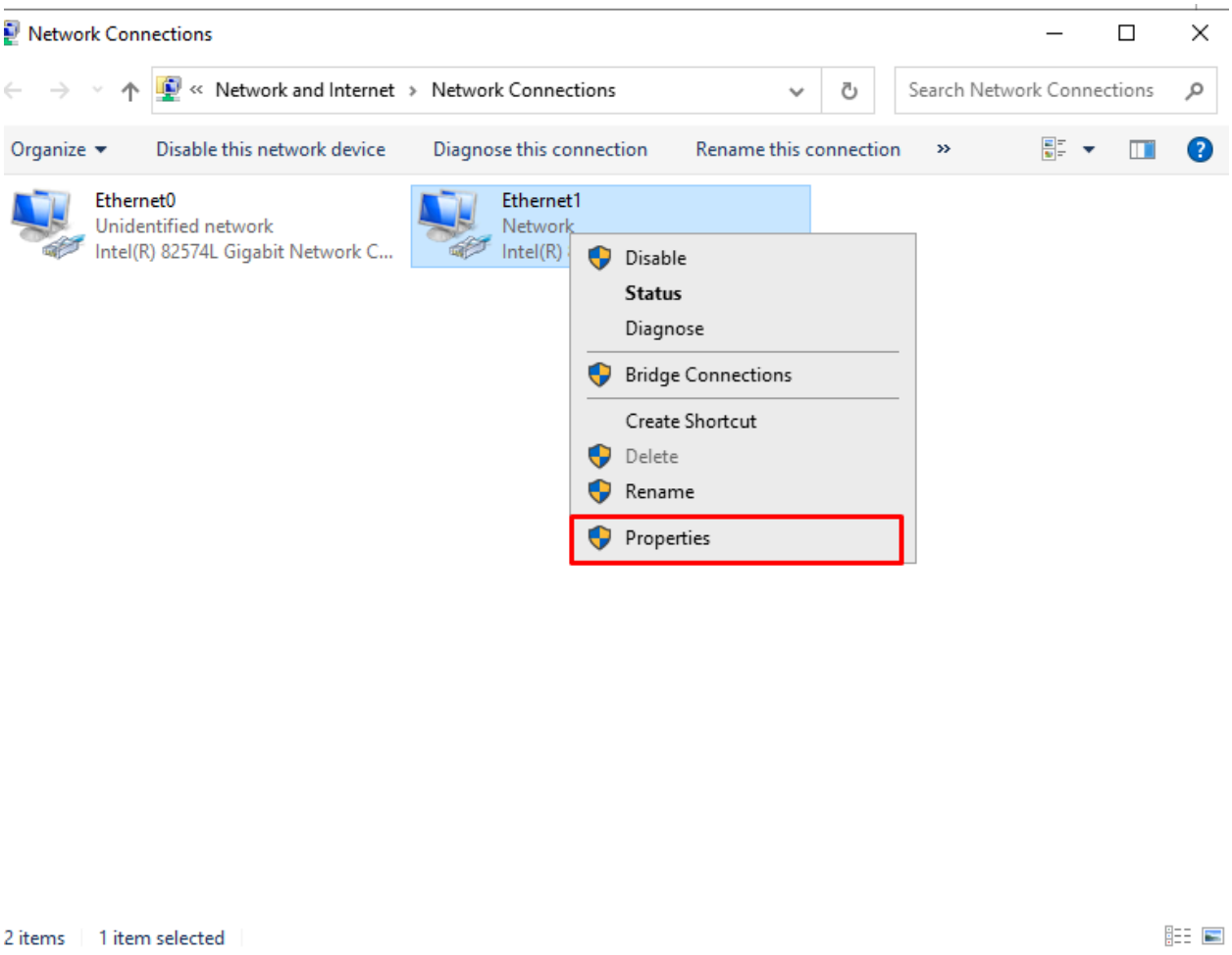


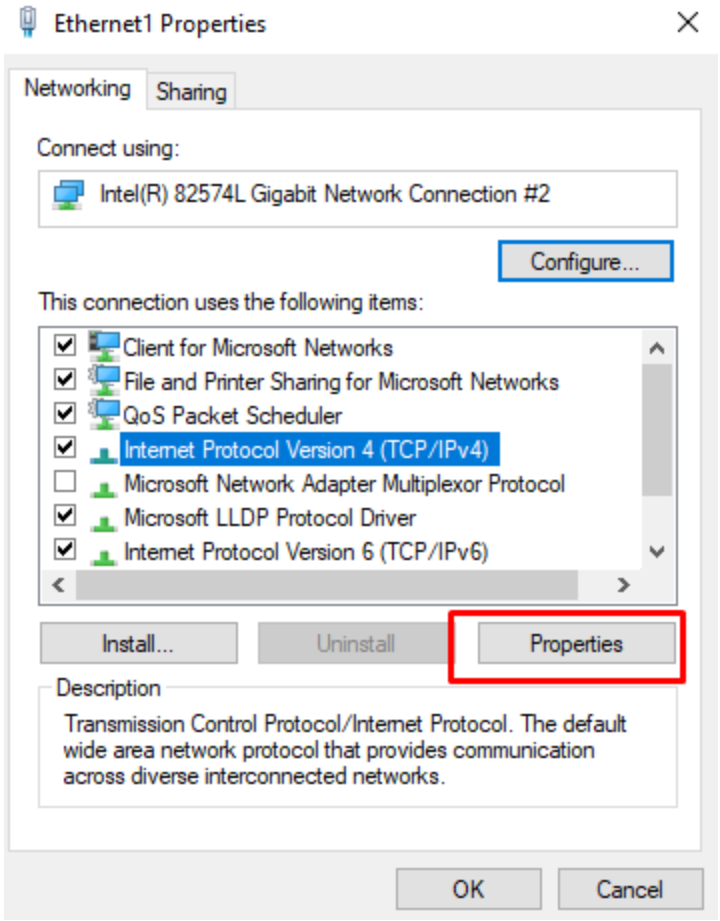

Network Connections
Network and Internet › Network Connections
Search Network Connections
Organize
Disable this network device
Diagnose this connection
Rename this connection
Ethernet0
Unidentified network
Intel(R) 82574L G
Ethernet1
Network
2574L Gigabit Network C...
Disable
Status
Diagnose
Bridge Connections
Create Shortcut
Delete
Rename
Properties
2 items
1 item selected

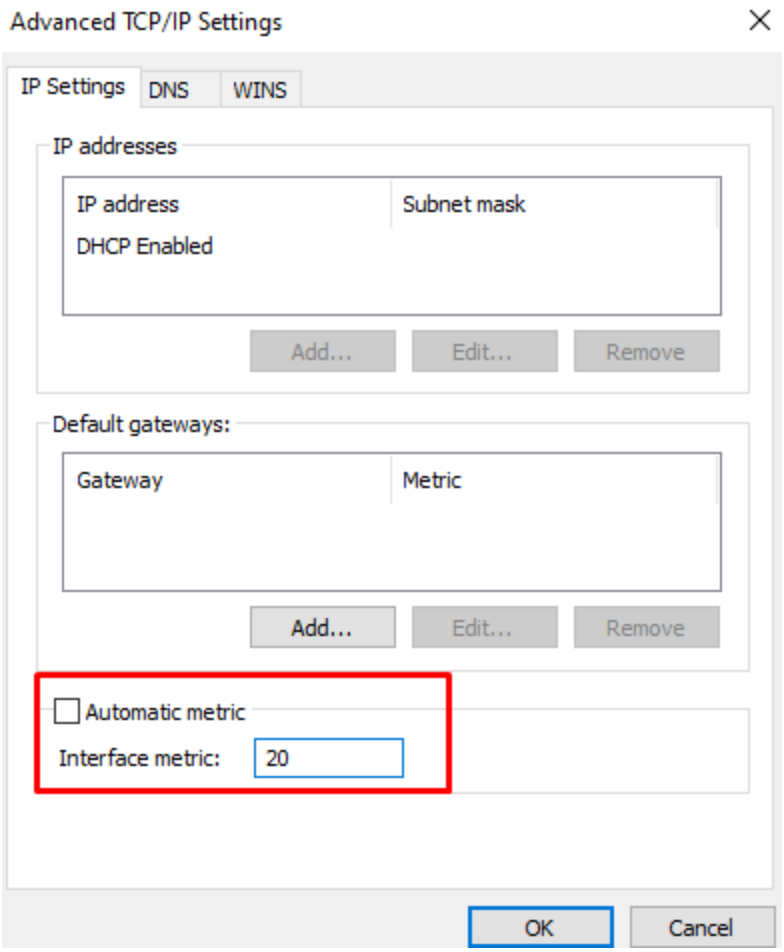

Organize
Disable this network device
Diagnose this conn
Ethernet0 Properties
Networking
Sharing
Connect using:
Intel(R) 82574L Gigabit Network Connection
Configure...
This connection uses the following items:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
QoS Packet Scheduler
Internet Protocol Version 4 (TCP/IPv4)
Microsoft Network Adapter Multiplexor Protocol
Microsoft LLDP Protocol Driver
Internet Protocol Version 6 (TCP/IPv6)
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
OK
Cancel


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:
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
127 . 0 . 0 . 1
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel


Advanced TCP/IP Settings
IP Settings
DNS
WINS
IP addresses
IP address
Subnet mask
192.168.72.10
255.255.255.0
Add...
Edit...
Remove
Default gateways:
Gateway
Metric
192.168.56.2
Automatic
Add...
Edit...
Remove
Automatic metric
Interface metric:
5
OK
Cancel


Network Connections
Network and Internet
Network Connections
Search Network Connections
Organize
Disable this network device
Diagnose this connection
Rename this connection
Ethernet0
Unidentified network
Intel(R) 82574L Gigabit Network C...
Ethernet1
Network
Intel(R)
Disable
Status
Diagnose
Bridge Connections
Create Shortcut
Delete
Rename
Properties
2 items
1 item selected

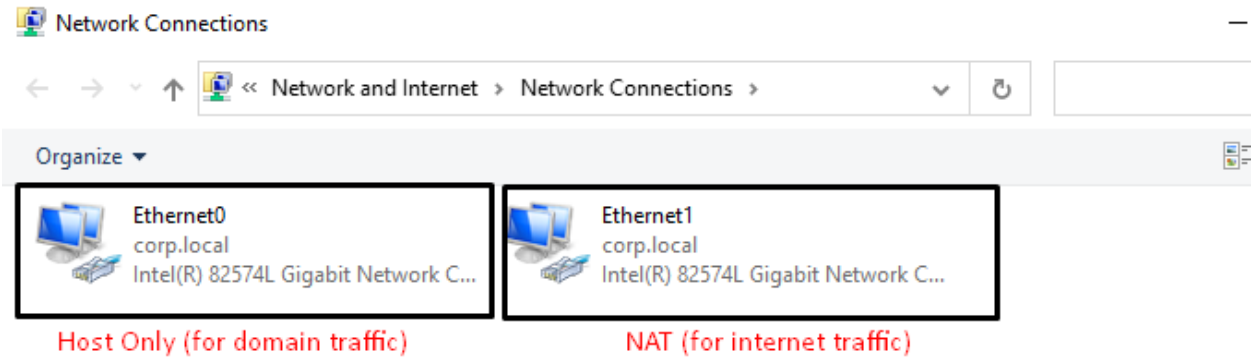

Ethernet1 Properties
Networking
Sharing
Connect using:
Intel(R) 82574L Gigabit Network Connection #2
Configure...
This connection uses the following items:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
QoS Packet Scheduler
Internet Protocol Version 4 (TCP/IPv4)
Microsoft Network Adapter Multiplexor Protocol
Microsoft LLDP Protocol Driver
Internet Protocol Version 6 (TCP/IPv6)
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
OK
Cancel



Windows uses Interface Metrics to decide which adapter to prefer:

- Lower number = preferred.
- Higher number = fallback.

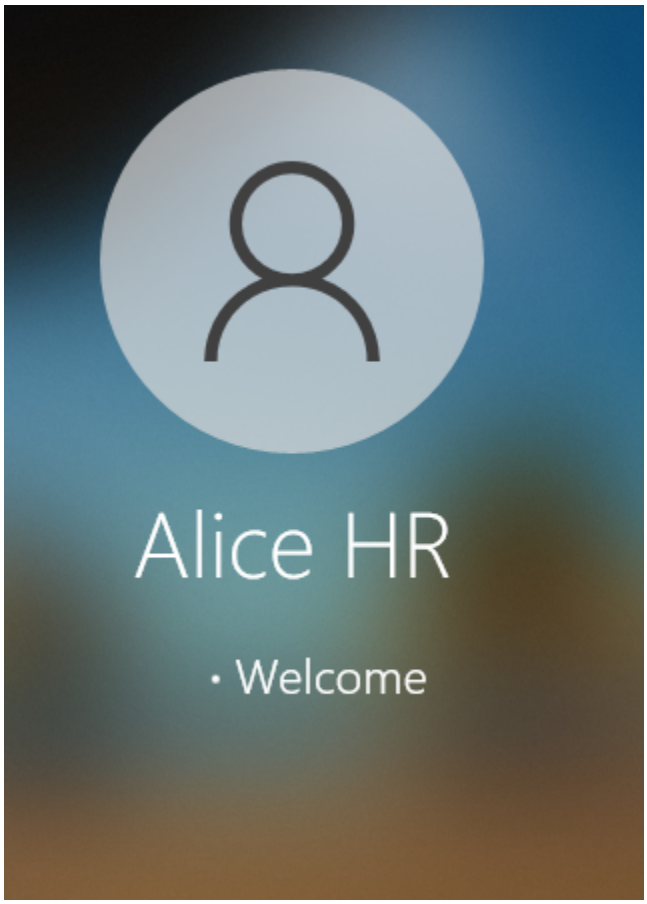
Host-Only (for domain traffic) = **lower metric (5)**.
NAT (for internet traffic) = **higher metric (20)**.



Successfully Created and Configured:

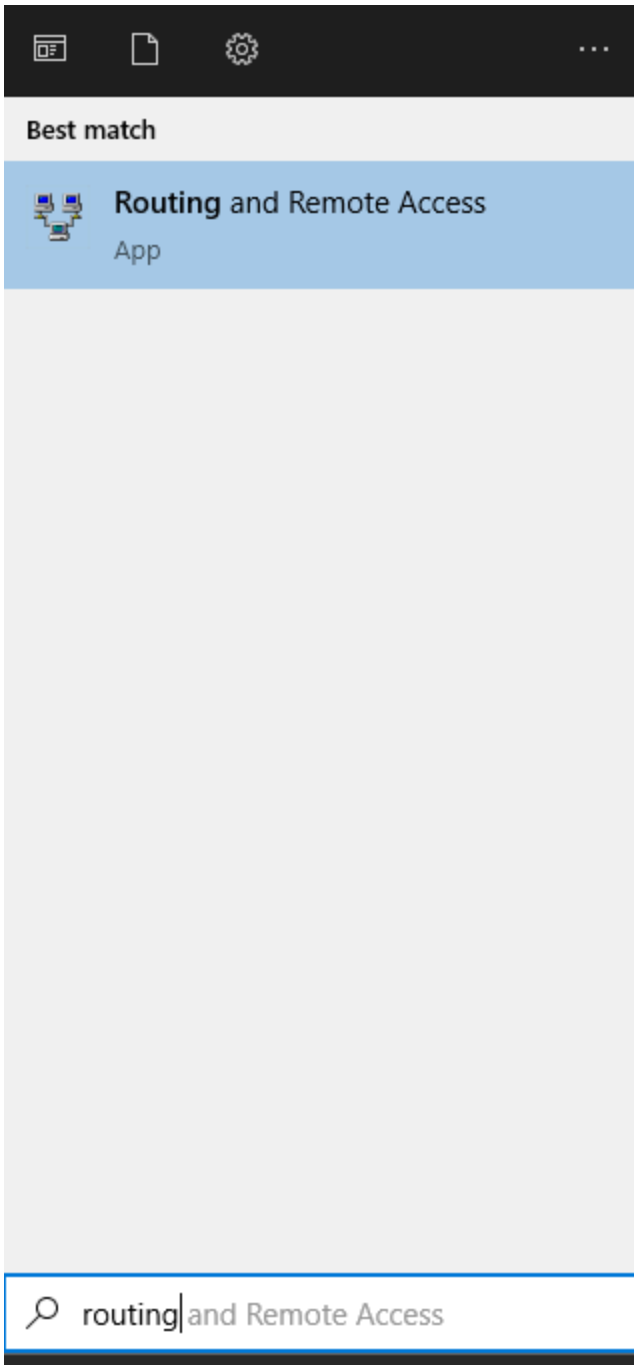
- Domain Controller traffic (corp.local, DNS, LDAP) = Host-Only adapter.
- Internet traffic = NAT adapter.

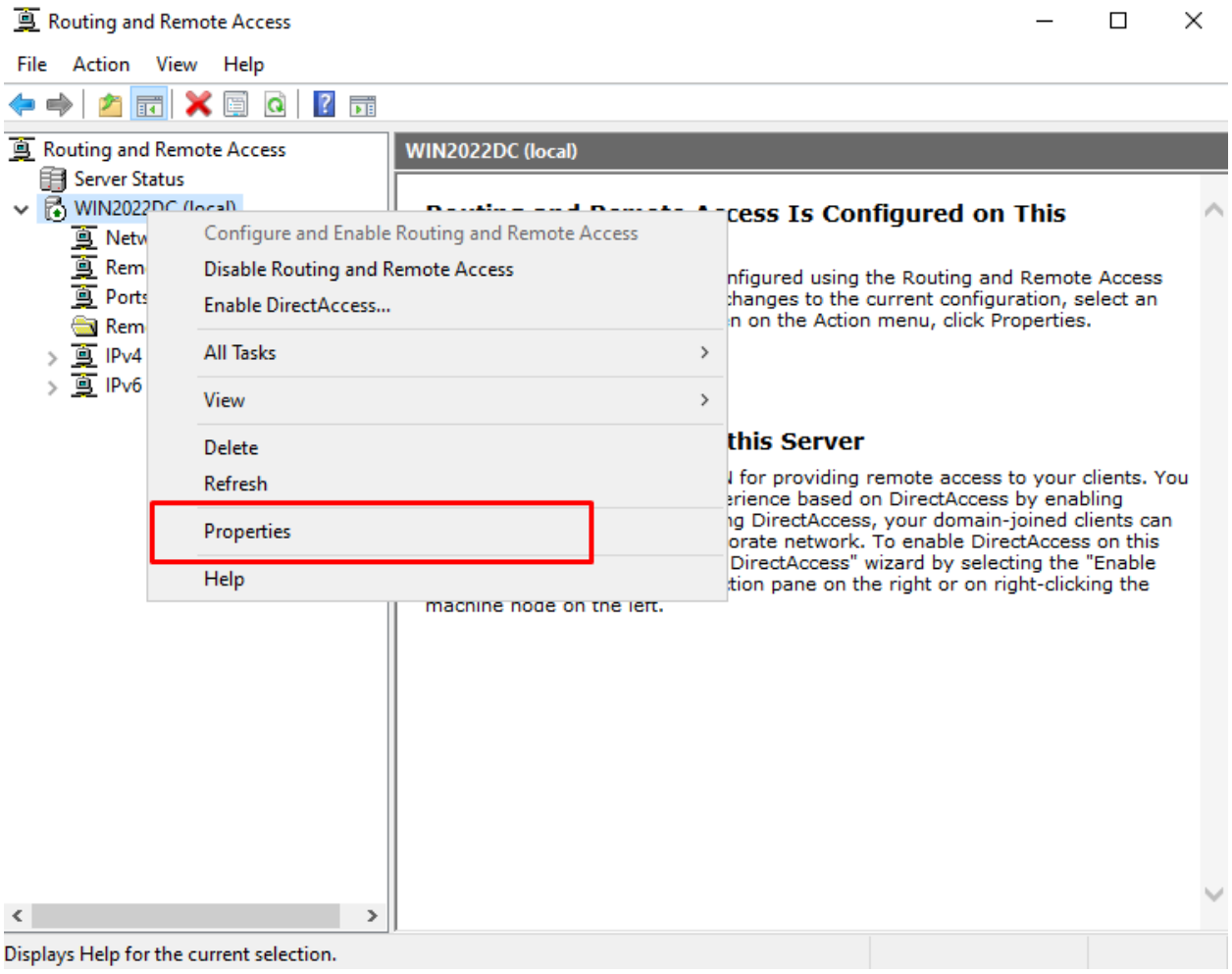
Repeat Above Steps for Windows 10 VM:

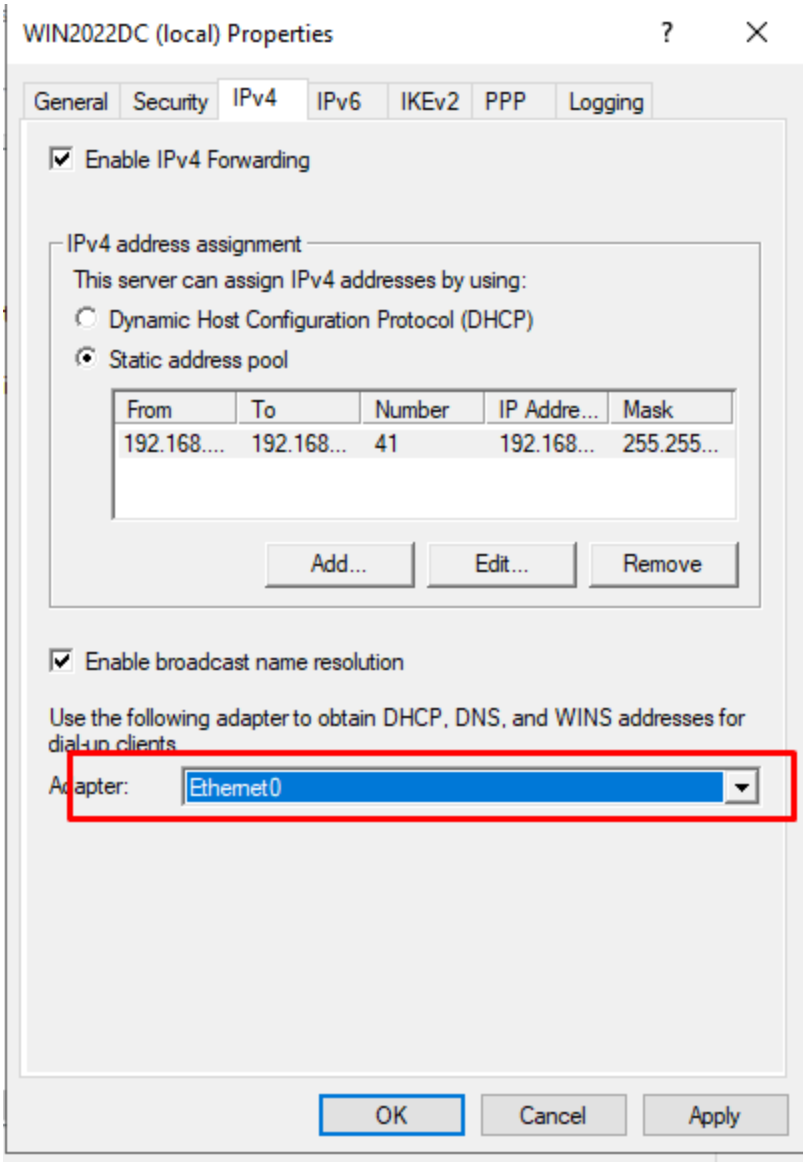


Configure VPN with newly added network:

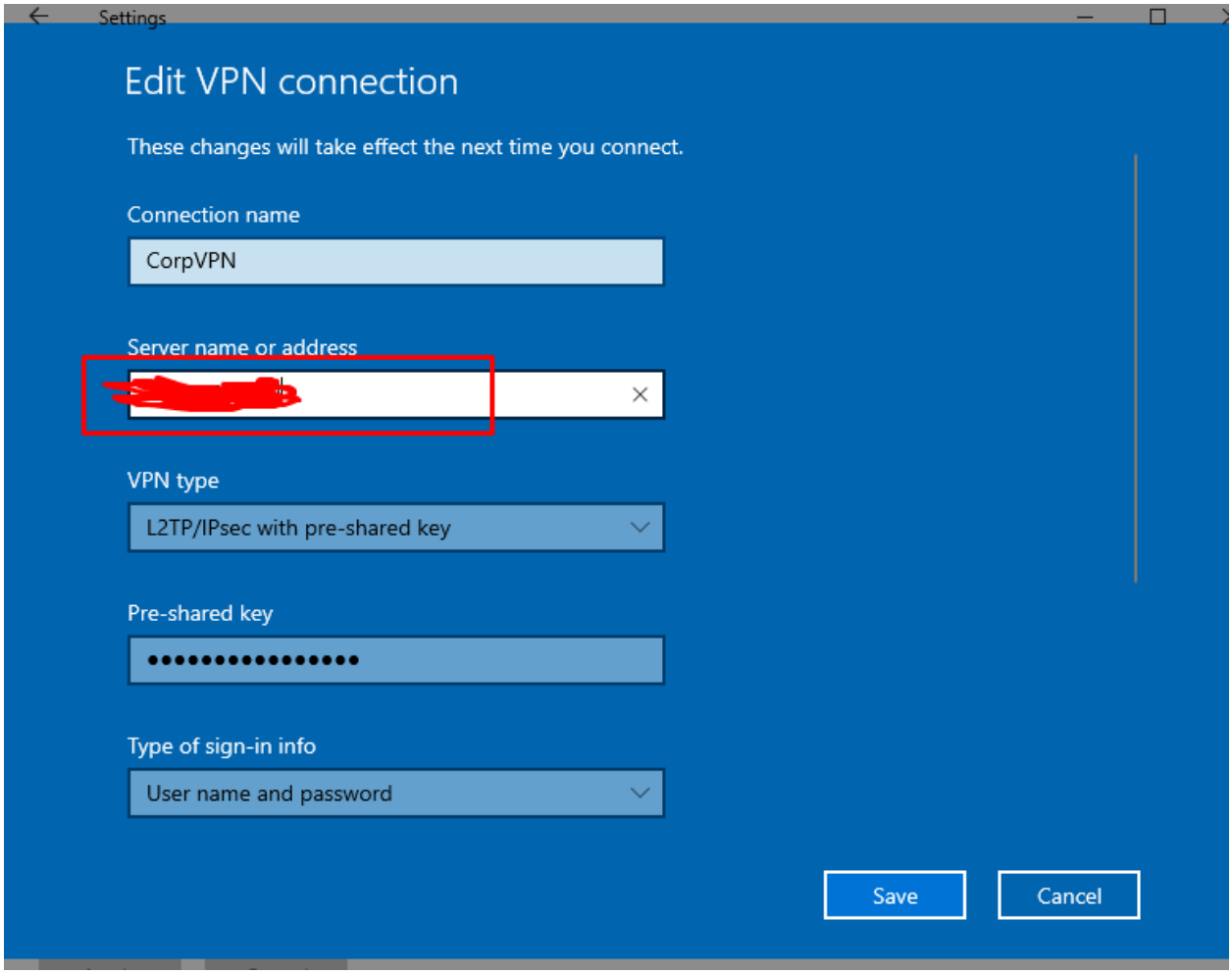
Go on windows server 2022

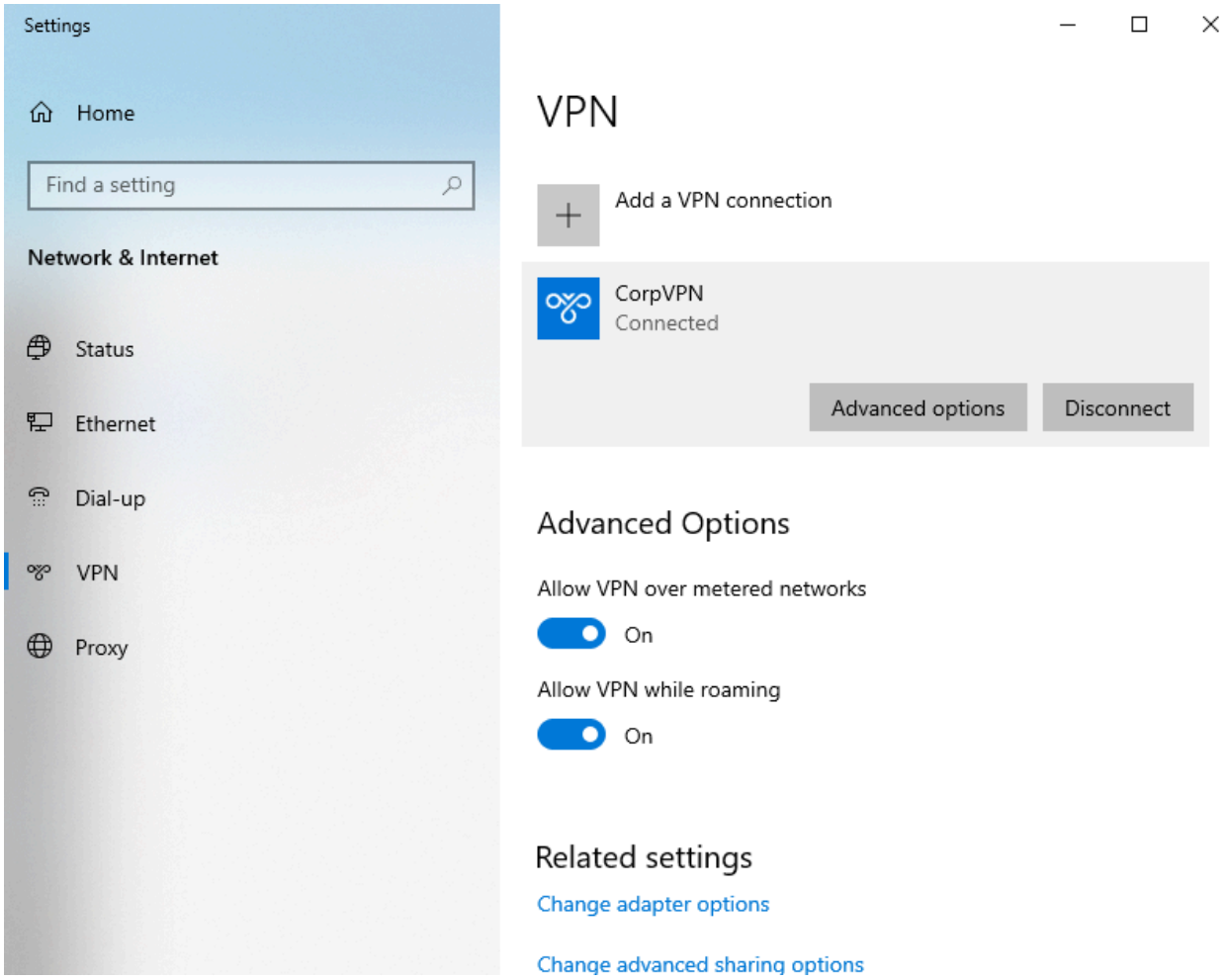



Routing and Remote Access
File Action View Help
Routing and Remote Access
Server Status
WIN2022DC (local)
Netw
Rem
Ports
Rem
IPv4
IPv6
WIN2022DC (local)
Configure and Enable Routing and Remote Access
Disable Routing and Remote Access
Enable DirectAccess...
All Tasks
View
Delete
Refresh
Properties
Help
cess Is Configured on This
nfigured using the Routing and Remote Access
hanges to the current configuration, select an
n on the Action menu, click Properties.
this Server
for providing remote access to your clients. You
erience based on DirectAccess by enabling
g DirectAccess, your domain-joined clients can
orate network. To enable DirectAccess on this
DirectAccess" wizard by selecting the "Enable
tion pane on the right or on right-clicking the
machine node on the left.
Displays Help for the current selection.


WIN2022DC (local) Properties
General
Security
IPv4
IPv6
IKEv2
PPP
Logging
Enable IPv4 Forwarding
IPv4 address assignment
This server can assign IPv4 addresses by using:
Dynamic Host Configuration Protocol (DHCP)
Static address pool
From
To
Number
IP Addre...
Mask
192.168....
192.168...
41
192.168...
255.255...
Add...
Edit...
Remove
Enable broadcast name resolution
Use the following adapter to obtain DHCP, DNS, and WINS addresses for dial-up clients
Adapter:
Ethernet0
OK
Cancel
Apply

Go to Windows 10 VM:





VPN successful on the newly created Host-only and NAT network.