VIET NAM NATIONAL UNIVERSITY - HCMC

UNIVERSITY OF INFORMATION TECHNOLOGY

FACULTY OF NETWORKS AND COMMUNICATIONS

UIT

Tran Phuc Hoang Duy – 21522011

Ly The Nguyen – 21522389

Le Trieu Vi - 21522785

FINAL REPORT

Subject: Network and System Administration

Class: NT132.O12.ATCL

DEPLOY WINDOWS SERVER REMOTE ACCESS - VPN

Lecturer: MSc Tran Thi Dung

HO CHI MINH CITY, 2023

Contents

I. INTRODUCTION

1.1 General Information

- ***Overview***

A remote access virtual private network (VPN) enables users to connect to a private network remotely using a VPN. Employees who need to access their company's network from off-site locations or people who want to securely connect to a private network from a public area frequently use this kind of VPN.

Different types of remote access VPNs exist, each using its own protocols to encrypt and tunnel data sent over the internet. This prevents unauthorized users from connecting to private networks. Once connected, users have full access to all of your network's resources, just as if they are connected on-premises.

- ***Protocols***

There are several common VPN protocols widely known:

- OpenVPN: OpenVPN is known for its trong security features. It supports various encryption algorithms and is highly configurable.
- IPSec (Internet Protocol Security): IPSec provides robust security and is often used in site-to-site VPNs. It can use various encryption and authentication methods.
- L2TP/IPSec (Layer 2 Tunneling Protocol with IPSec): L2TP/IPSec combines the tunneling capabitlities of L2TP with the security of IPSec. It’s a widely used protocol for securing communications.
- PPTP (Point-to-Point Tunneling Protocol): PPTP is known for its speed but is considered less secure due to vulnerabilities. It’s often used when speed is a priority but security requirements are lower.
- SSTP (Secure Socket Tunneling Protocol): SSTP is designed to provide a secure connection over the SSL/TLS protocol, making it highlt secure.

- IKEv2 (Internet Key Exchange Version 2): IKEv2 offers strong security features and is often used for mobile device VPN connections.

1.2 Component

To establish the VPN connection, we'll need serveral components including the VPN server and the necessary client-side configurations. Here are the key components:

- ***Server-side components:***

- VPN Server: This is the core component that handles incoming VPN connections. The server can be a physical or virtual machine running VPN server software.
- Server Operating System: The VPN server typically runs on an operating system that supports VPN services. Common choices include Windows Server, Linux (with OpenVPN, IPsec, etc.), or dedicated VPN appliances.
- Static IP or DNS: For easy access, the server should have a static public IP address or a DNS name that clients can use to connect to it. Alternatively, dynamic DNS services can be used to maintain a DNS name for a server with a dynamic IP address.
- Authentication and User Management: Set up user accounts and authentication mechanisms (username/password, certificates, multi-factor authentication) to control who can connect to the VPN.
- VPN Protocol Configuration: Choose and configure the VPN protocol(s) we want to use, such as PPTP, L2TP, IPsec, SSTP, OpenVPN. The configuration may include encryption settings, authentication methods, and allowed IP ranges.
- Firewall and Network Rules: Configure firewall rules on the server to allow VPN traffic through to the server.

- ***Client-side components:***

- Client Device: This is the device from which we want to connect to the VPN. It could be a computer, smartphone, or tablet.
- Client Operating System: The client device should have an operating system that supports VPN connections. Common client operating systems include Windows, macOS, Linux, Android, and iOS.
- VPN Client Software: Install the appropriate VPN client software for our client device's operating system. Many operating systems have built-in VPN clients. However, for some protocols, we may need to install third-party clients.
- VPN Configuration Settings: We need the configuration details provided by the VPN server administrator. This includes the server's IP or DNS address, protocol settings, and, if applicable, username and password or certificates for authentication.
- Network Connection: Ensure that the client device has an internet connection, whether through Wi-Fi, Ethernet, or mobile data.
- Firewall Rules: If the client device is behind a firewall or router, we might need to configure port forwarding or allow outbound VPN traffic.

1.3 Operation

- **Initiation:**
  - The user initiates a connection request to access the private network remotely.
  - This request is typically made through a VPN client installed on the user's device.

- **Authentication:**
  - The VPN client sends authentication credentials (username, password, sometimes a security certificate) to the VPN server for verification.

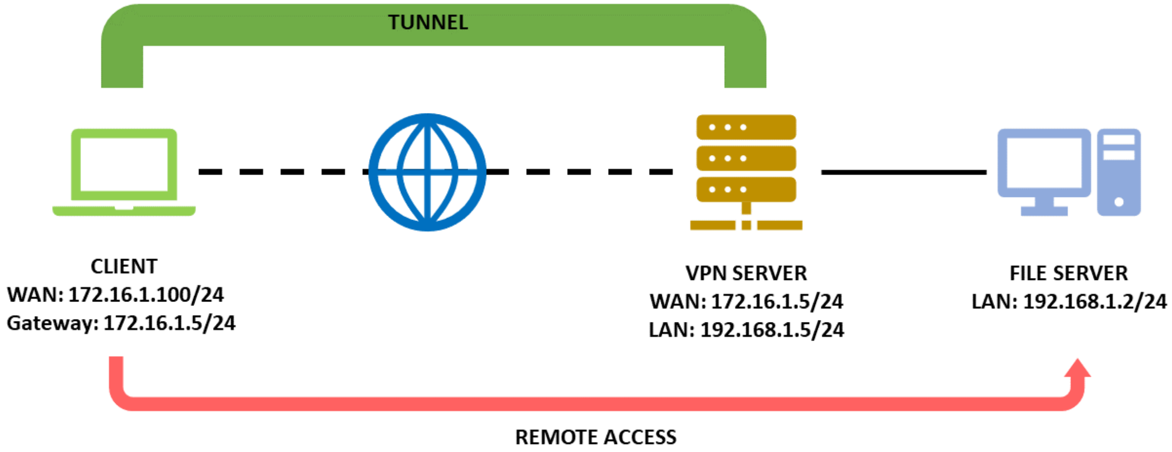
- **Secure Connection Establishment:**
  - Once authenticated, the VPN server verifies the user's credentials.
  - It then establishes an encrypted connection with the client using various protocols like PPTP, L2TP/IPsec, SSTP, or OpenVPN.

- **Tunnel Creation:**
  - A secure tunnel is created between the user's device and the private network.
  - This tunnel encrypts all data passing between the user's device and the VPN server, ensuring confidentiality.

- **Access to Resources:**
  - Once the tunnel is established, the user's device is virtually part of the private network.
  - The user can now access resources within the private network, such as files, applications, printers, or databases, as if they were physically connected to that network.

II. IMPLEMENTATION

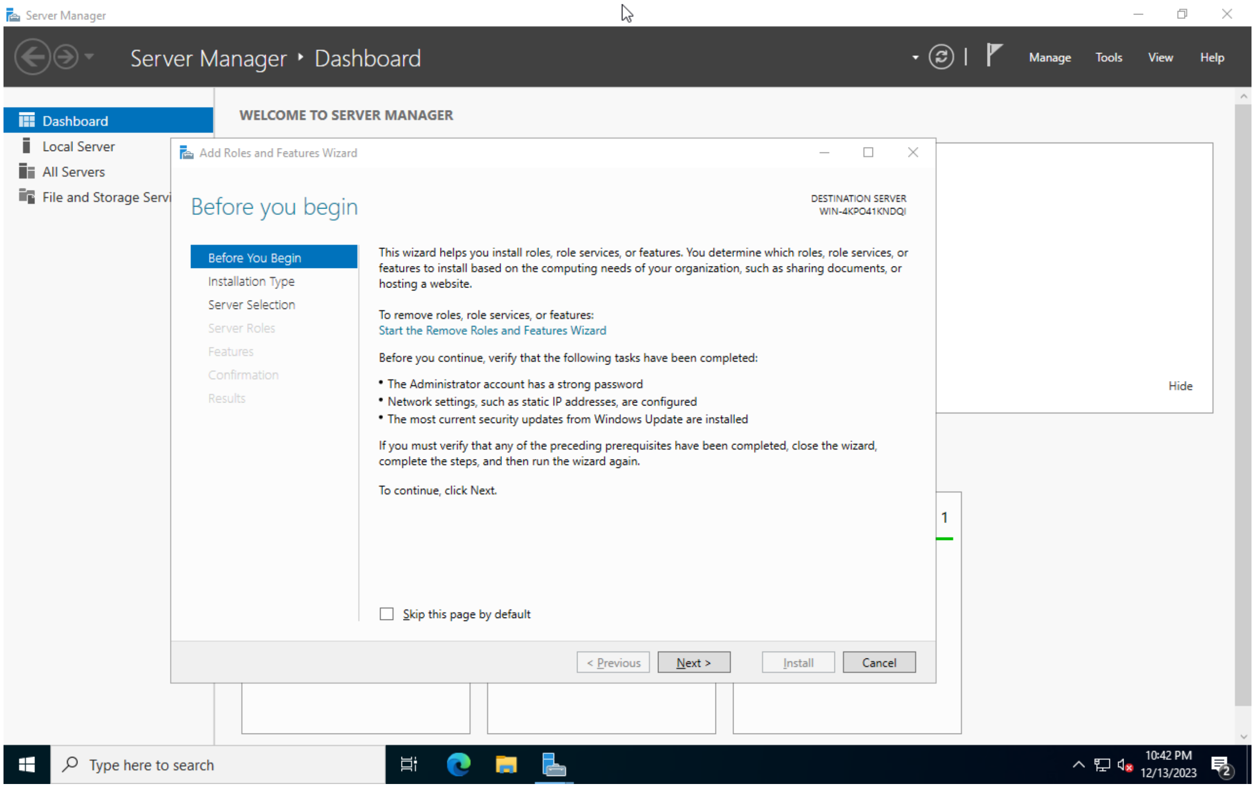
2.1 Topology



Device	IP Address	OS
Client	172.16.1.100/24	Window
VPN Server	172.16.1.5/24 192.168.1.5/24	Window Server
File Server	192.168.1.2/24	Window Server

2.2 Installation

- Install Remote Access in VPN Server.
  - Open Server Manager. Go to Add Roles and Features from the Manage dropdown menu in navigation.



Before you begin

DESTINATION SERVER
WIN-4KPO41KNDQI

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

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
Start the Remove Roles and Features Wizard

Before you continue, verify that the following tasks have been completed:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

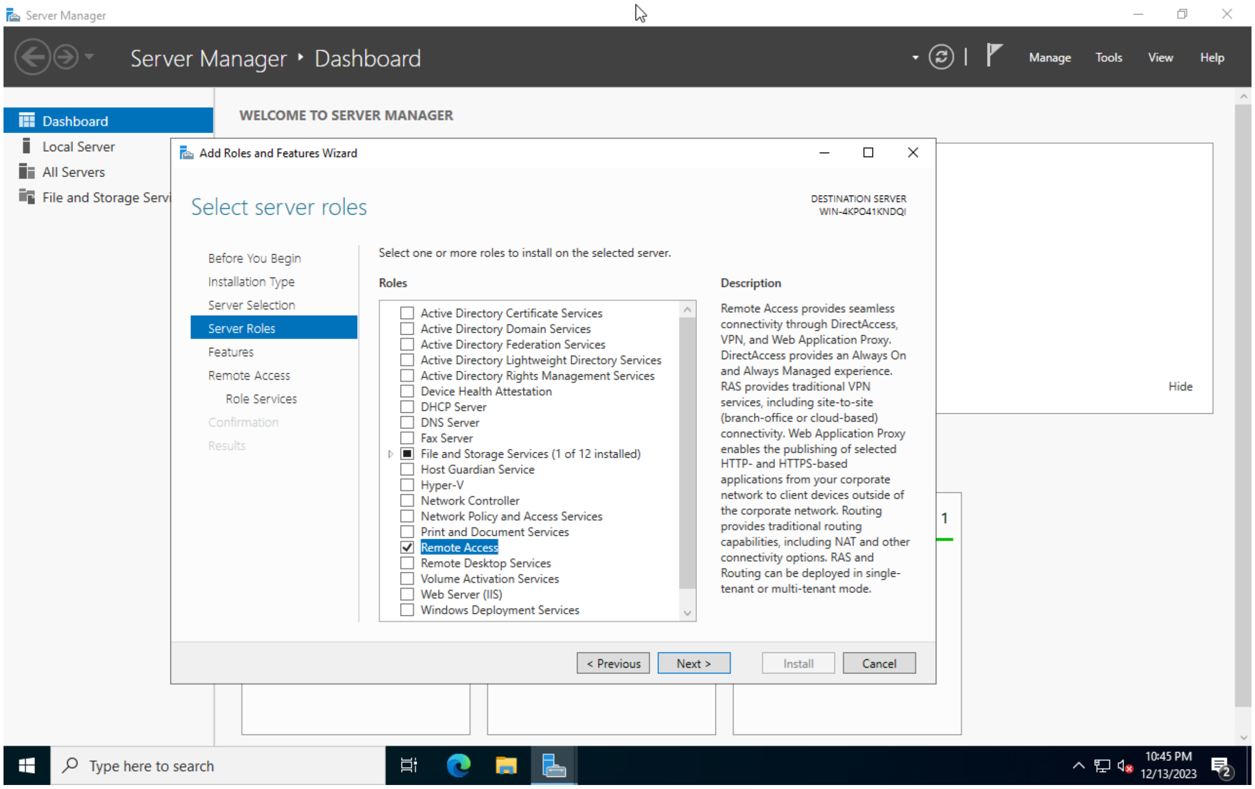
If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

□ Skip this page by default

< Previous | Next > | Install | Cancel

- Tick on Remote Access.



Select server roles

DESTINATION SERVER
WIN-4KPO41KNDQI

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Remote Access
Role Services
Confirmation
Results

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

Roles

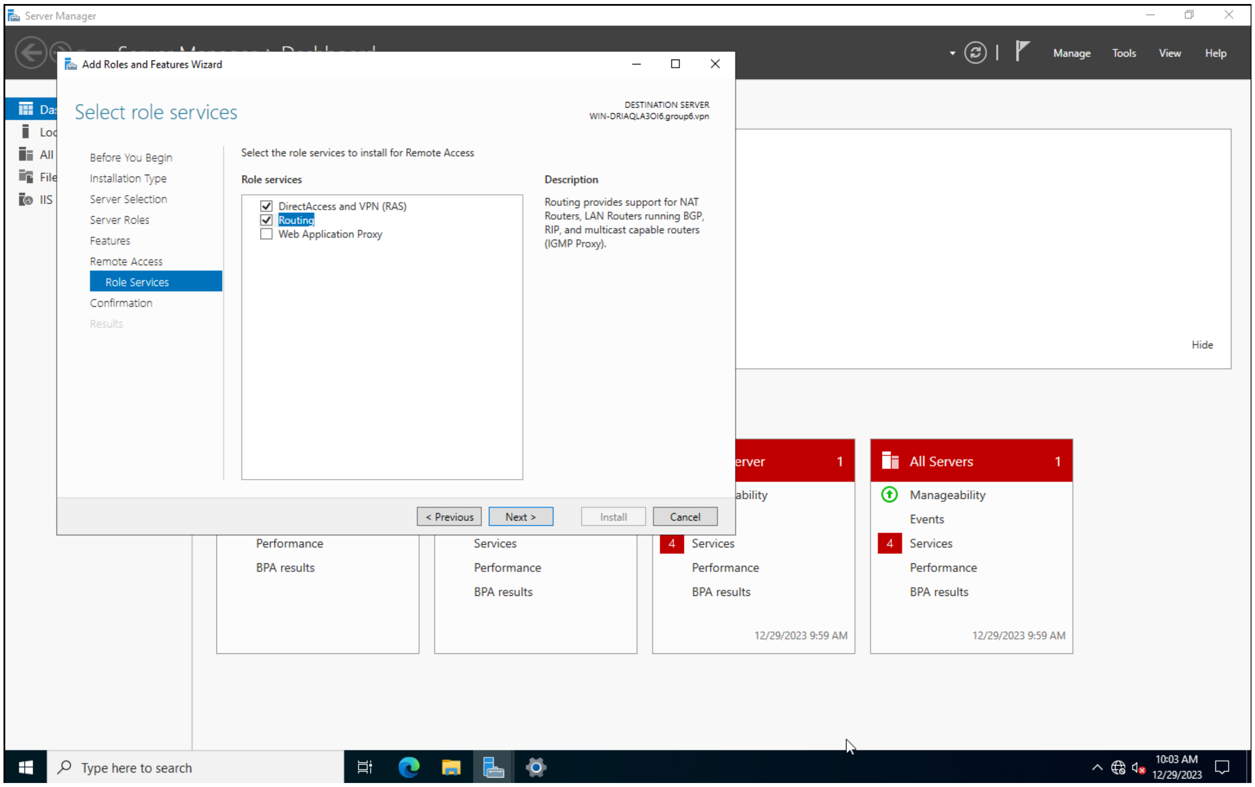
□ Active Directory Certificate Services
□ Active Directory Domain Services
□ Active Directory Federation Services
□ Active Directory Lightweight Directory Services
□ Active Directory Rights Management Services
□ Device Health Attestation
□ DHCP Server
□ DNS Server
□ Fax Server
■ File and Storage Services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

Description

Remote Access provides seamless connectivity through DirectAccess, VPN, and Web Application Proxy. DirectAccess provides an Always On and Always Managed experience. RAS provides traditional VPN services, including site-to-site (branch-office or cloud-based) connectivity. Web Application Proxy enables the publishing of selected HTTP- and HTTPS-based applications from your corporate network to client devices outside of the corporate network. Routing provides traditional routing capabilities, including NAT and other connectivity options. RAS and Routing can be deployed in single-tenant or multi-tenant mode.

< Previous | Next > | Install | Cancel

- At the Select Role Services, select “DirectAccess and VPN(RAS)” and “Routing”.



Select role services

DESTINATION SERVER
WIN-DRIAQLA3OI6.group6.vpn

Select the role services to install for Remote Access

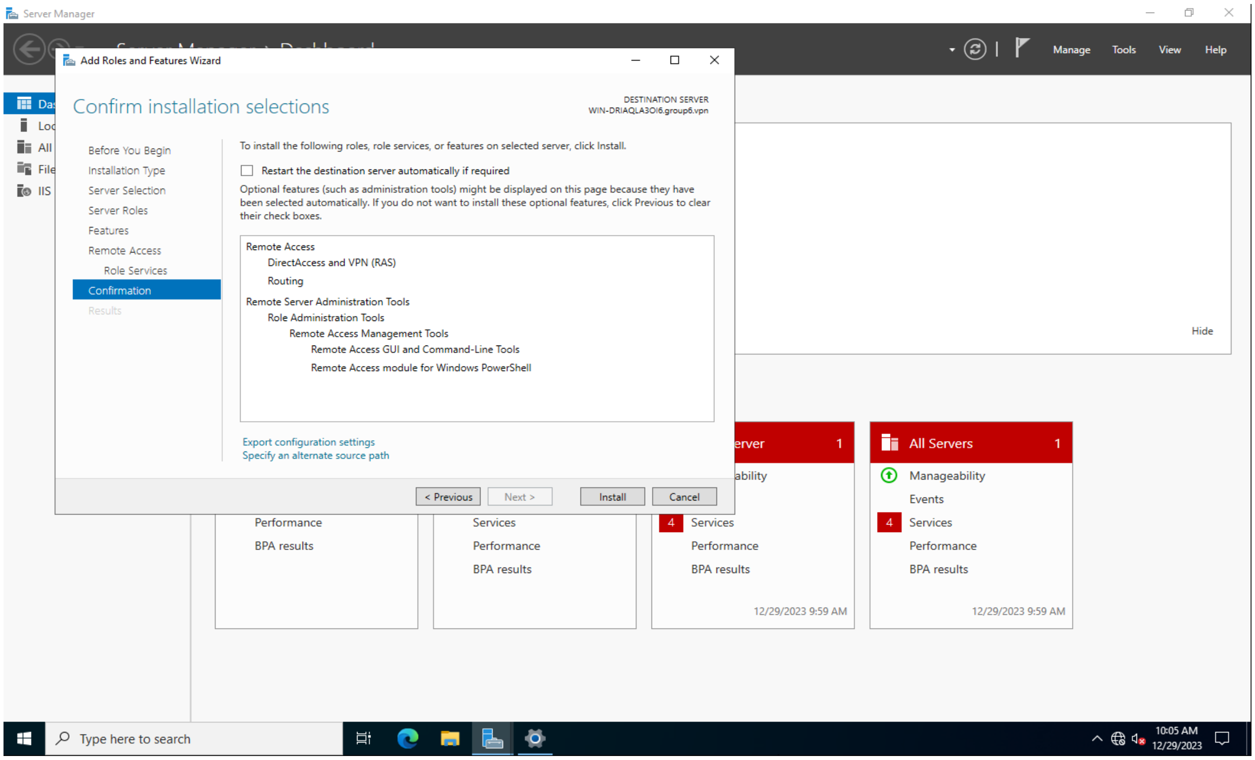
Role services

☑ DirectAccess and VPN (RAS)
☑ Routing
☐ Web Application Proxy

Description

Routing provides support for NAT Routers, LAN Routers running BGP, RIP, and multicast capable routers (IGMP Proxy).

- Click “Install”.



Confirm installation selections

DESTINATION SERVER
WIN-DRIAQLA3OI6.group6.vpn

To install the following roles, role services, or features on selected server, click Install.

☐ Restart the destination server automatically if required

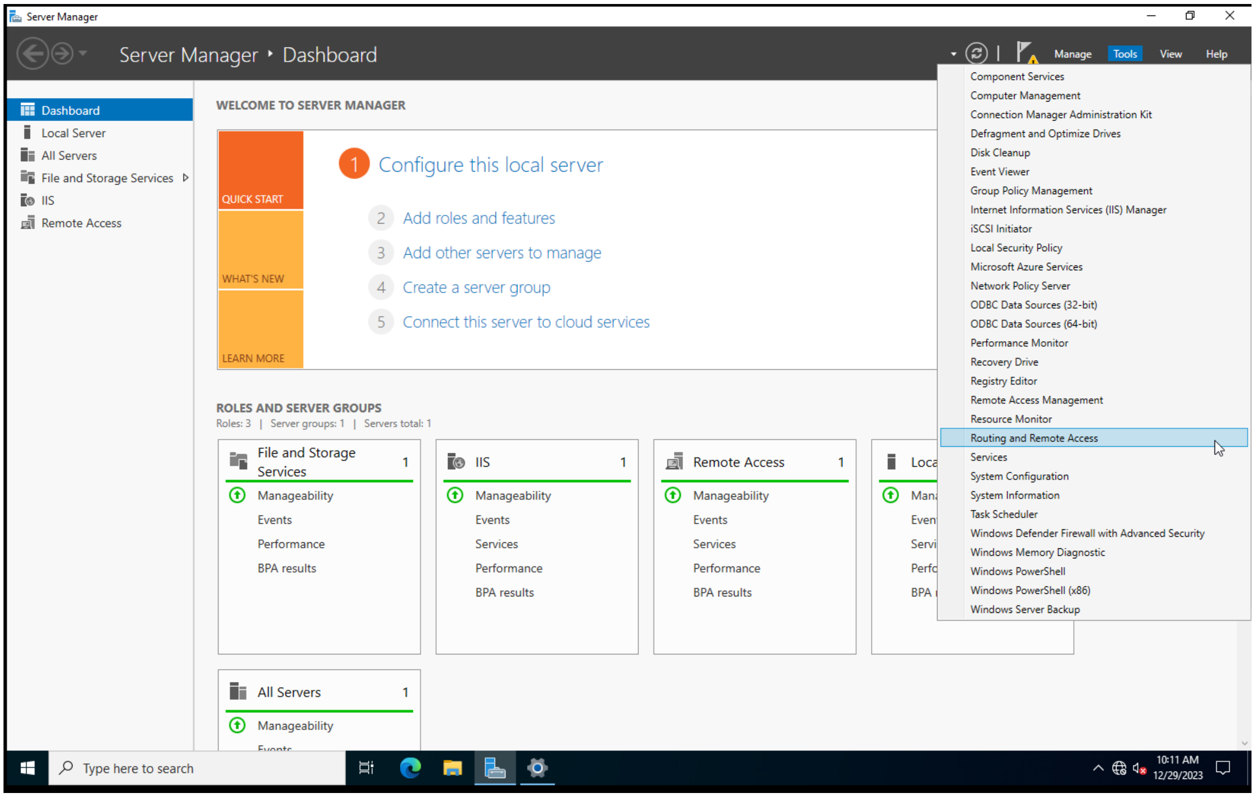
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

```
Remote Access
    DirectAccess and VPN (RAS)
    Routing
Remote Server Administration Tools
    Role Administration Tools
        Remote Access Management Tools
            Remote Access GUI and Command-Line Tools
            Remote Access module for Windows PowerShell
```

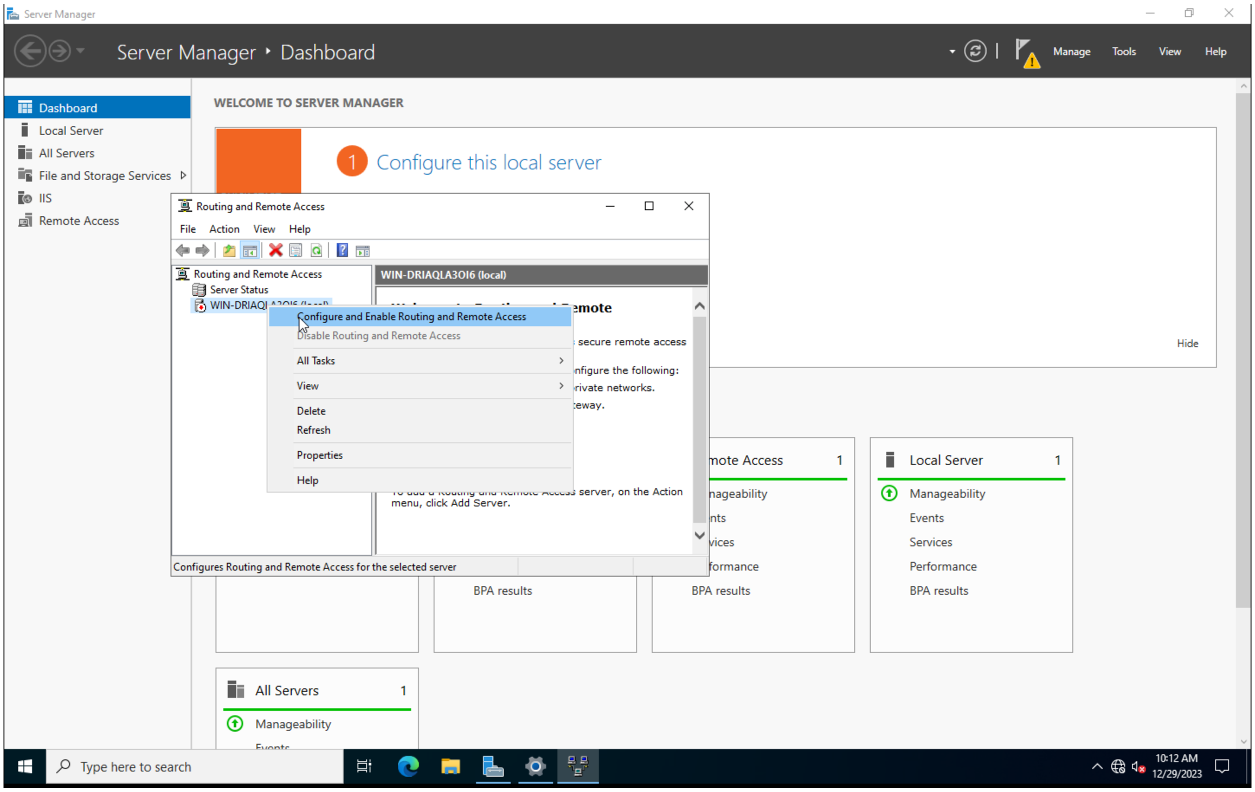
Export configuration settings
Specify an alternate source path

2.3 Configuration

- **Setting up VPN Server.**
  - Select “Tools” -> “Routing and Remote Access”.

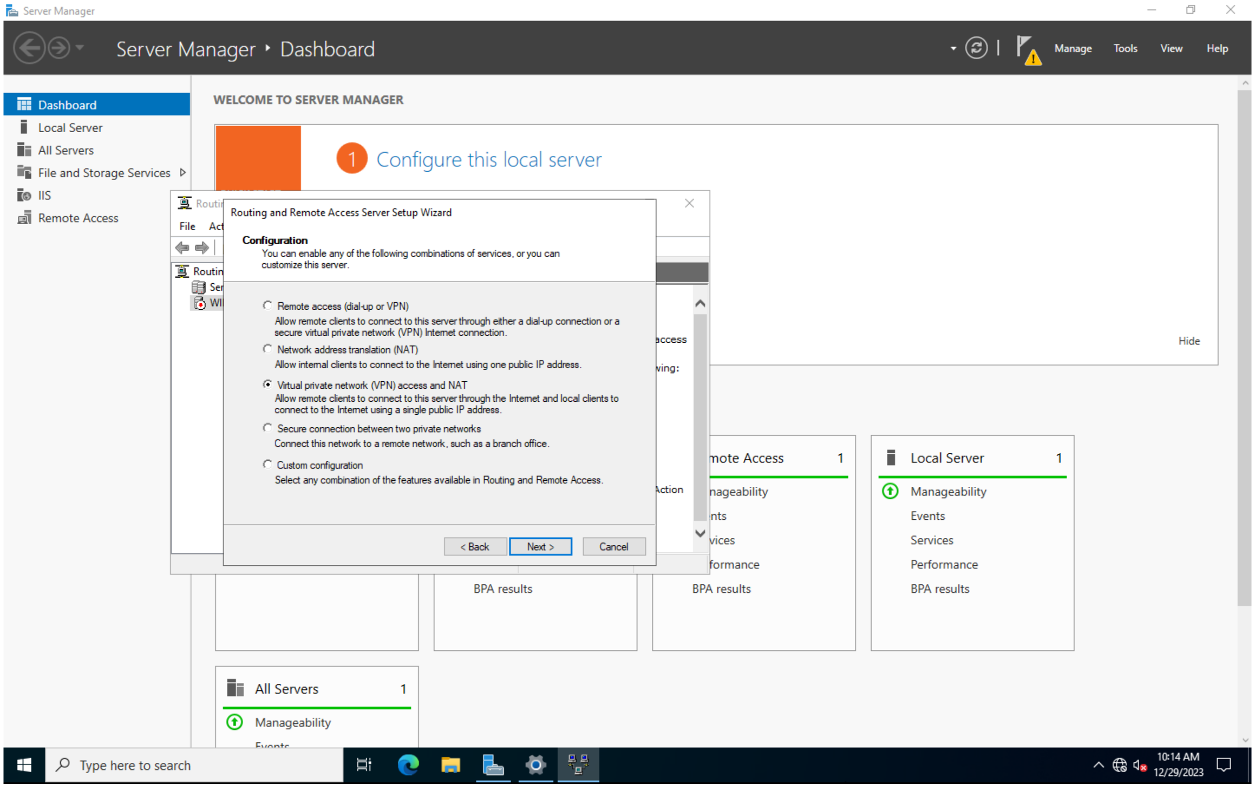


  - Right click on Server’s name then click on “Configure and Enable Routing and Remote Access”.



Configures Routing and Remote Access for the selected server

- Select “Virtual Private network (VPN) access and NAT”.



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.

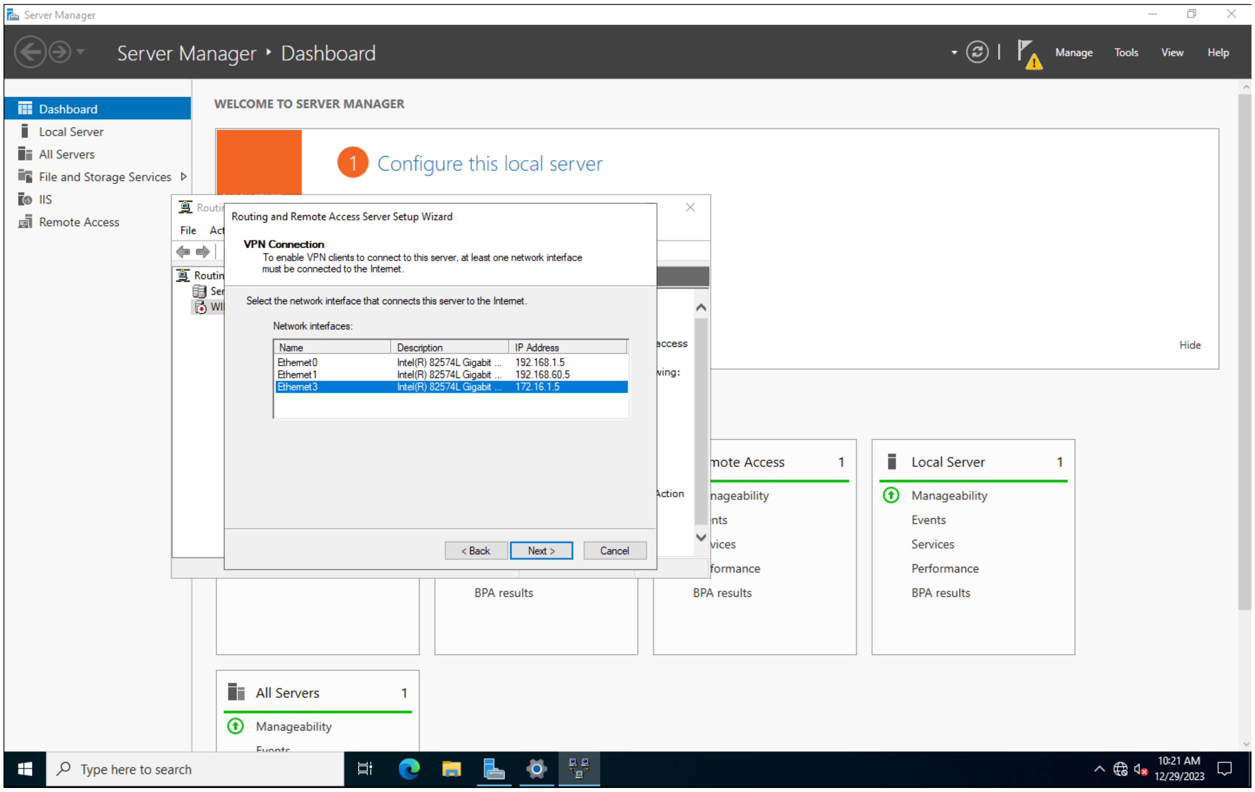
○ Network address translation (NAT)
Allow internal clients to connect to the Internet using one public IP address.

● 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.

- Choose WAN interface.



Routing and Remote Access Server Setup Wizard

VPN Connection

To enable VPN clients to connect to this server, at least one network interface must be connected to the Internet.

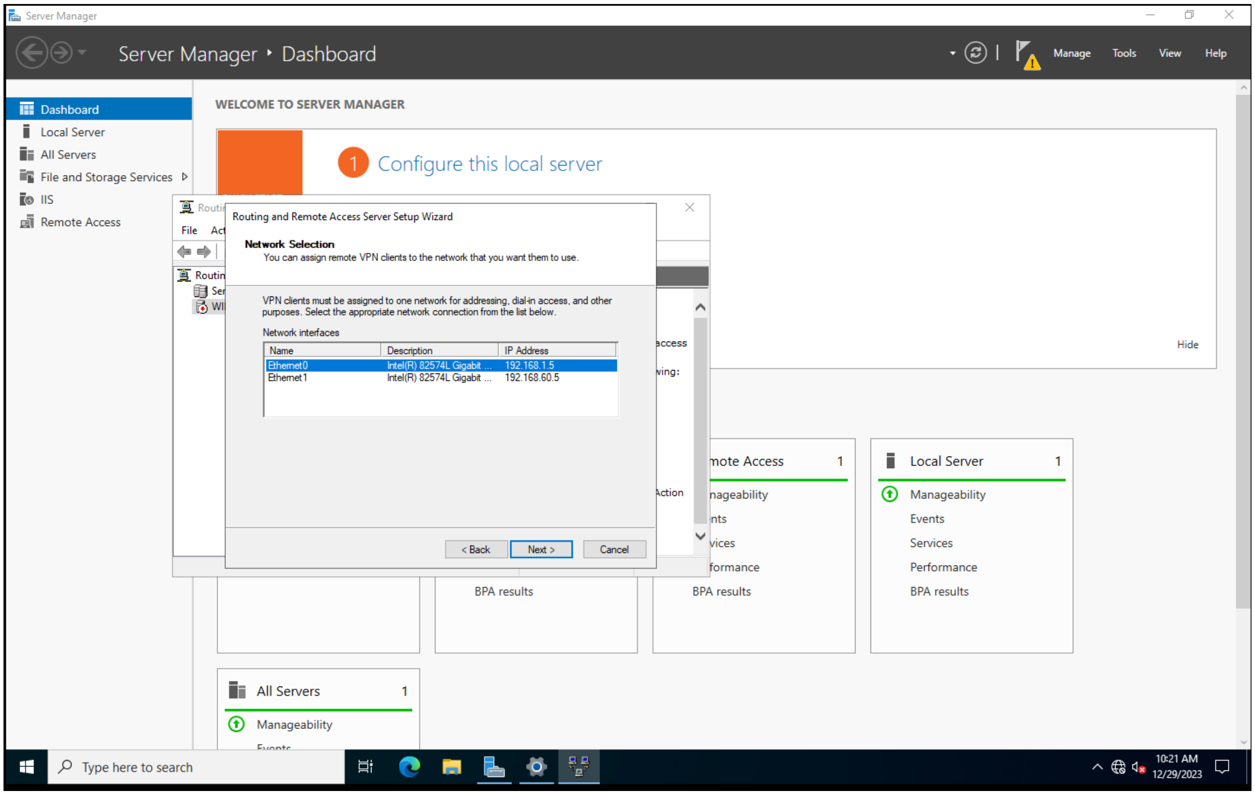
Select the network interface that connects this server to the Internet.

Network interfaces:

Name	Description	IP Address
Ethernet0	Intel(R) 82574L Gigabit ...	192.168.1.5
Ethernet1	Intel(R) 82574L Gigabit ...	192.168.60.5
Ethernet3	Intel(R) 82574L Gigabit ...	172.16.1.5

< Back | Next > | Cancel

- Choose LAN interface.



Routing and Remote Access Server Setup Wizard

Network Selection

You can assign remote VPN clients to the network that you want them to use.

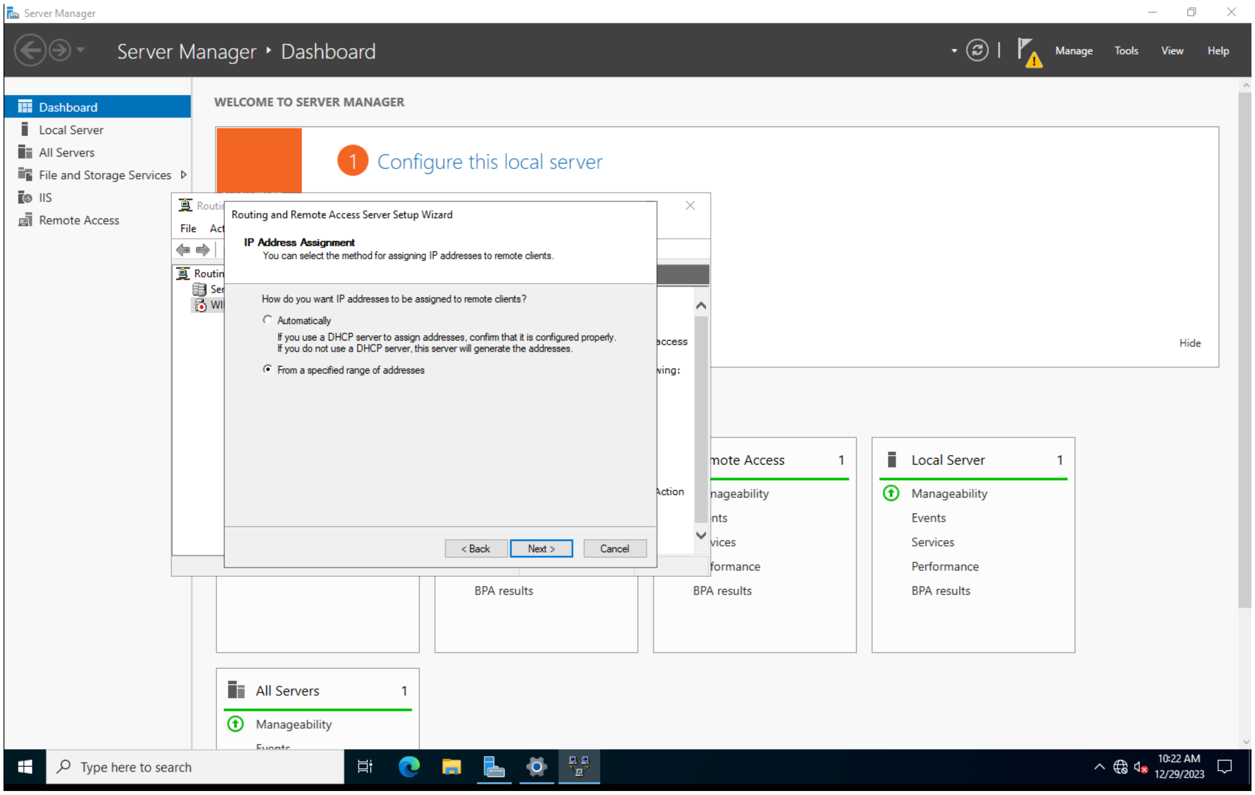
VPN clients must be assigned to one network for addressing, dial-in access, and other purposes. Select the appropriate network connection from the list below.

Network interfaces

Name	Description	IP Address
Ethernet0	Intel(R) 82574L Gigabit ...	192.168.1.5
Ethernet1	Intel(R) 82574L Gigabit ...	192.168.60.5

< Back | Next > | Cancel

- Select “From a specific IP range”.



Routing and Remote Access Server Setup Wizard

IP Address Assignment
You can select the method for assigning IP addresses to remote clients.

How do you want IP addresses to be assigned to remote clients?

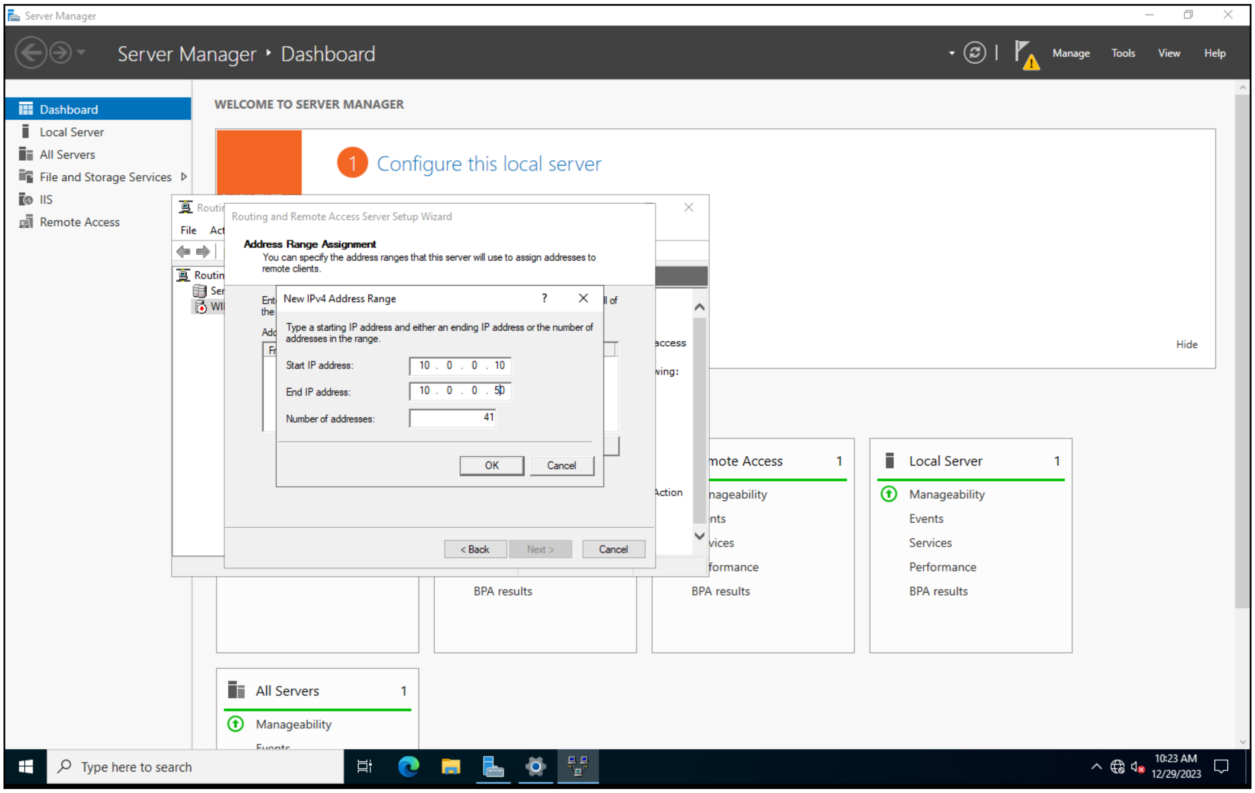
○ Automatically

If you use a DHCP server to assign addresses, confirm that it is configured properly.
If you do not use a DHCP server, this server will generate the addresses.

● From a specified range of addresses

< Back | Next > | Cancel

- Create new range by clicking “New” and entering a specific range.



Routing and Remote Access Server Setup Wizard

Address Range Assignment
You can specify the address ranges that this server will use to assign addresses to remote clients.

New IPv4 Address Range

Type a starting IP address and either an ending IP address or the number of addresses in the range.

Start IP address: 10 . 0 . 0 . 10

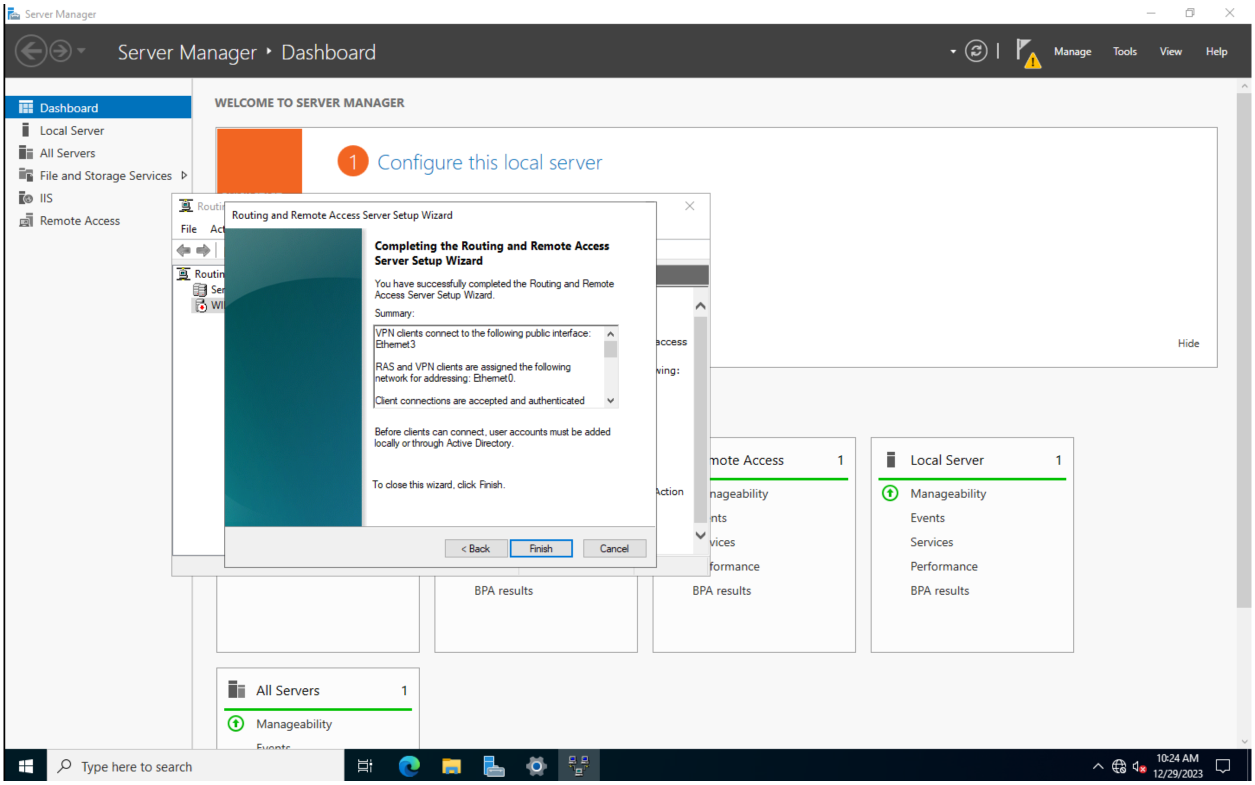
End IP address: 10 . 0 . 0 . 50

Number of addresses: 41

OK | Cancel

< Back | Next > | Cancel

- Hit “Finish”.



Routing and Remote Access Server Setup Wizard

Completing the Routing and Remote Access Server Setup Wizard

You have successfully completed the Routing and Remote Access Server Setup Wizard.

Summary:

VPN clients connect to the following public interface: Ethernet3

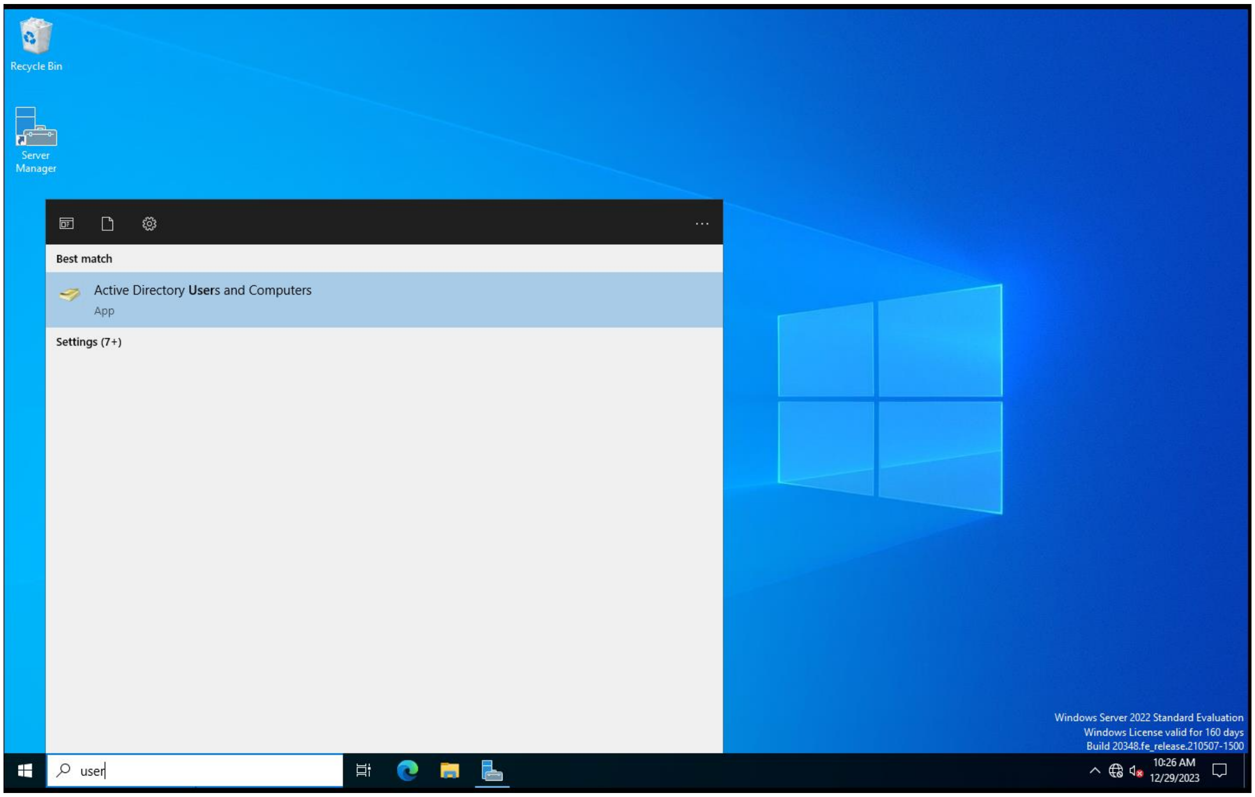
RAS and VPN clients are assigned the following network for addressing: Ethernet0.

Client connections are accepted and authenticated

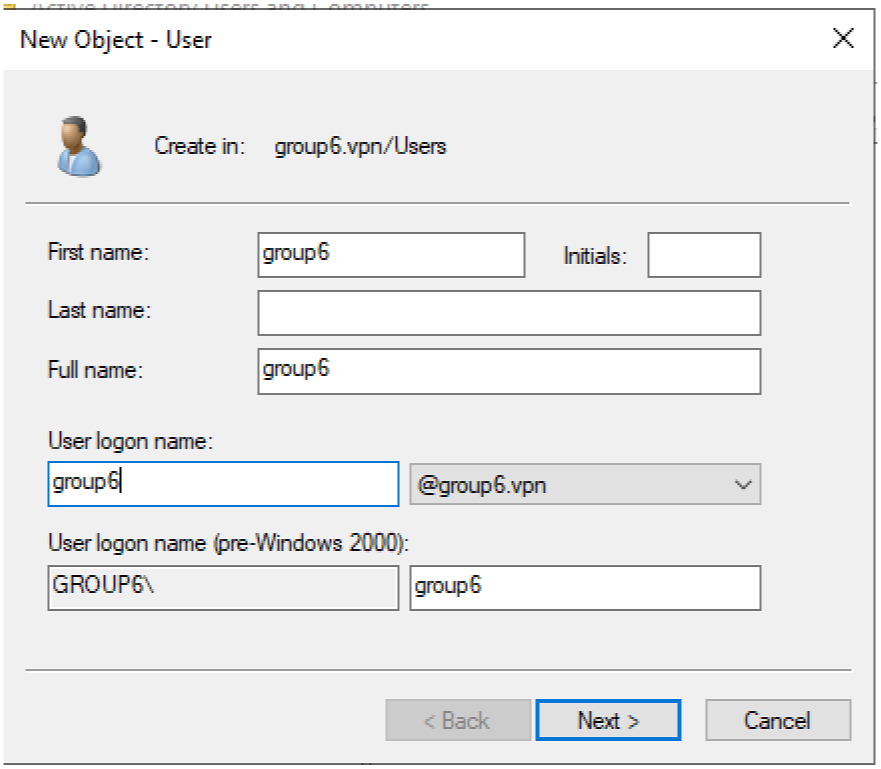
Before clients can connect, user accounts must be added locally or through Active Directory.

To close this wizard, click Finish.

- **Setting up File Server**
  - Add a new user by searching “Active directory Users and Computer”.


Recycle Bin
Server Manager
Best match
Active Directory Users and Computers
App
Settings (7+)
user
Windows Server 2022 Standard Evaluation
Windows License valid for 160 days
Build 20348.fe_release.210507-1500
10:26 AM
12/29/2023

- Right click on "User" -> "New" -> "User".
- Add credentials.


New Object - User

Create in: group6.vpn/Users

First name: group6

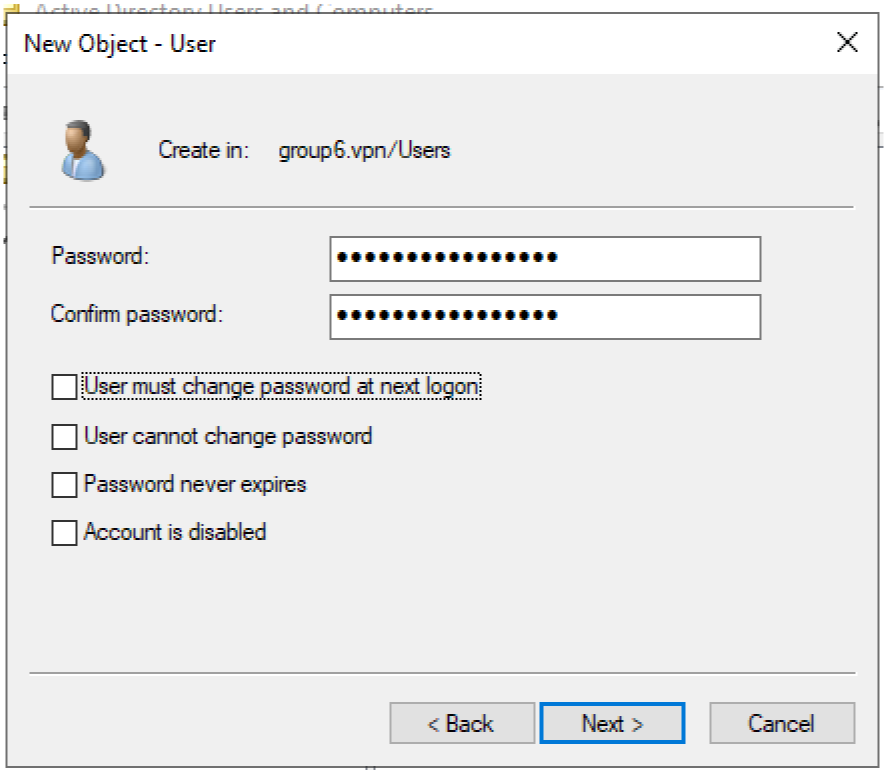
Initials:

Last name:

Full name: group6

User logon name: group6 @group6.vpn

User logon name (pre-Windows 2000): GROUP6\ group6


New Object - User

Create in: group6.vpn/Users

Password: ●●●●●●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●●●●●●

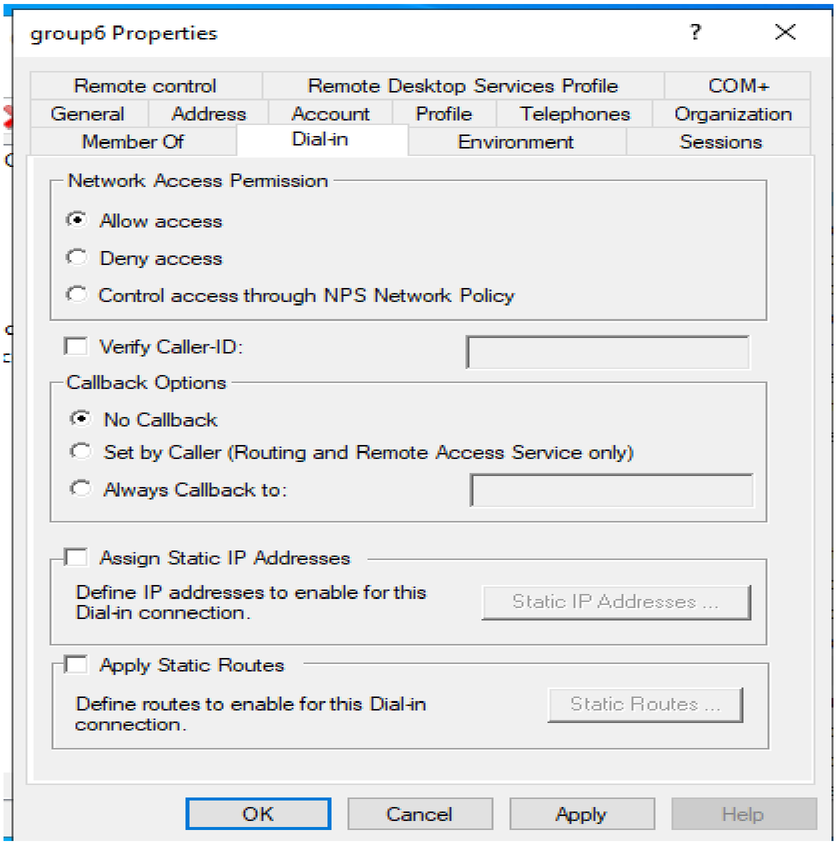
□ User must change password at next logon

□ User cannot change password

□ Password never expires

□ Account is disabled

- After finished creating new user, double click on that user and go to “Dial-in” tab then tick on “Allow access”. Finally, hit “Apply”


group6 Properties

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:

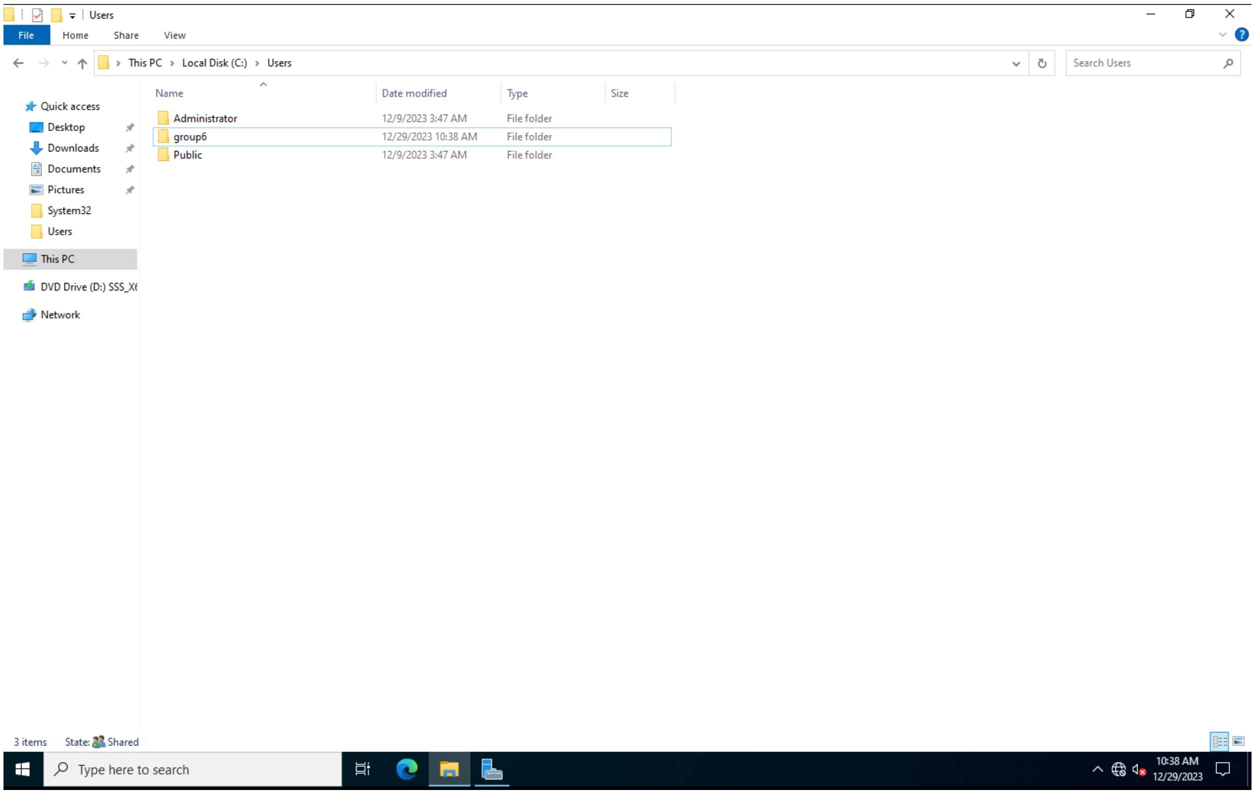
□ Assign Static IP Addresses

Define IP addresses to enable for this Dial-in connection.

□ Apply Static Routes

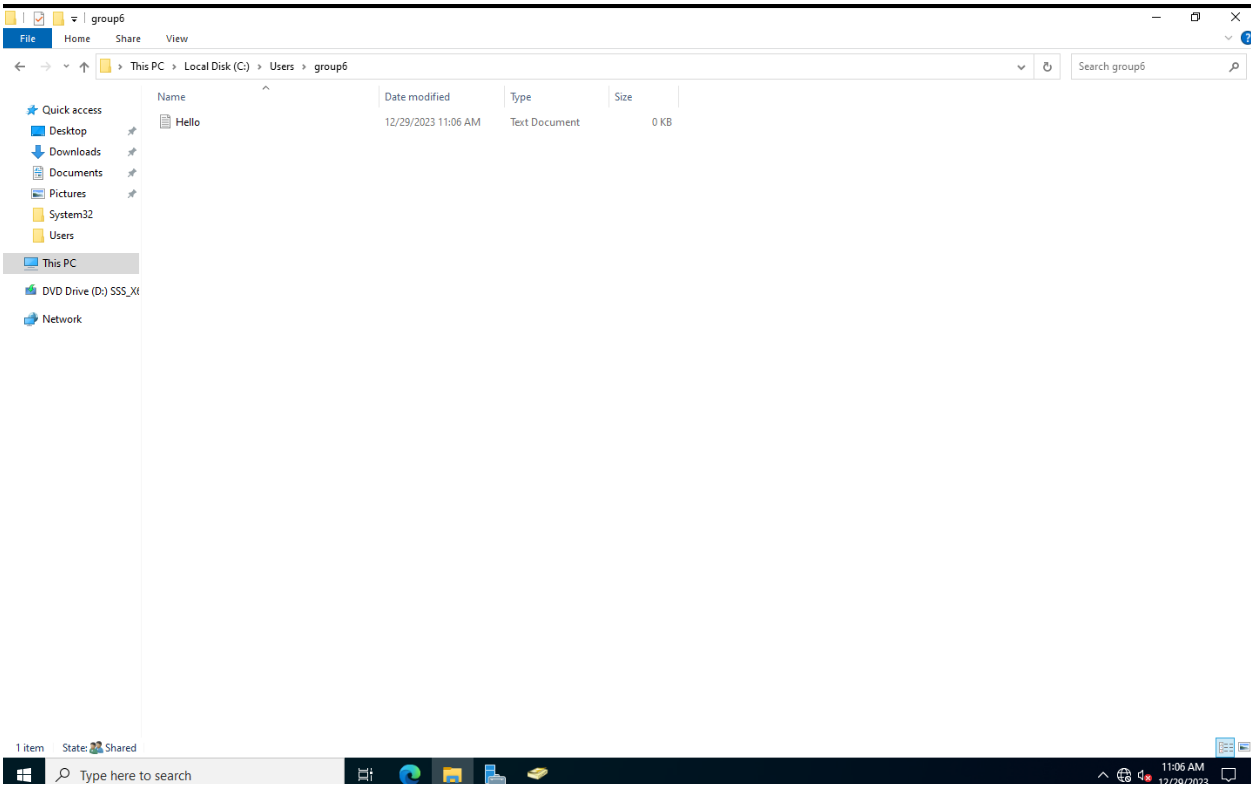
Define routes to enable for this Dial-in connection.

- Navigate to “C:\Users” and create a “group6” folder there for the user.



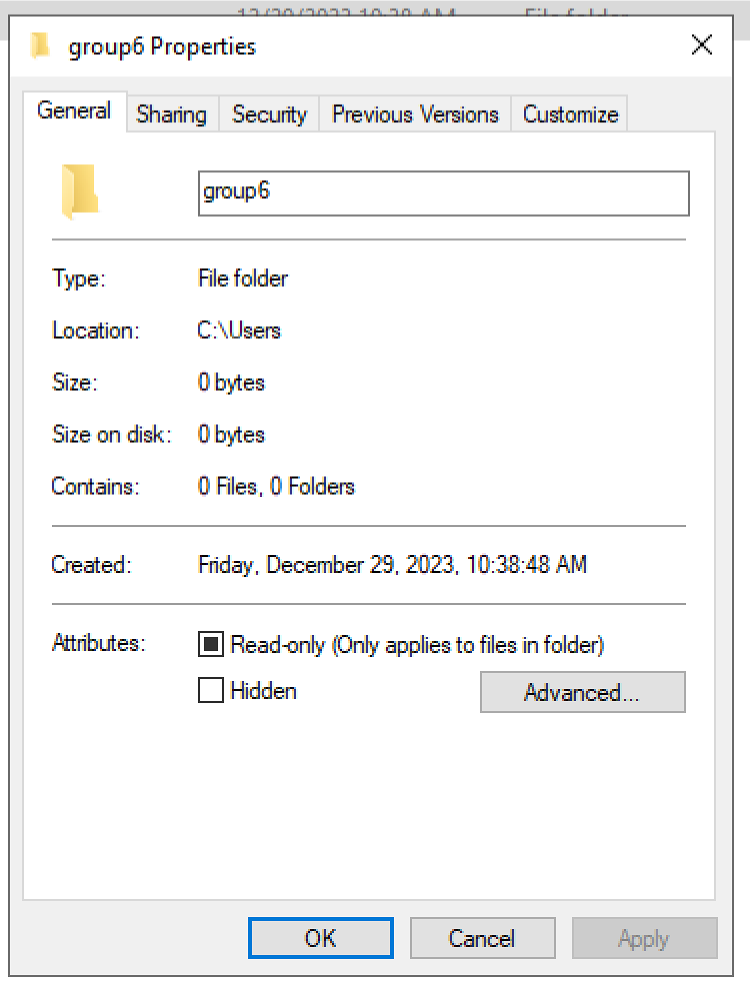
Name	Date modified	Type	Size
Administrator	12/9/2023 3:47 AM	File folder	
group6	12/29/2023 10:38 AM	File folder	
Public	12/9/2023 3:47 AM	File folder	

- In the folder, create a txt file.



Name	Date modified	Type	Size
Hello	12/29/2023 11:06 AM	Text Document	0 KB

- Right click on the folder and click “Properties”.



group6

Type: File folder

Location: C:\Users

Size: 0 bytes

Size on disk: 0 bytes

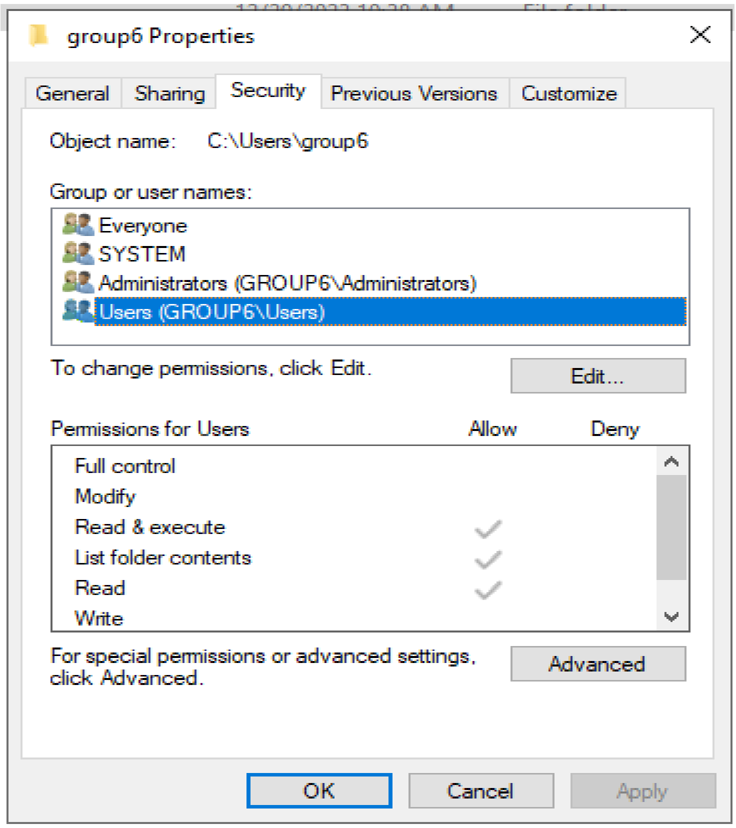
Contains: 0 Files, 0 Folders

Created: Friday, December 29, 2023, 10:38:48 AM

Attributes: ■ Read-only (Only applies to files in folder)

□ Hidden

- Select “Security” tab and click on “Edit”.



Object name: C:\Users\group6

Group or user names:

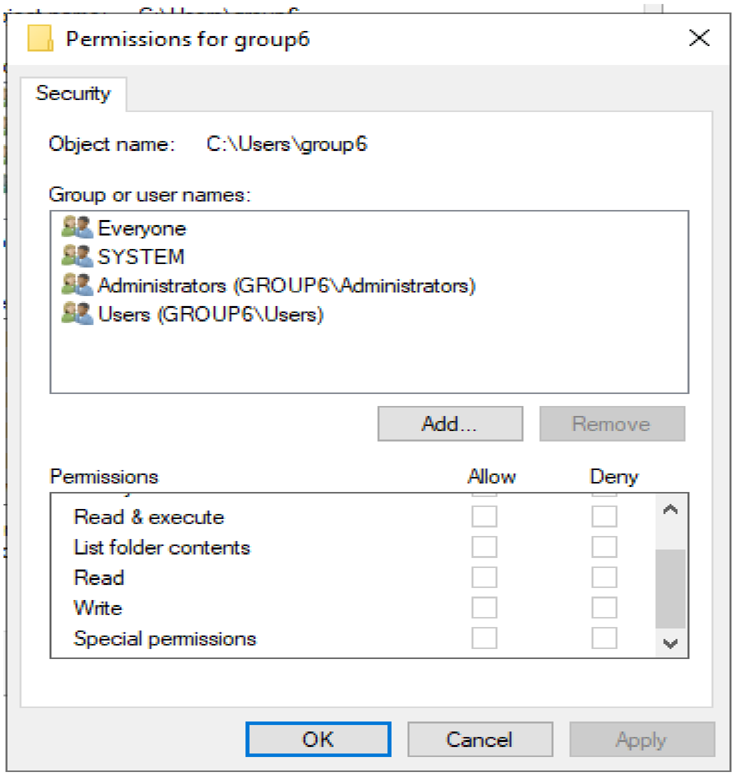
- Everyone
- SYSTEM
- Administrators (GROUP6\Administrators)
- Users (GROUP6\Users)

To change permissions, click Edit.

Permissions for Users	Allow	Deny
Full control		
Modify		
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write		

For special permissions or advanced settings, click Advanced.

- Select “Add”.



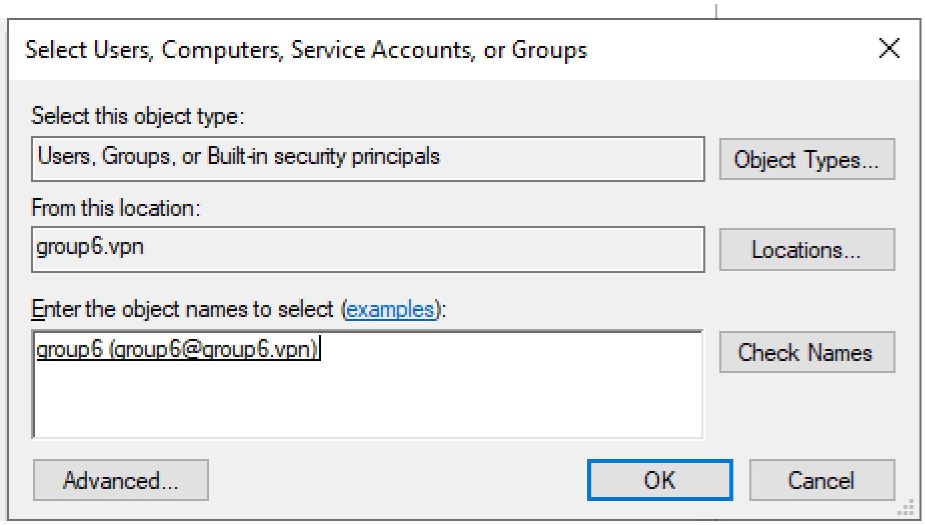
Object name: C:\Users\group6

Group or user names:

- Everyone
- SYSTEM
- Administrators (GROUP6\Administrators)
- Users (GROUP6\Users)

Permissions	Allow	Deny
Read & execute	□	□
List folder contents	□	□
Read	□	□
Write	□	□
Special permissions	□	□

- Type the name of the user and click on “Check Names” and the user should be there.



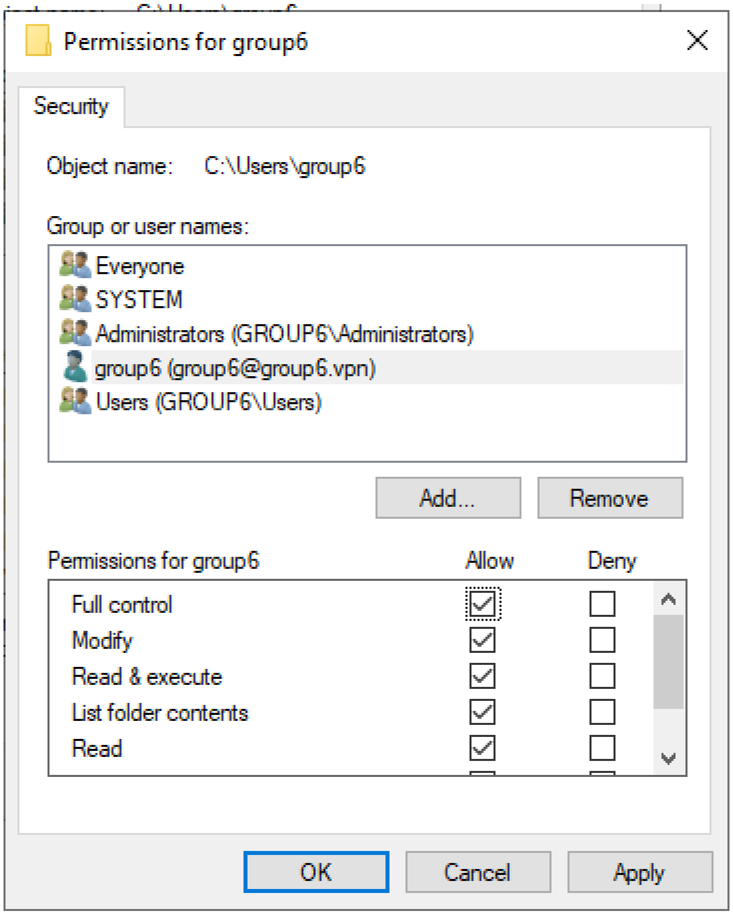
Select Users, Computers, Service Accounts, or Groups

Select this object type: Users, Groups, or Built-in security principals

From this location: group6.vpn

Enter the object names to select (examples): group6 (group6@group6.vpn)

- We gave this user to have full control of the folder.



Permissions for group6

Security

Object name: C:\Users\group6

Group or user names:

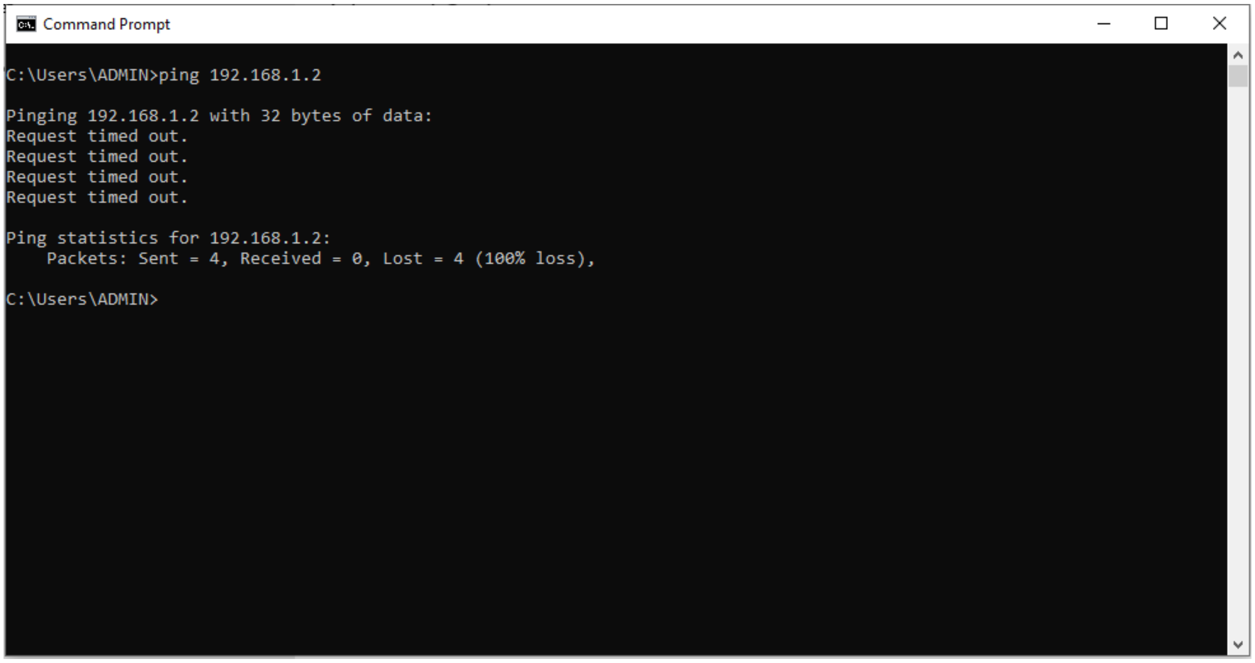
Everyone
SYSTEM
Administrators (GROUP6\Administrators)
group6 (group6@group6.vpn)
Users (GROUP6\Users)

Permissions for group6	Allow	Deny
Full control	☑	□
Modify	☑	□
Read & execute	☑	□
List folder contents	☑	□
Read	☑	□

III. RESULT

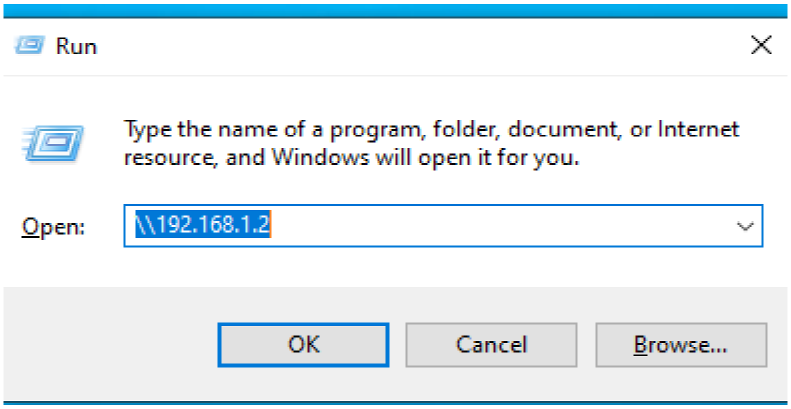
3.1 Check the connection.

- First, we will check connection to the File Server from Client before connecting to VPN.



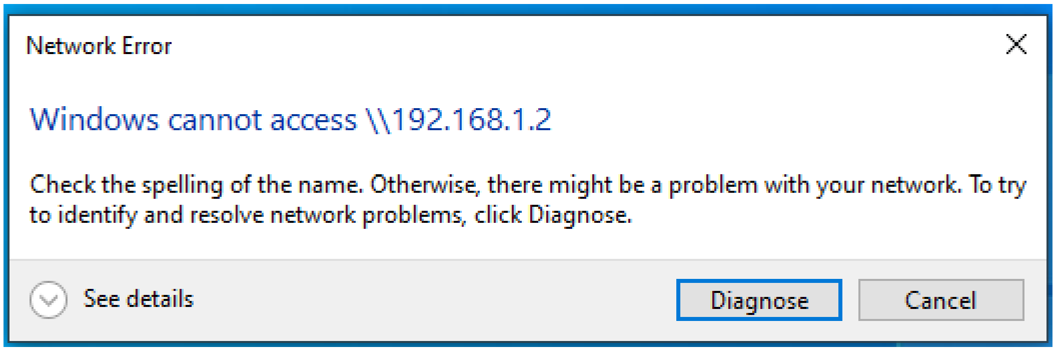
```
C:\Users\ADMIN>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\ADMIN>
```

- After that, let’s try to access to the File Server using Win + R



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: \\192.168.1.2

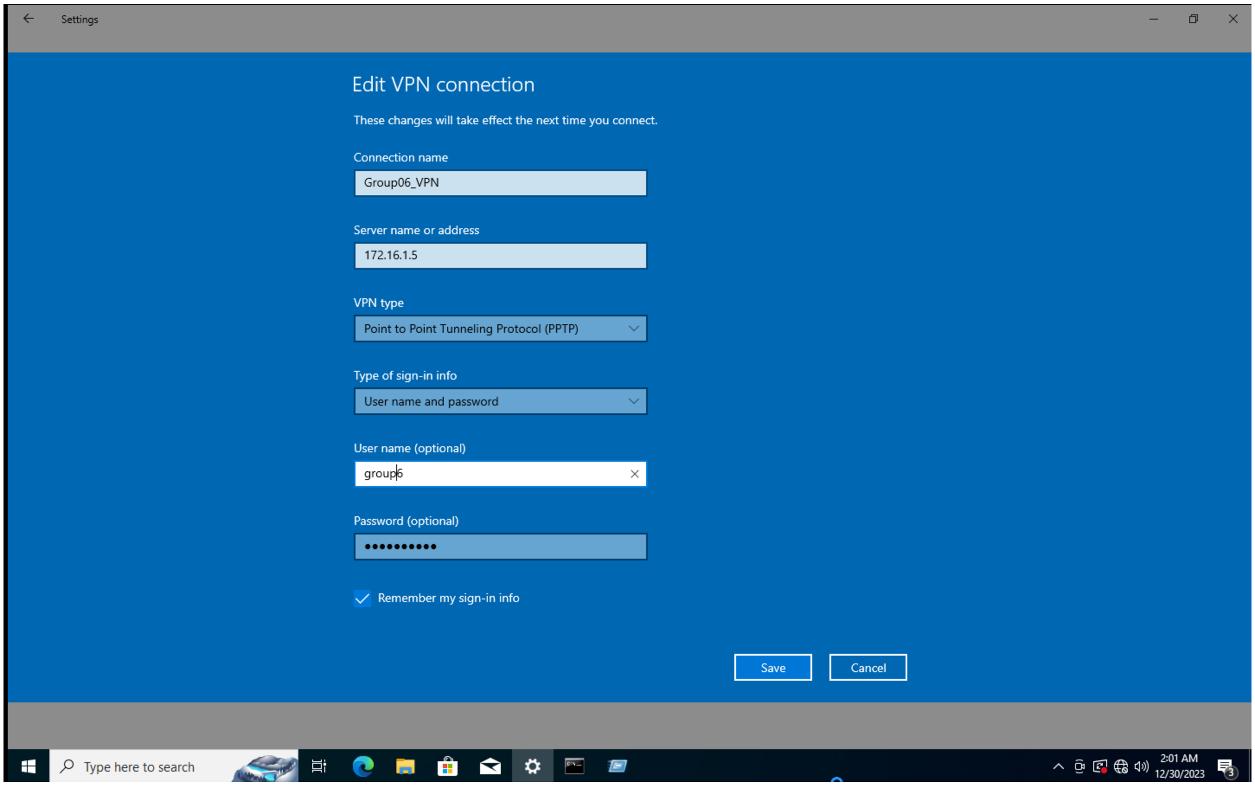


Network Error

Windows cannot access \\192.168.1.2

Check the spelling of the name. Otherwise, there might be a problem with your network. To try to identify and resolve network problems, click Diagnose.

- Now, we will create a VPN connection with these following configurations.



Edit VPN connection

These changes will take effect the next time you connect.

Connection name: Group06_VPN

Server name or address: 172.16.1.5

VPN type: Point to Point Tunneling Protocol (PPTP)

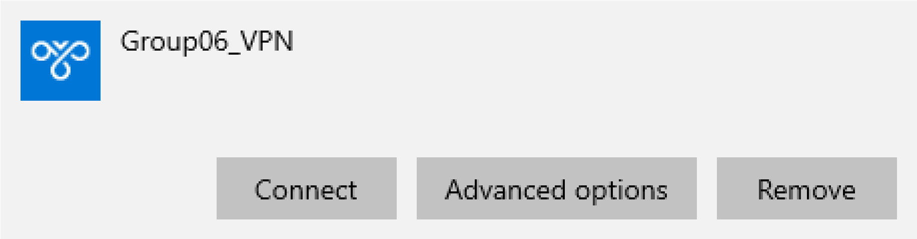
Type of sign-in info: User name and password

User name (optional): group6

Password (optional): ••••••••••

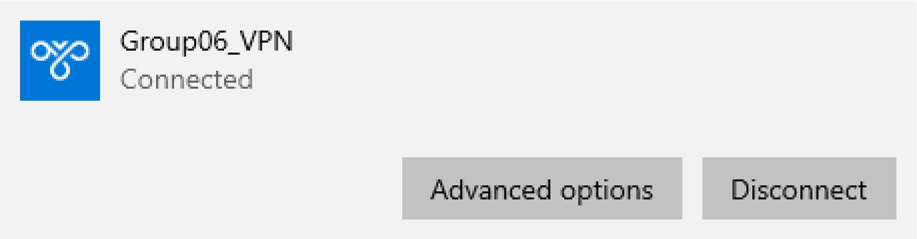
☑ Remember my sign-in info

- Then click on “Connect”.

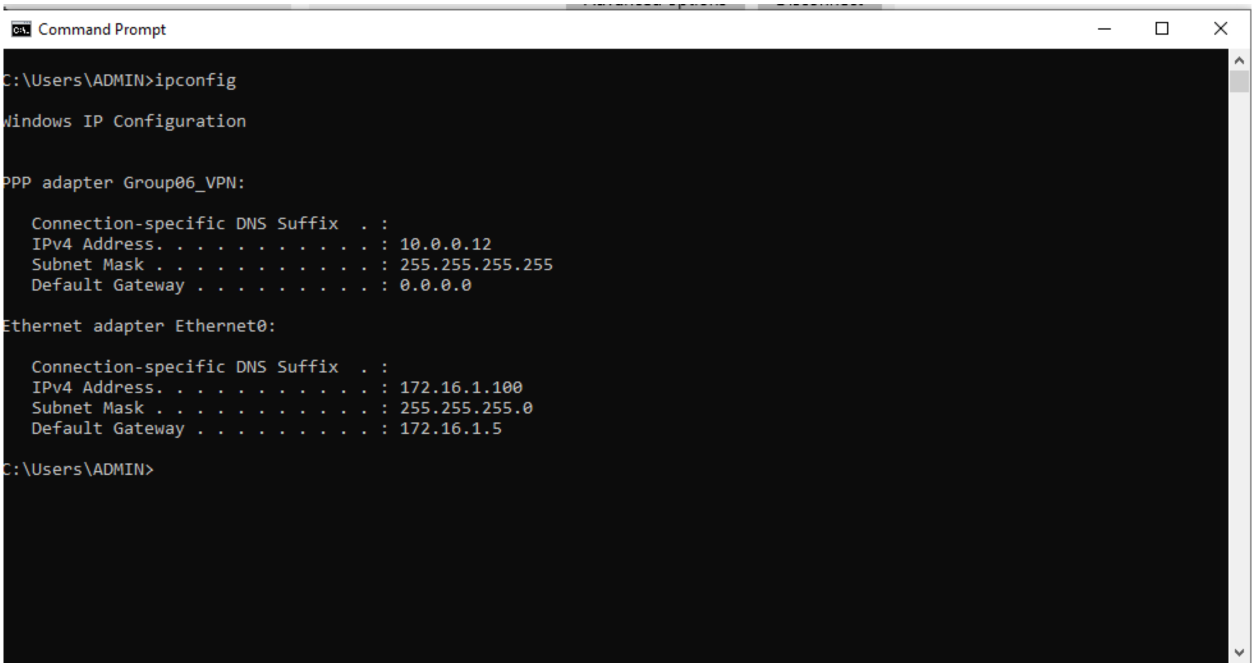


Group06_VPN

- The result:

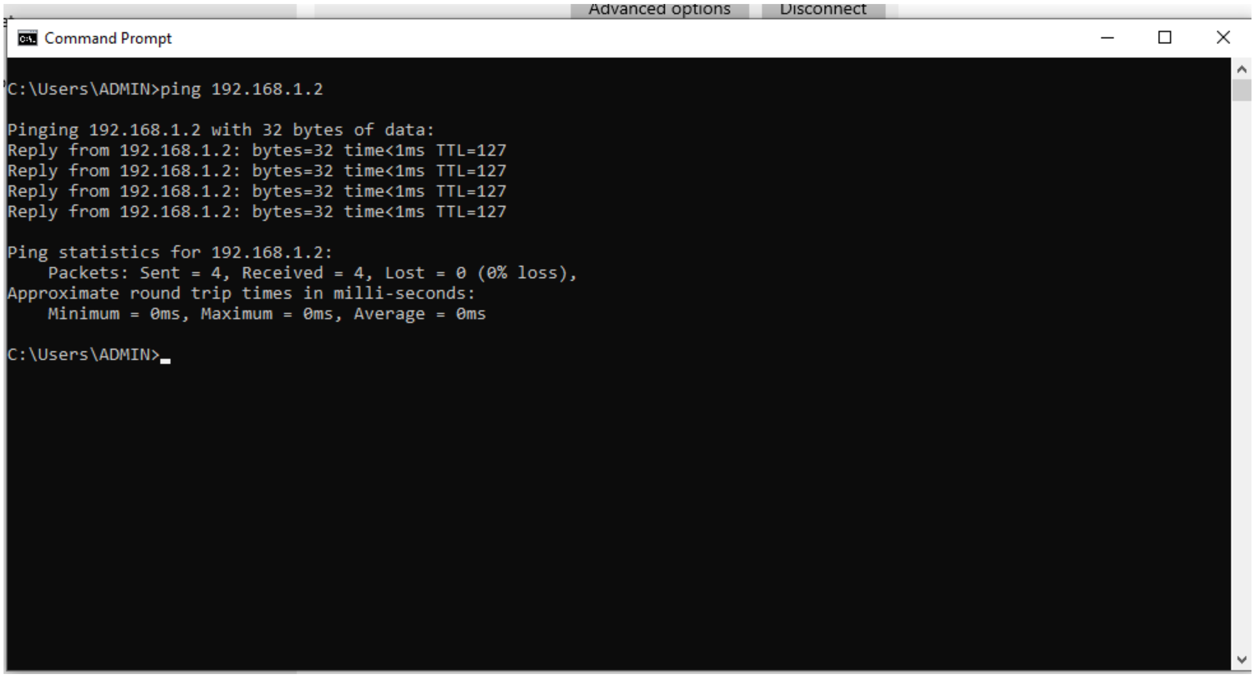


Group06_VPN
Connected



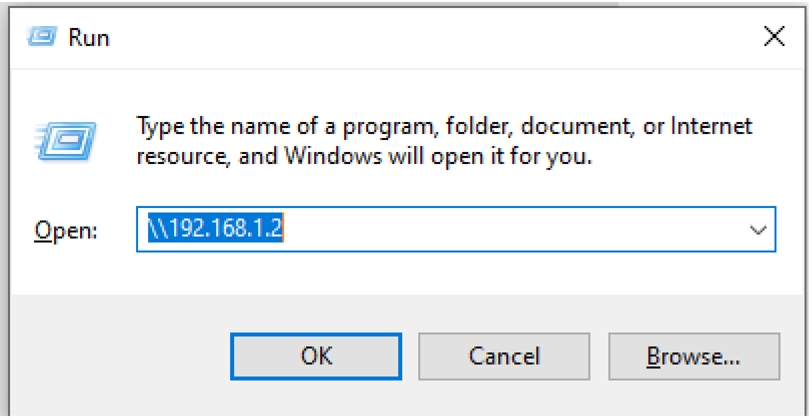
```
C:\Users\ADMIN>ipconfig

Windows IP Configuration


PPP adapter Group06_VPN:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.0.0.12
   Subnet Mask . . . . . . . . . . . : 255.255.255.255
   Default Gateway . . . . . . . . . : 0.0.0.0

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 172.16.1.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.16.1.5

C:\Users\ADMIN>
```

- Again, let’s check the connection to File Server by pinging.



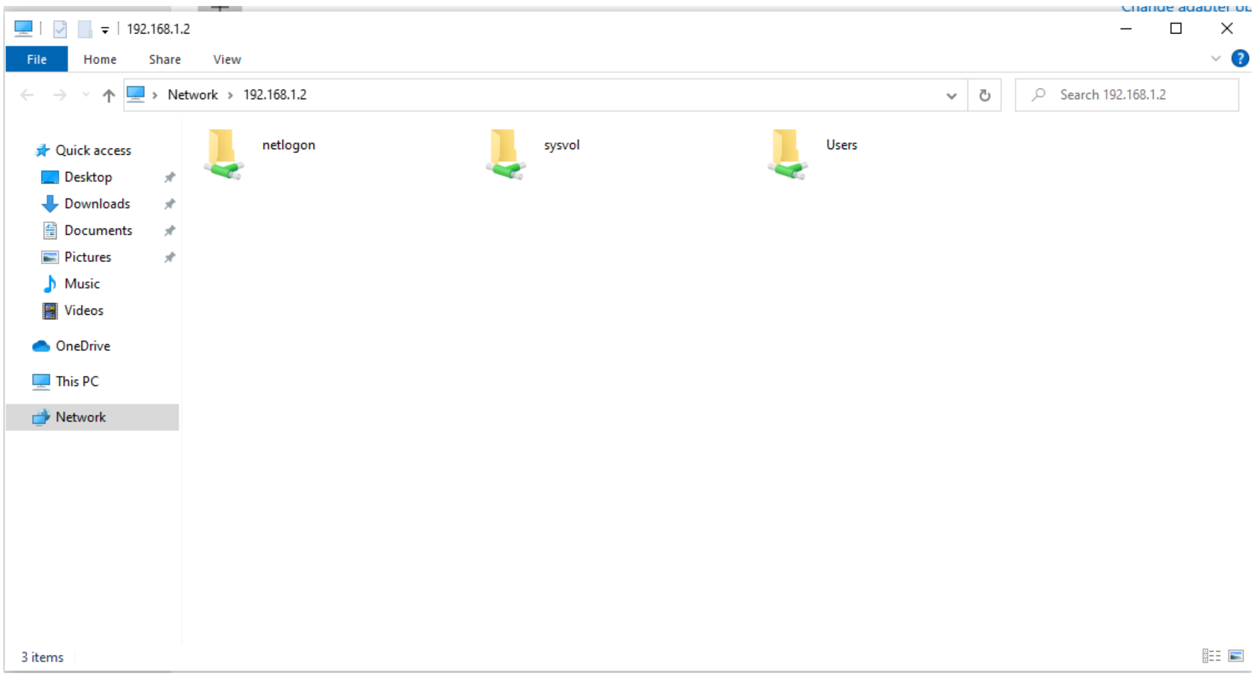
```
C:\Users\ADMIN>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\ADMIN>_
```

- Let’s run Win + R to access to File Server.

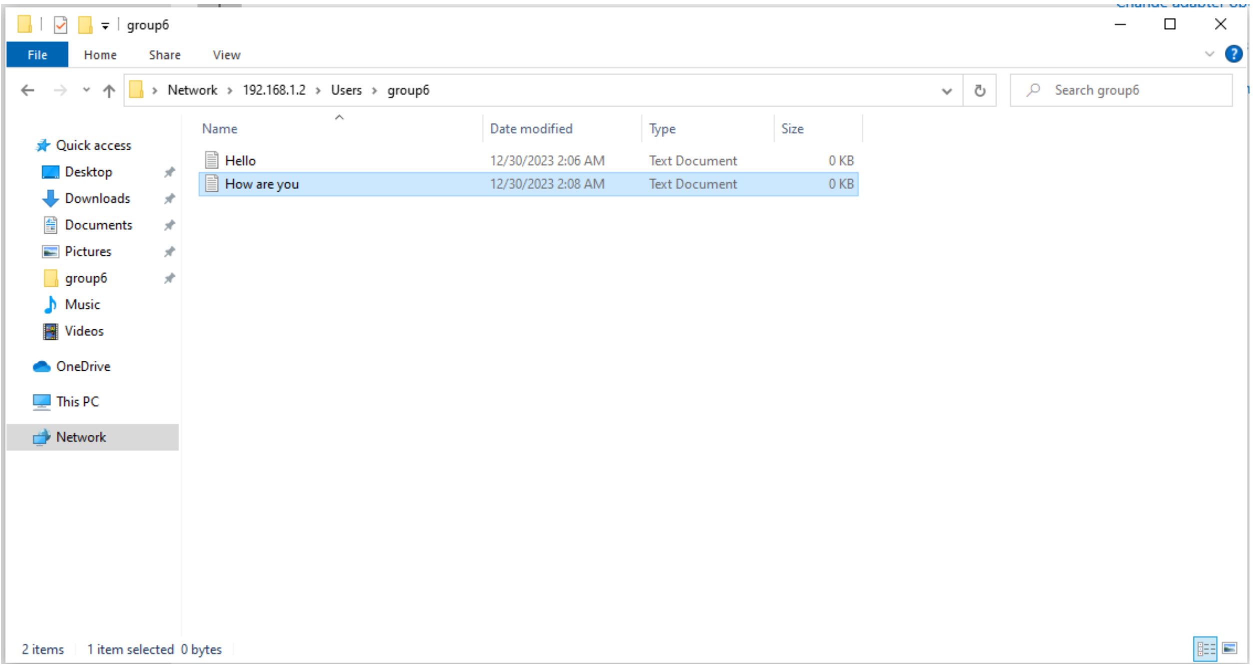


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: \\192.168.1.2



- ○ Next, navigate to the created folder for “group6” user and create another .txt file to check the permissions.

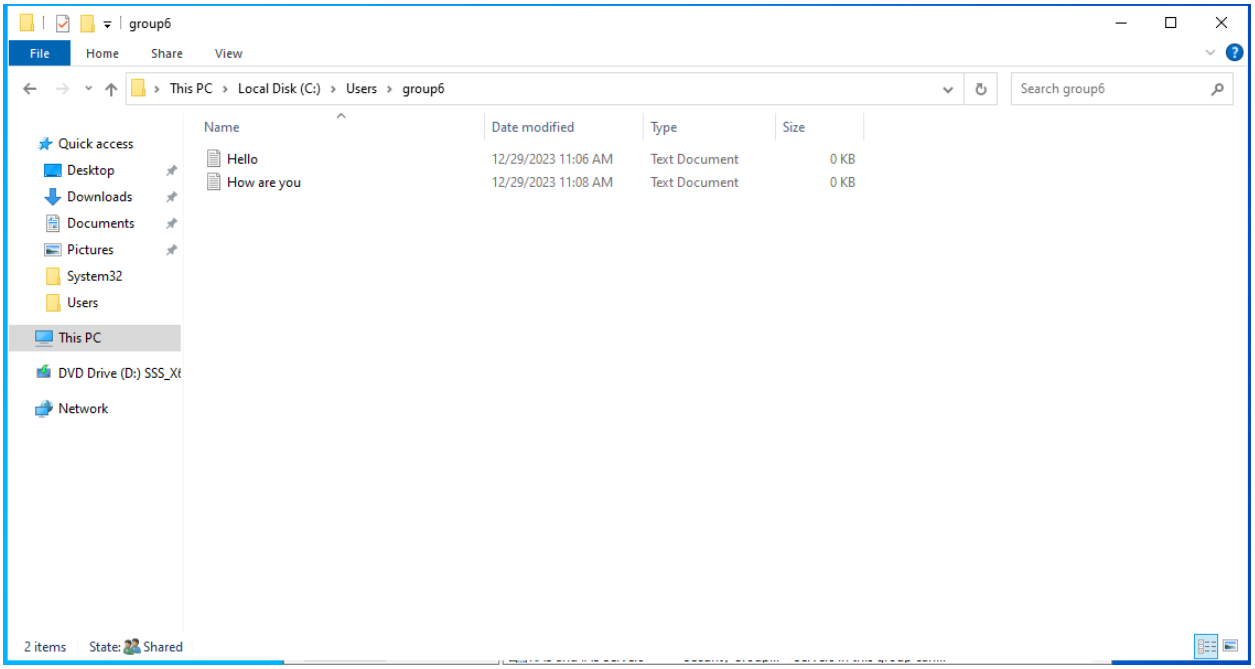


Network > 192.168.1.2 > Users > group6

Name	Date modified	Type	Size
Hello	12/30/2023 2:06 AM	Text Document	0 KB
How are you	12/30/2023 2:08 AM	Text Document	0 KB

2 items 1 item selected 0 bytes

- Then, we will go back to File Server and check the new .txt file.



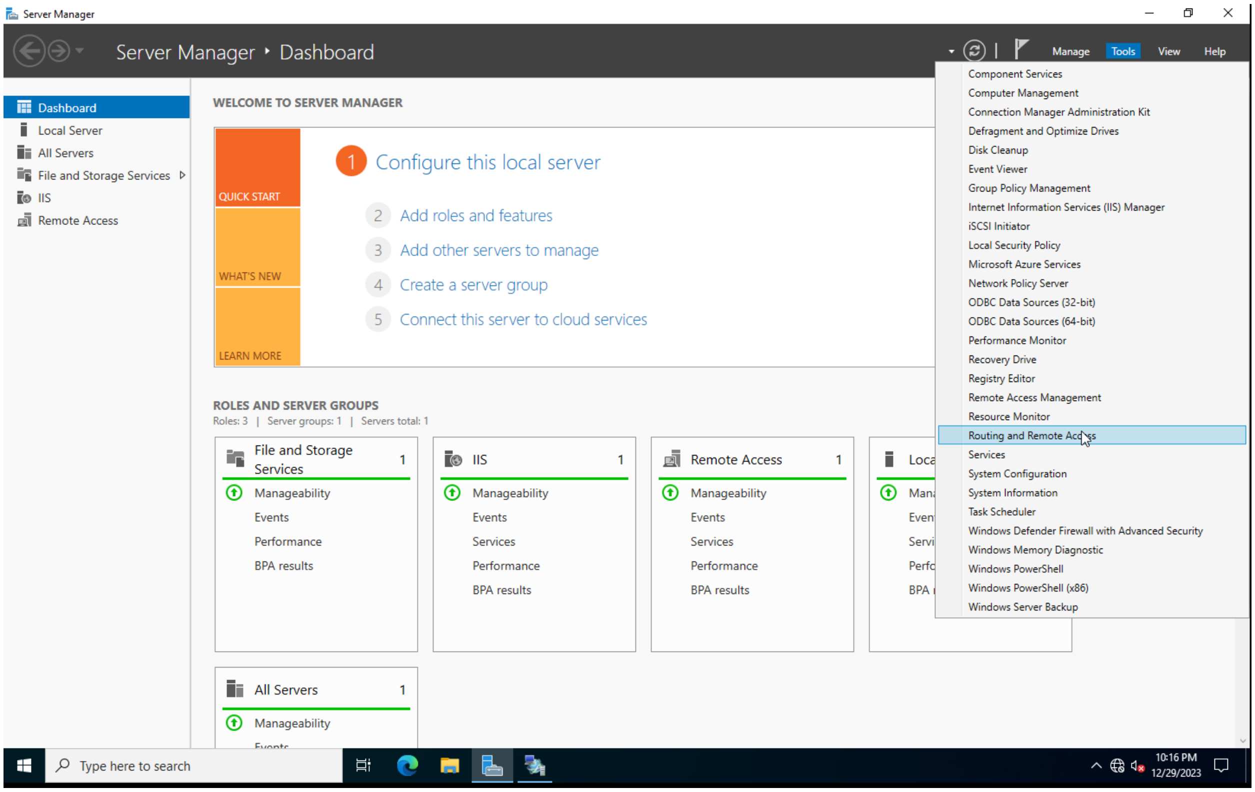
This PC > Local Disk (C:) > Users > group6

Name	Date modified	Type	Size
Hello	12/29/2023 11:06 AM	Text Document	0 KB
How are you	12/29/2023 11:08 AM	Text Document	0 KB

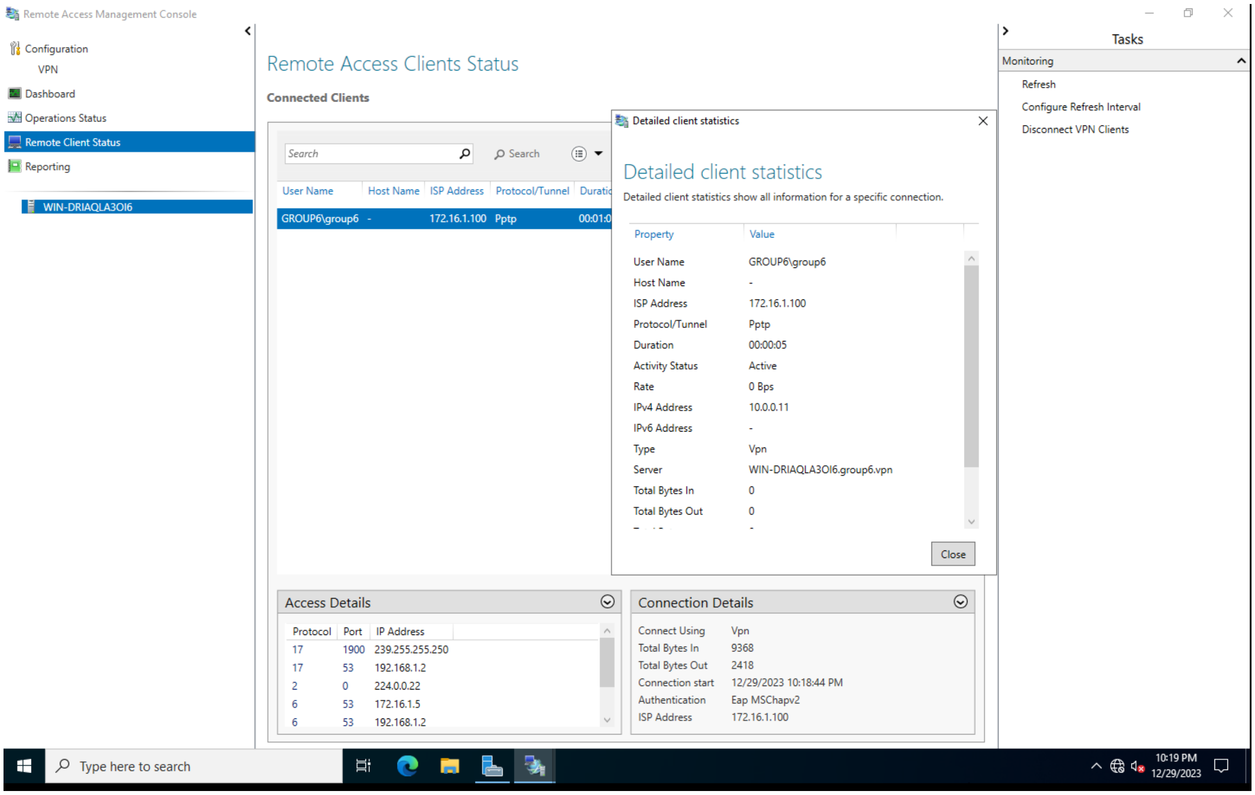
2 items State: Shared

3.2 Monitor VPN Server

- Open “Server Manger” on VPN and navigate to Tool -> Remote Access Management.



- At "Remote Client Status" we can check user's VPN connections and monitor them.



Remote Access Clients Status

Connected Clients

User Name	Host Name	ISP Address	Protocol/Tunnel	Duratio
GROUP6\group6	-	172.16.1.100	Pptp	00:01:0

Detailed client statistics

Detailed client statistics show all information for a specific connection.

Property	Value
User Name	GROUP6\group6
Host Name	-
ISP Address	172.16.1.100
Protocol/Tunnel	Pptp
Duration	00:00:05
Activity Status	Active
Rate	0 Bps
IPv4 Address	10.0.0.11
IPv6 Address	-
Type	Vpn
Server	WIN-DRIAQLA3OI6.group6.vpn
Total Bytes In	0
Total Bytes Out	0

Access Details

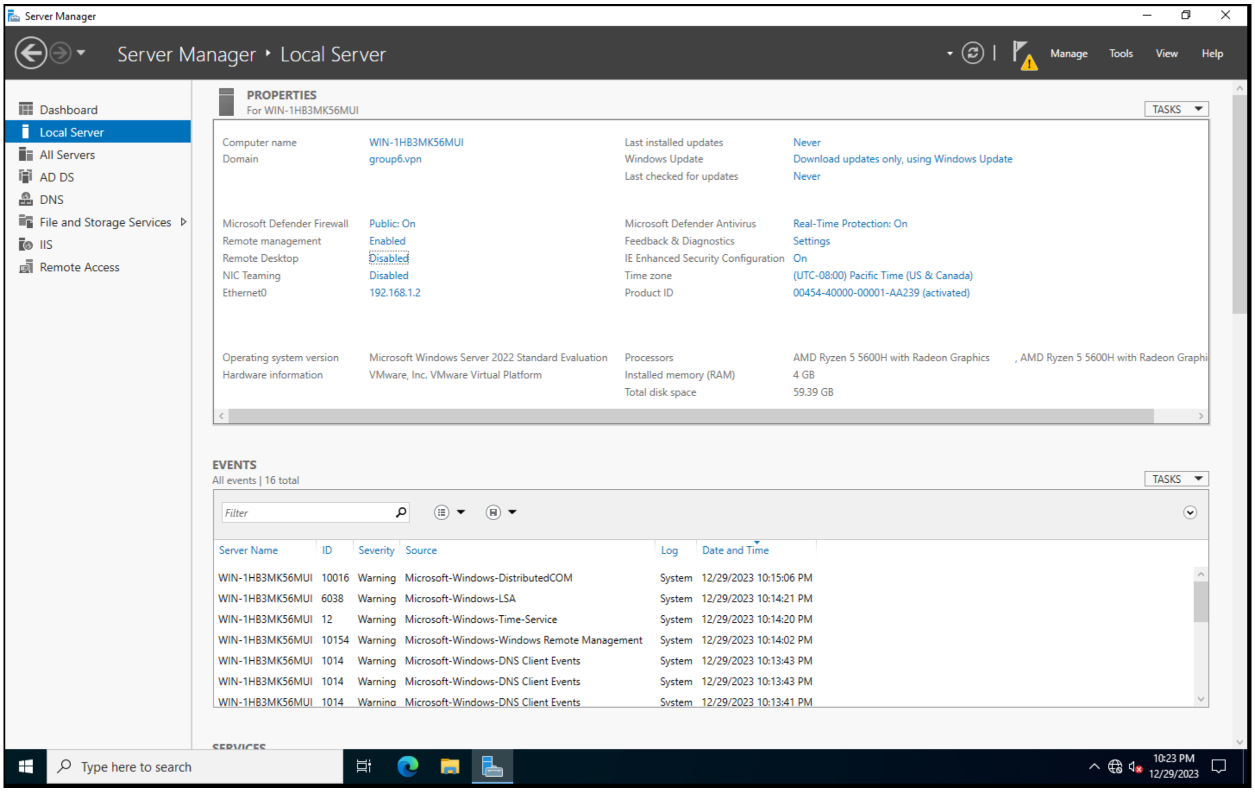
Protocol	Port	IP Address
17	1900	239.255.255.250
17	53	192.168.1.2
2	0	224.0.0.22
6	53	172.16.1.5
6	53	192.168.1.2

Connection Details

Connect Using	Vpn
Total Bytes In	9368
Total Bytes Out	2418
Connection start	12/29/2023 10:18:44 PM
Authentication	Eap MSChapv2
ISP Address	172.16.1.100

3.3 Advance: Remote Desktop

- At File Server, search for the “Local Server” tab and locate “Remote Desktop” and check if it is enabled or not.



PROPERTIES
For WIN-1HB3MK56MUI

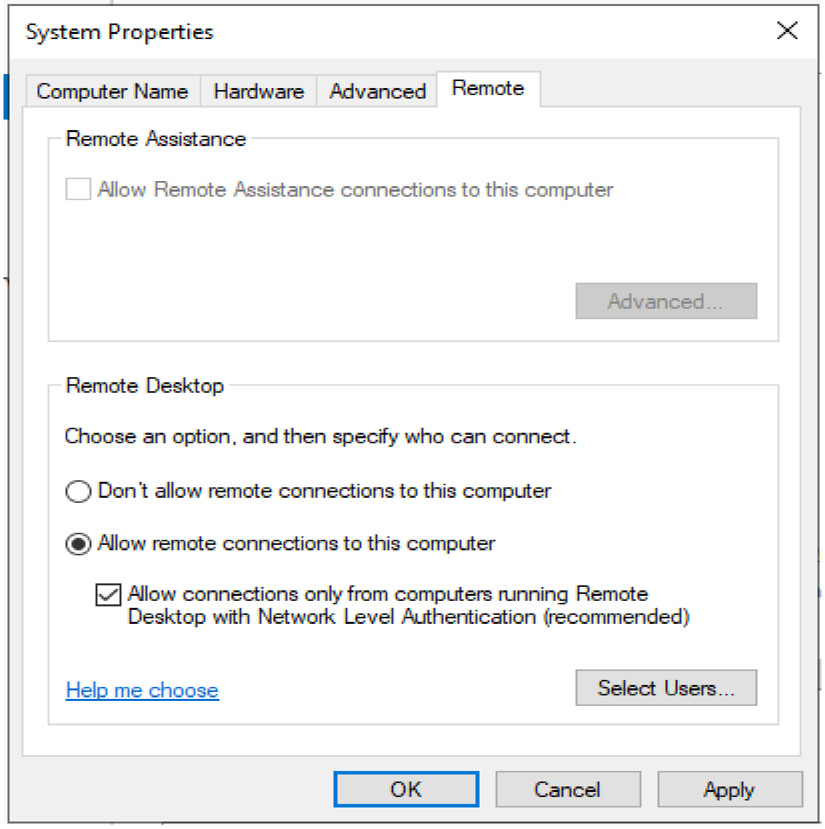
Computer name	WIN-1HB3MK56MUI	Last installed updates	Never
Domain	group6.vpn	Windows Update	Download updates only, using Windows Update
		Last checked for updates	Never
Microsoft Defender Firewall	Public: On	Microsoft Defender Antivirus	Real-Time Protection: On
Remote management	Enabled	Feedback & Diagnostics	Settings
Remote Desktop	Disabled	IE Enhanced Security Configuration	On
NIC Teaming	Disabled	Time zone	(UTC-08:00) Pacific Time (US & Canada)
Ethernet0	192.168.1.2	Product ID	00454-40000-00001-AA239 (activated)
Operating system version	Microsoft Windows Server 2022 Standard Evaluation	Processors	AMD Ryzen 5 5600H with Radeon Graphics , AMD Ryzen 5 5600H with Radeon Graphi
Hardware information	VMware, Inc. VMware Virtual Platform	Installed memory (RAM)	4 GB
		Total disk space	59.39 GB

EVENTS
All events | 16 total

Filter

Server Name	ID	Severity	Source	Log	Date and Time
WIN-1HB3MK56MUI	10016	Warning	Microsoft-Windows-DistributedCOM	System	12/29/2023 10:15:06 PM
WIN-1HB3MK56MUI	6038	Warning	Microsoft-Windows-LSA	System	12/29/2023 10:14:21 PM
WIN-1HB3MK56MUI	12	Warning	Microsoft-Windows-Time-Service	System	12/29/2023 10:14:20 PM
WIN-1HB3MK56MUI	10154	Warning	Microsoft-Windows-Windows Remote Management	System	12/29/2023 10:14:02 PM
WIN-1HB3MK56MUI	1014	Warning	Microsoft-Windows-DNS Client Events	System	12/29/2023 10:13:43 PM
WIN-1HB3MK56MUI	1014	Warning	Microsoft-Windows-DNS Client Events	System	12/29/2023 10:13:43 PM
WIN-1HB3MK56MUI	1014	Warning	Microsoft-Windows-DNS Client Events	System	12/29/2023 10:13:41 PM

- By default, it is disabled so let’s enable by clicking on it.
- A window will pop up, tick the “Allow remote connections to this computer”.



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

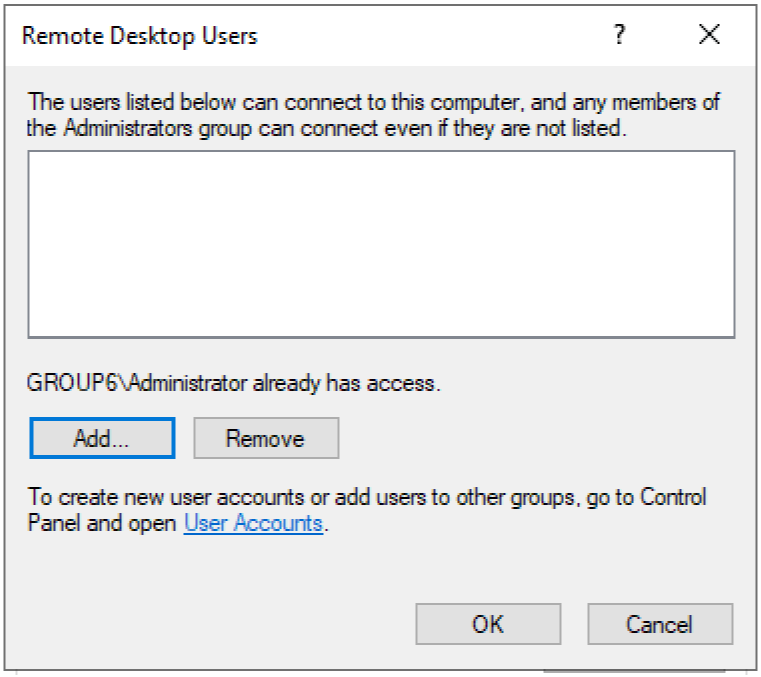
☑ Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)

Help me choose

Select Users...

OK | Cancel | Apply

- After that, hit "Selects Users…" and select "Add…".



Remote Desktop Users

The users listed below can connect to this computer, and any members of the Administrators group can connect even if they are not listed.

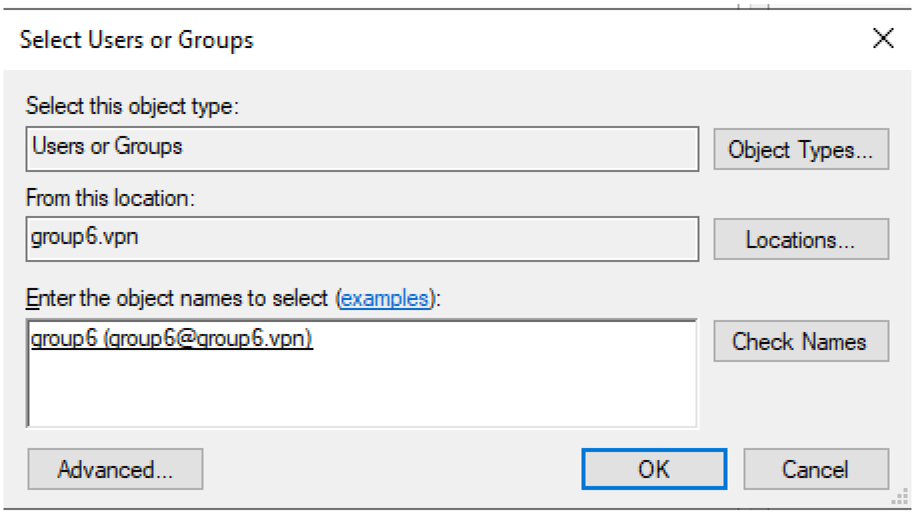
GROUP6\Administrator already has access.

Add... | Remove

To create new user accounts or add users to other groups, go to Control Panel and open User Accounts.

OK | Cancel

- Enter the username that we want and press "Check Names" then hit OK.

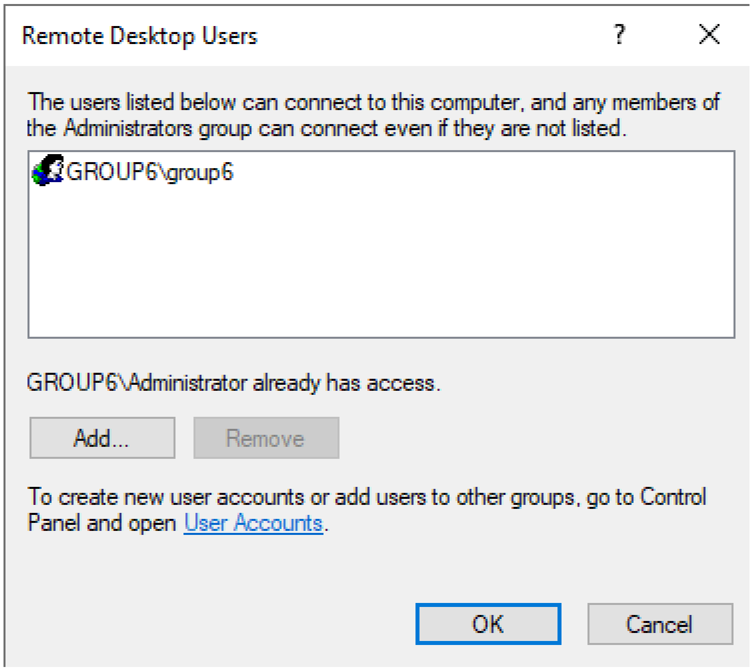


Select Users or Groups

Select this object type:
Users or Groups

From this location:
group6.vpn

Enter the object names to select (examples):
group6 (group6@group6.vpn)



Remote Desktop Users

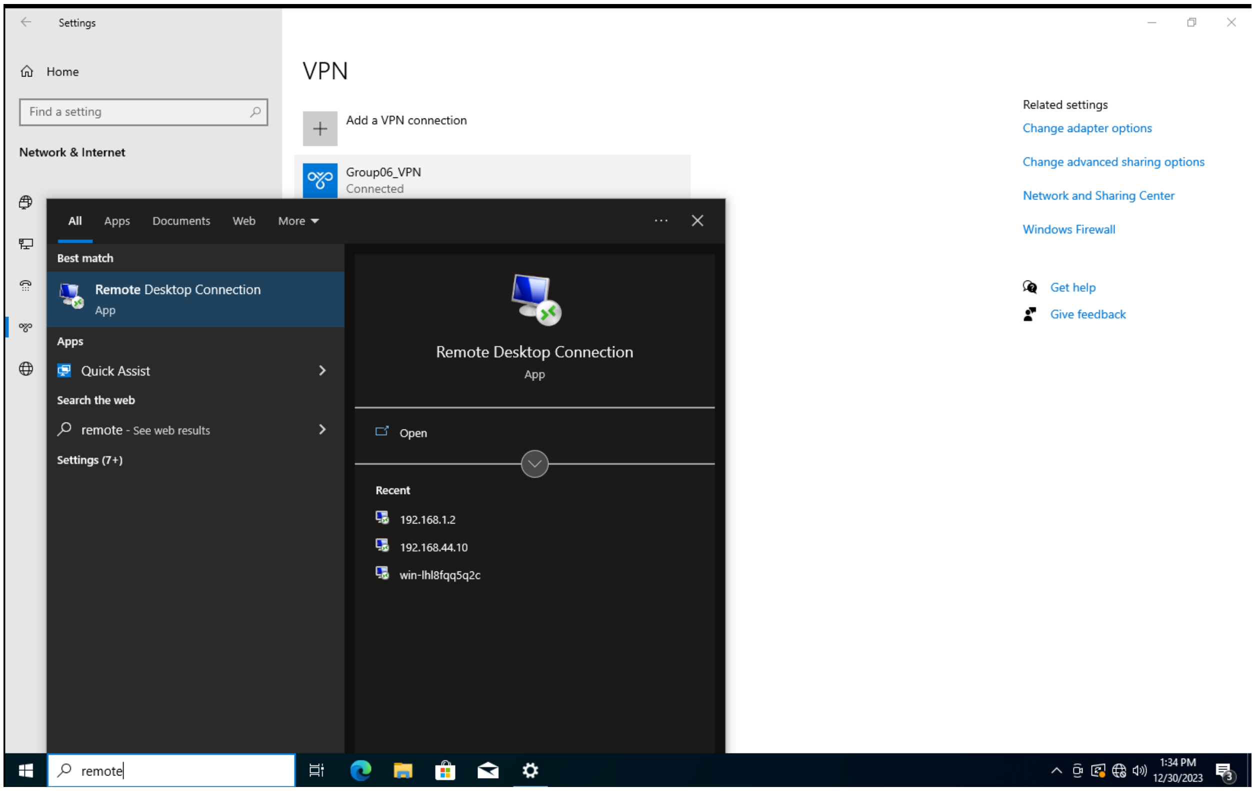
The users listed below can connect to this computer, and any members of the Administrators group can connect even if they are not listed.

GROUP6\group6

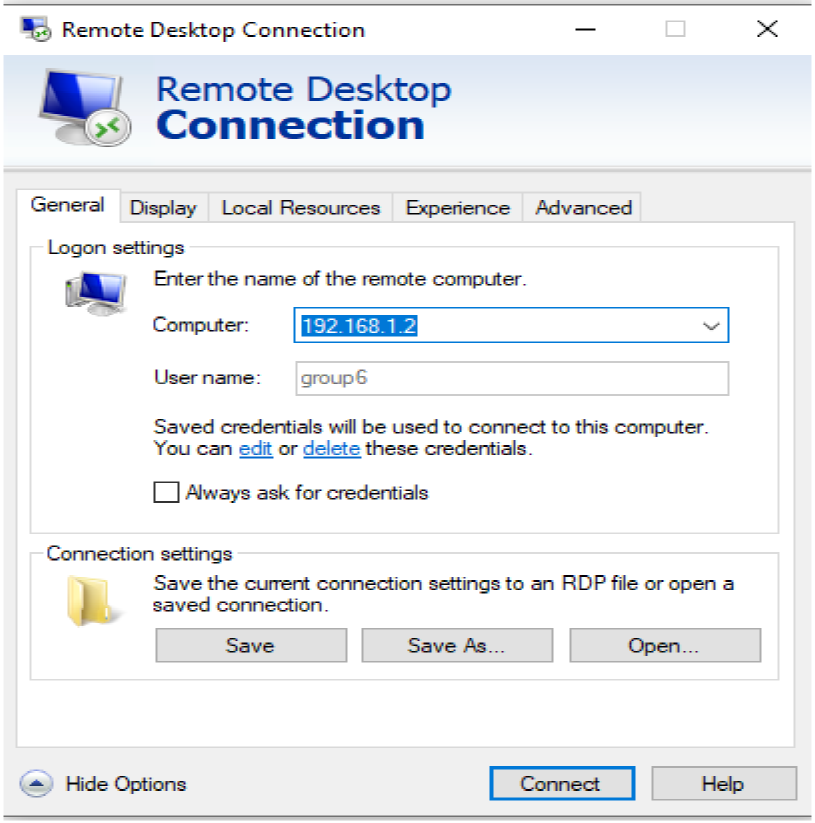
GROUP6\Administrator already has access.

To create new user accounts or add users to other groups, go to Control Panel and open User Accounts.

- Now we will check if the client can remote to the File Server.
- At client’s machine, search “Remote Desktop Connection”.



- A window will pop up, now what we need to do is to fill the File Server's ip address at "Computer:" box then hit "Connect"



Enter the name of the remote computer.

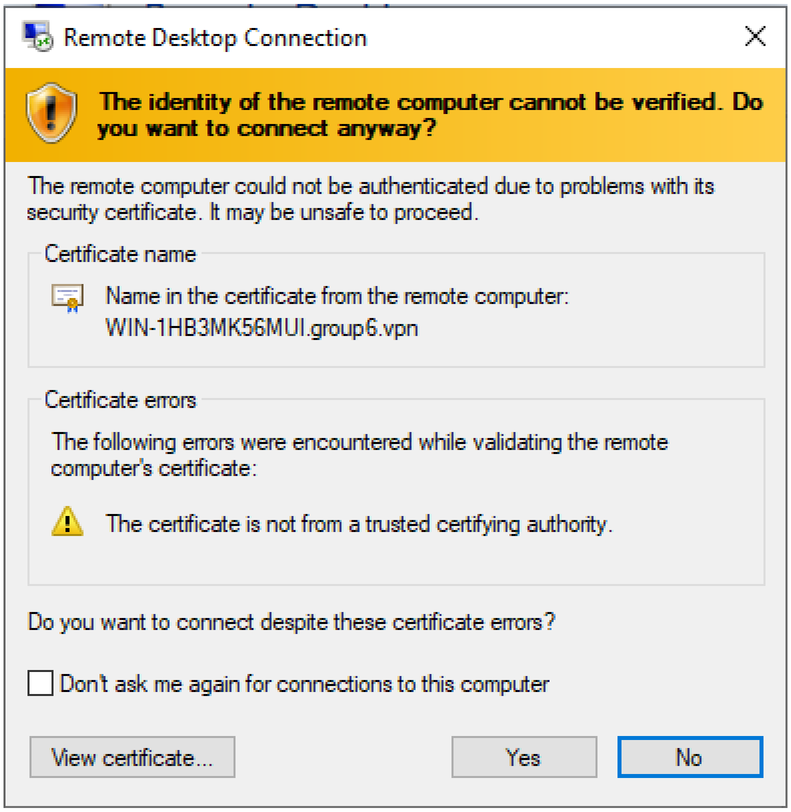
Computer: 192.168.1.2

User name: group6

Saved credentials will be used to connect to this computer. You can edit or delete these credentials.

☐ Always ask for credentials

Save the current connection settings to an RDP file or open a saved connection.



The identity of the remote computer cannot be verified. Do you want to connect anyway?

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Certificate name

Name in the certificate from the remote computer:
WIN-1HB3MK56MUI.group6.vpn

Certificate errors

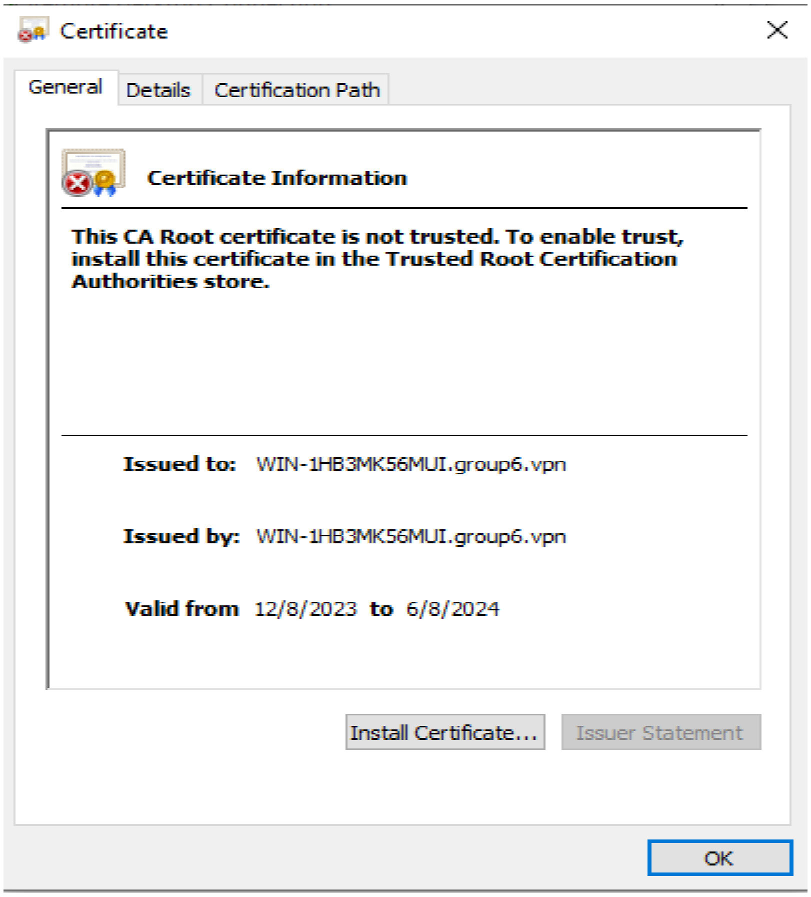
The following errors were encountered while validating the remote computer's certificate:

The certificate is not from a trusted certifying authority.

Do you want to connect despite these certificate errors?

☐ Don't ask me again for connections to this computer

- A warning pop up and say that the File Server's Certificate is not trustable so what we going to do here is hit "View certificate" and install it on the client's machine.



Certificate

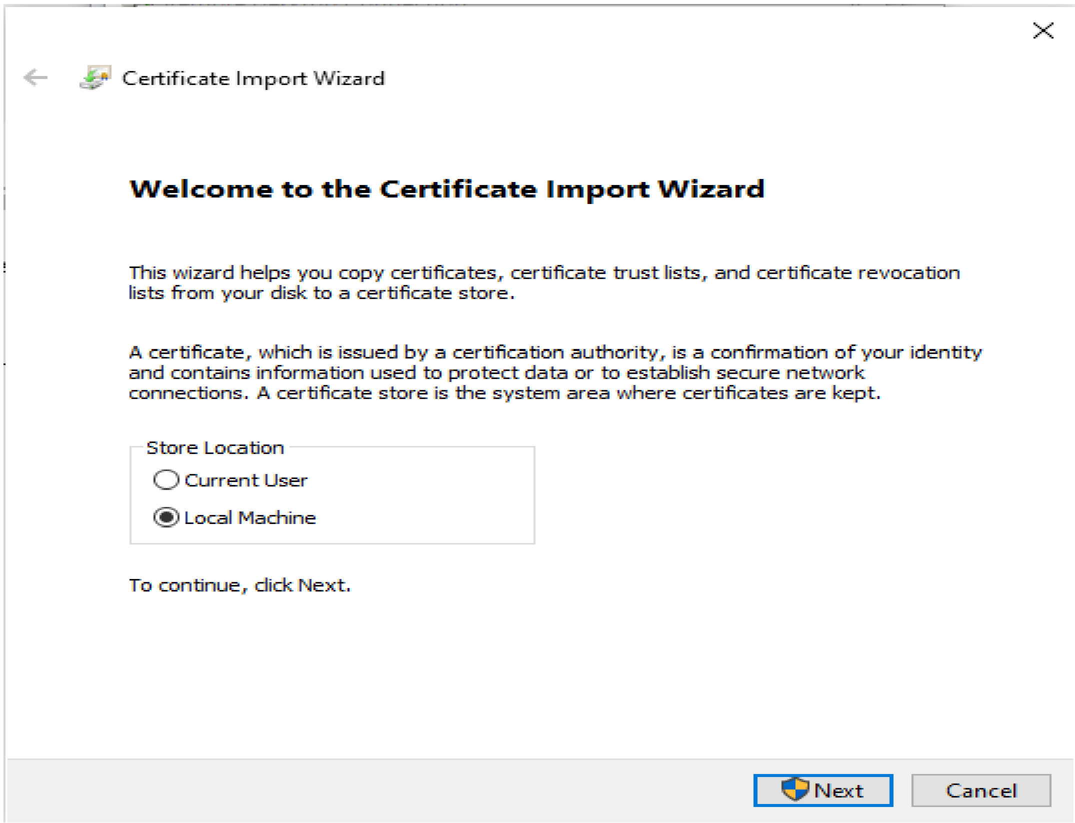
Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: WIN-1HB3MK56MUI.group6.vpn

Issued by: WIN-1HB3MK56MUI.group6.vpn

Valid from 12/8/2023 **to** 6/8/2024



Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

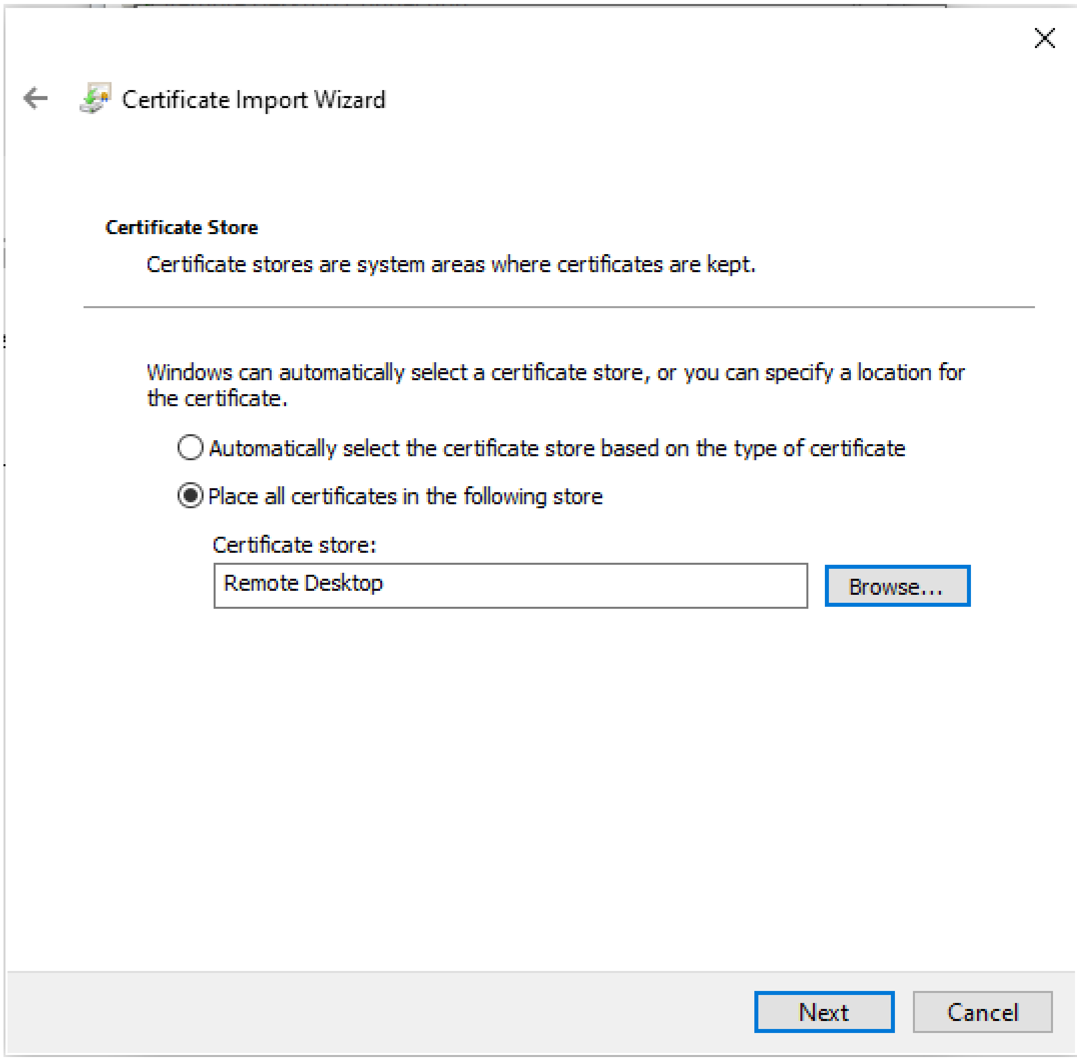
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location

○ Current User

● Local Machine

To continue, click Next.



Certificate Import Wizard

Certificate Store

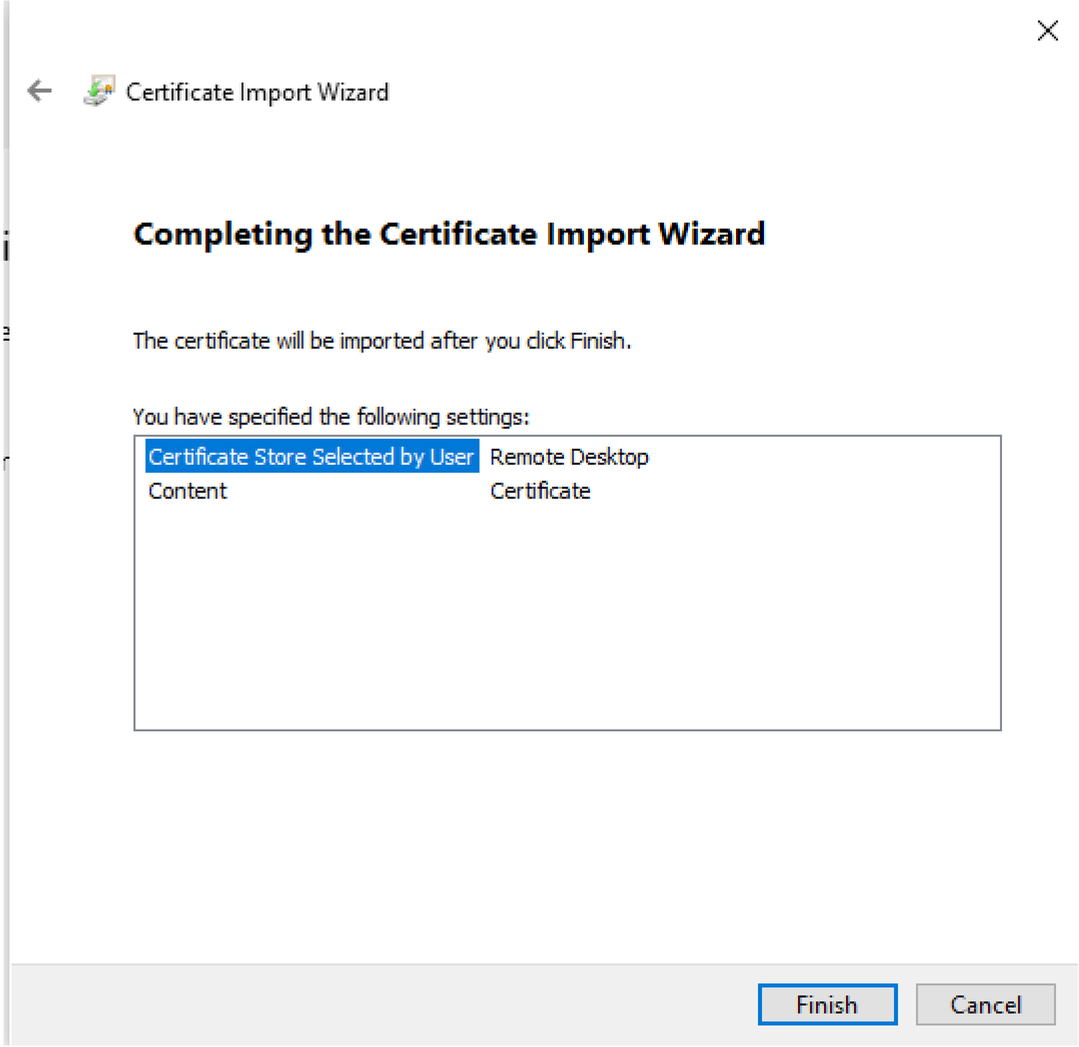
Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Remote Desktop



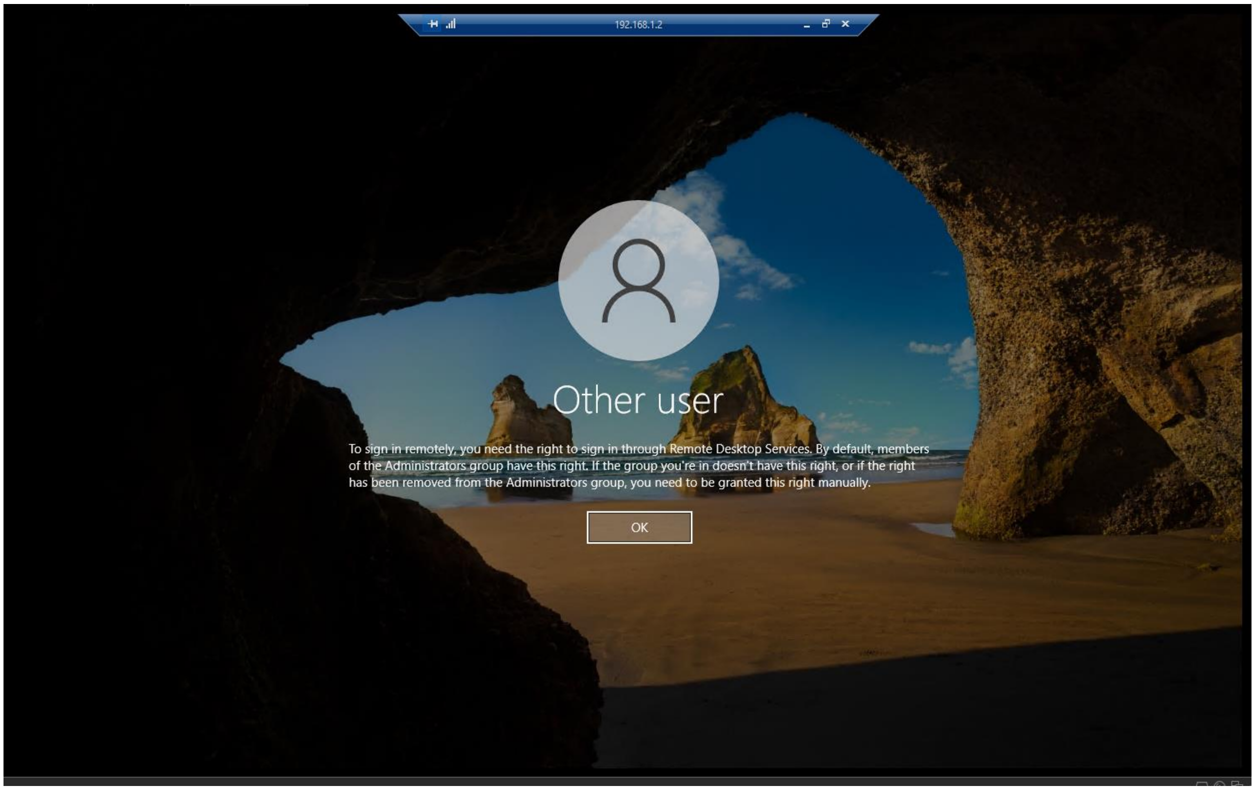
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Remote Desktop
Content	Certificate

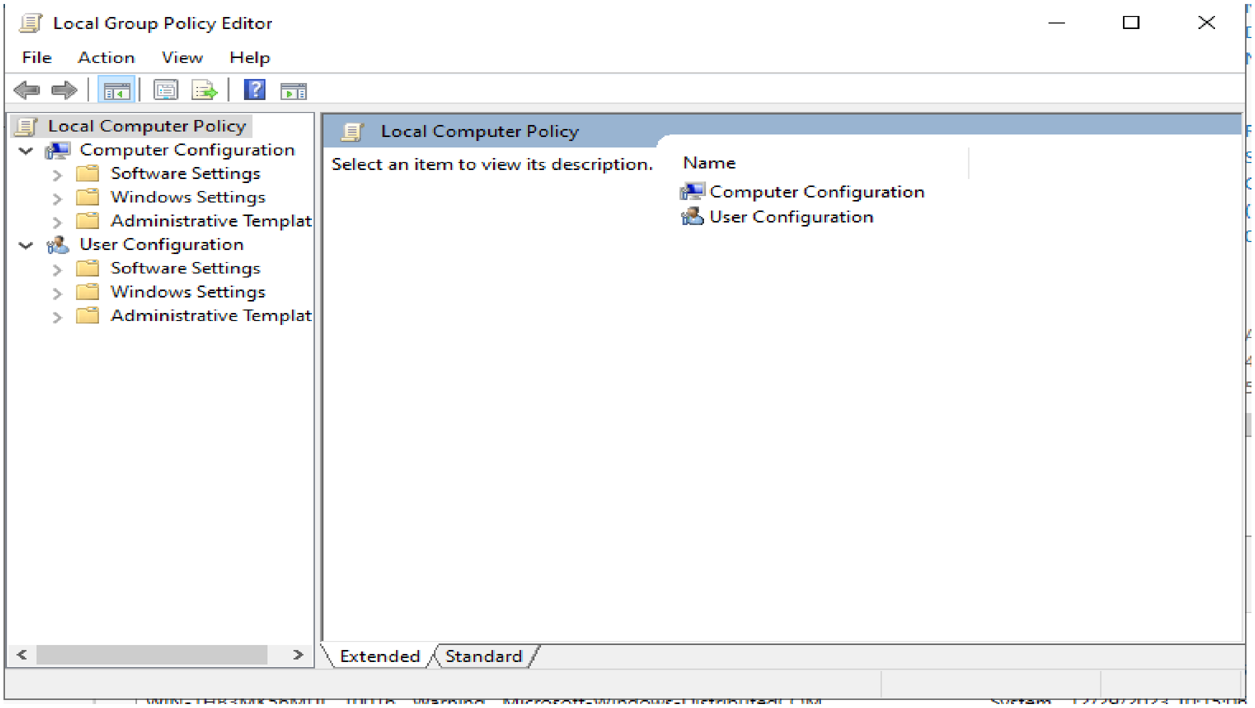
- Let’s proceed to the connection.



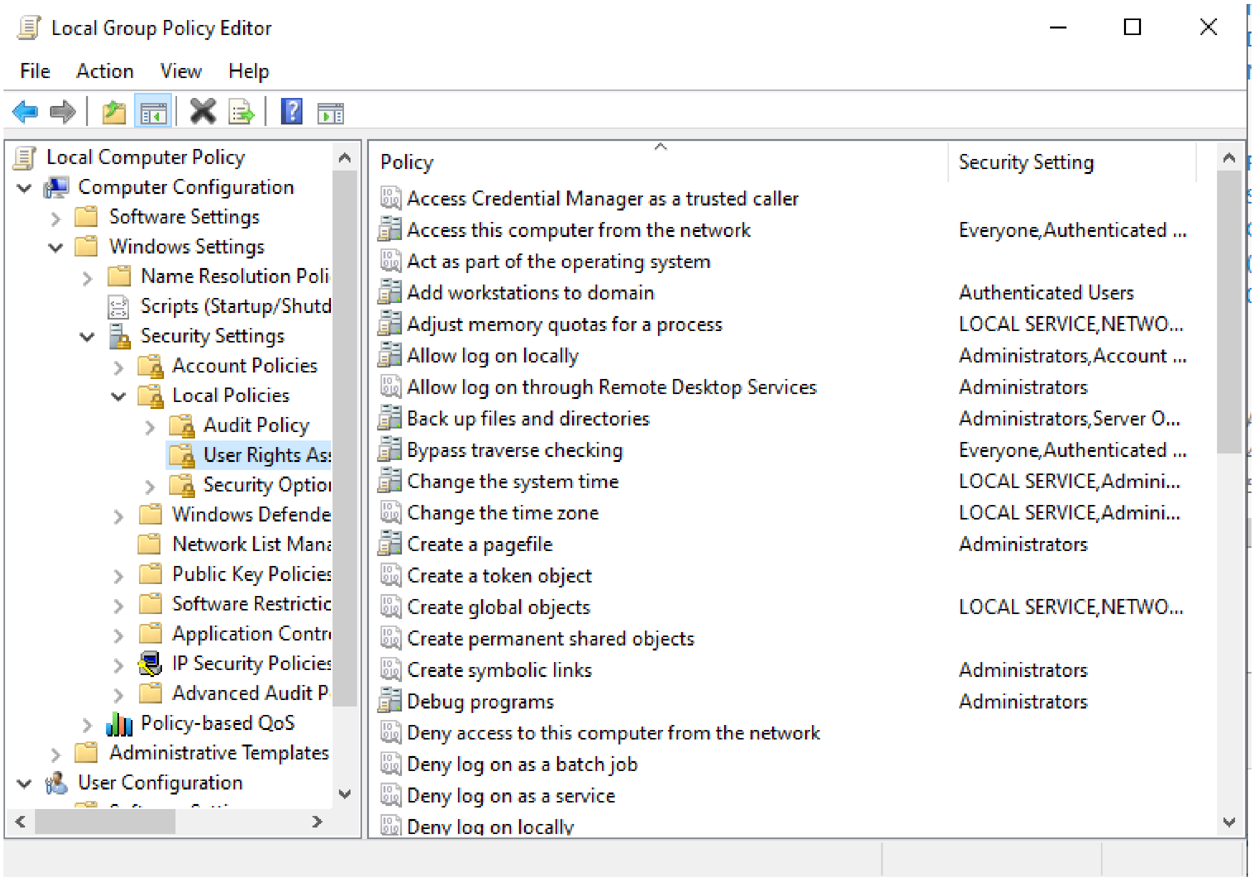
Other user

To sign in remotely, you need the right to sign in through Remote Desktop Services. By default, members of the Administrators group have this right. If the group you're in doesn't have this right, or if the right has been removed from the Administrators group, you need to be granted this right manually.

- Well, it did seem like we successfully connected to File Server but it said that we didn’t have the right to use this machine.
- We can allow this user to use this machine by editing group policy on File Server.
- Go to File Server and search for “Edit Group Policy” at the search bar.

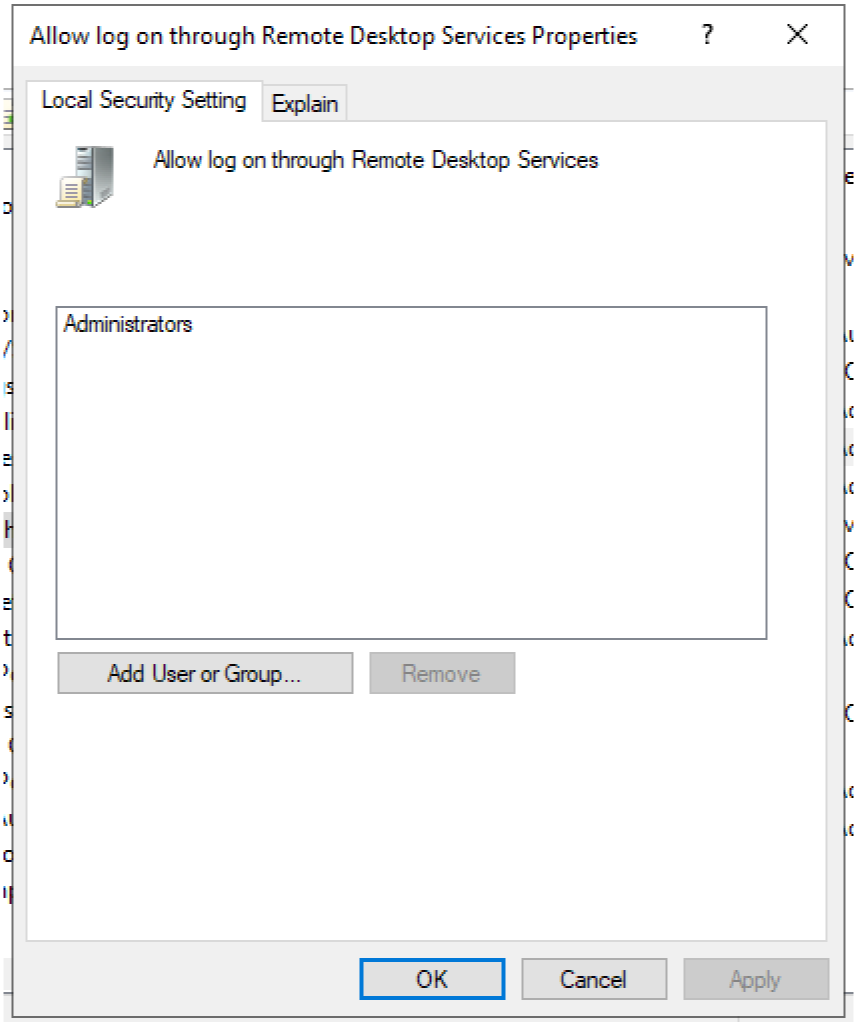


- "Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> User Rights Assigment".
- Find "Allow log on through Remote Desktop Services" then double click on it.



Policy	Security Setting
Access Credential Manager as a trusted caller	
Access this computer from the network	Everyone,Authenticated ...
Act as part of the operating system	
Add workstations to domain	Authenticated Users
Adjust memory quotas for a process	LOCAL SERVICE,NETWO...
Allow log on locally	Administrators,Account ...
Allow log on through Remote Desktop Services	Administrators
Back up files and directories	Administrators,Server O...
Bypass traverse checking	Everyone,Authenticated ...
Change the system time	LOCAL SERVICE,Admini...
Change the time zone	LOCAL SERVICE,Admini...
Create a pagefile	Administrators
Create a token object	
Create global objects	LOCAL SERVICE,NETWO...
Create permanent shared objects	
Create symbolic links	Administrators
Debug programs	Administrators
Deny access to this computer from the network	
Deny log on as a batch job	
Deny log on as a service	
Deny log on locally	

- "Add User or Group".

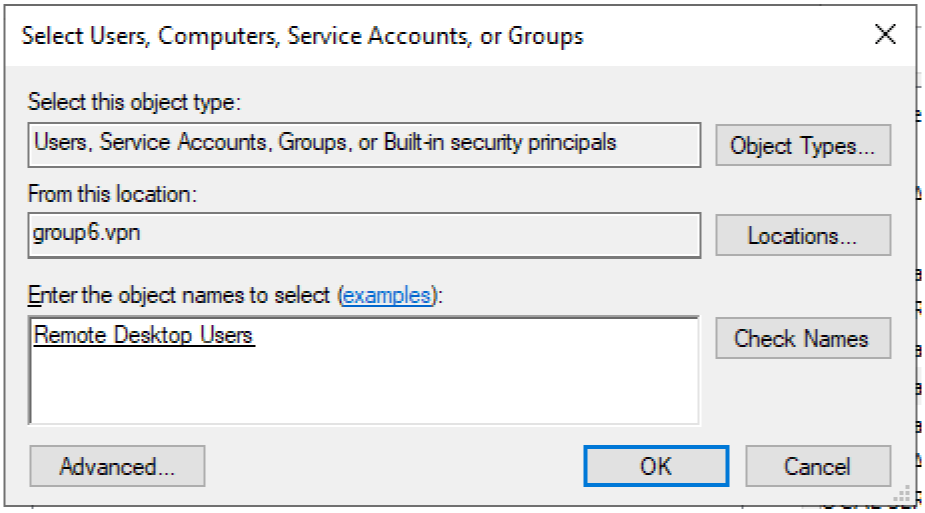


Allow log on through Remote Desktop Services Properties

Allow log on through Remote Desktop Services

Administrators

- Type in "Remote Desktop Users", that means any user in this group will have the right to use this machine through Remote Desktop Service then "Apply".

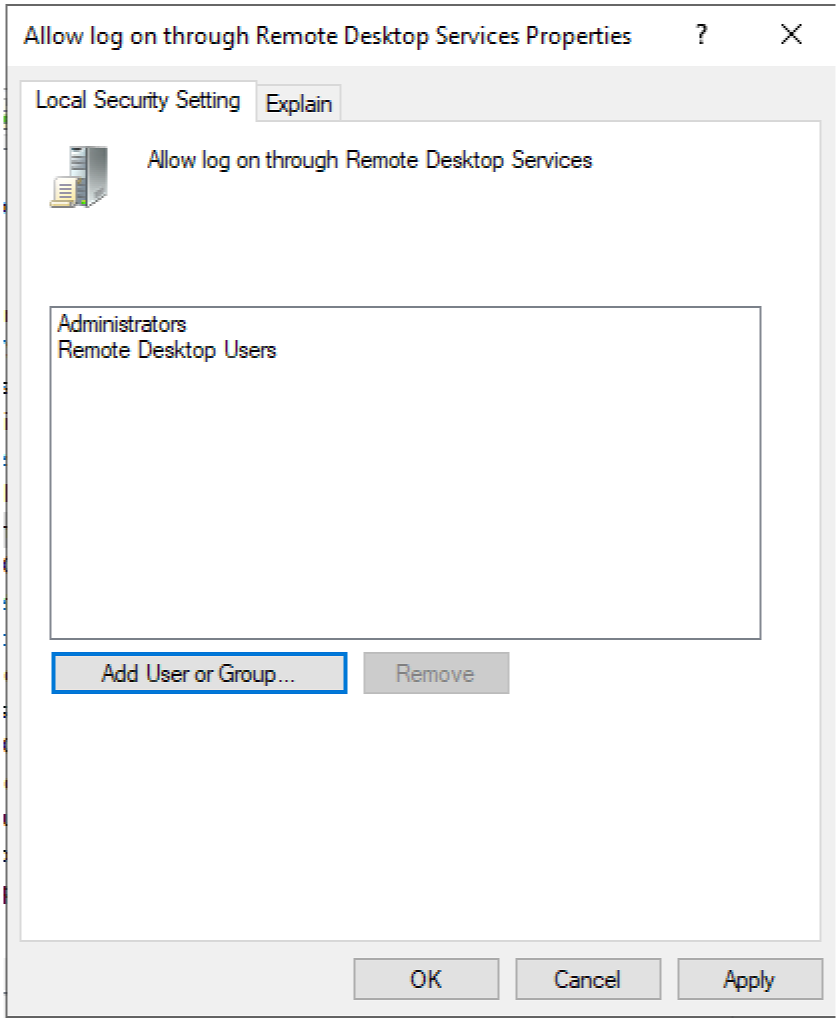


Select Users, Computers, Service Accounts, or Groups

Select this object type:
Users, Service Accounts, Groups, or Built-in security principals

From this location:
group6.vpn

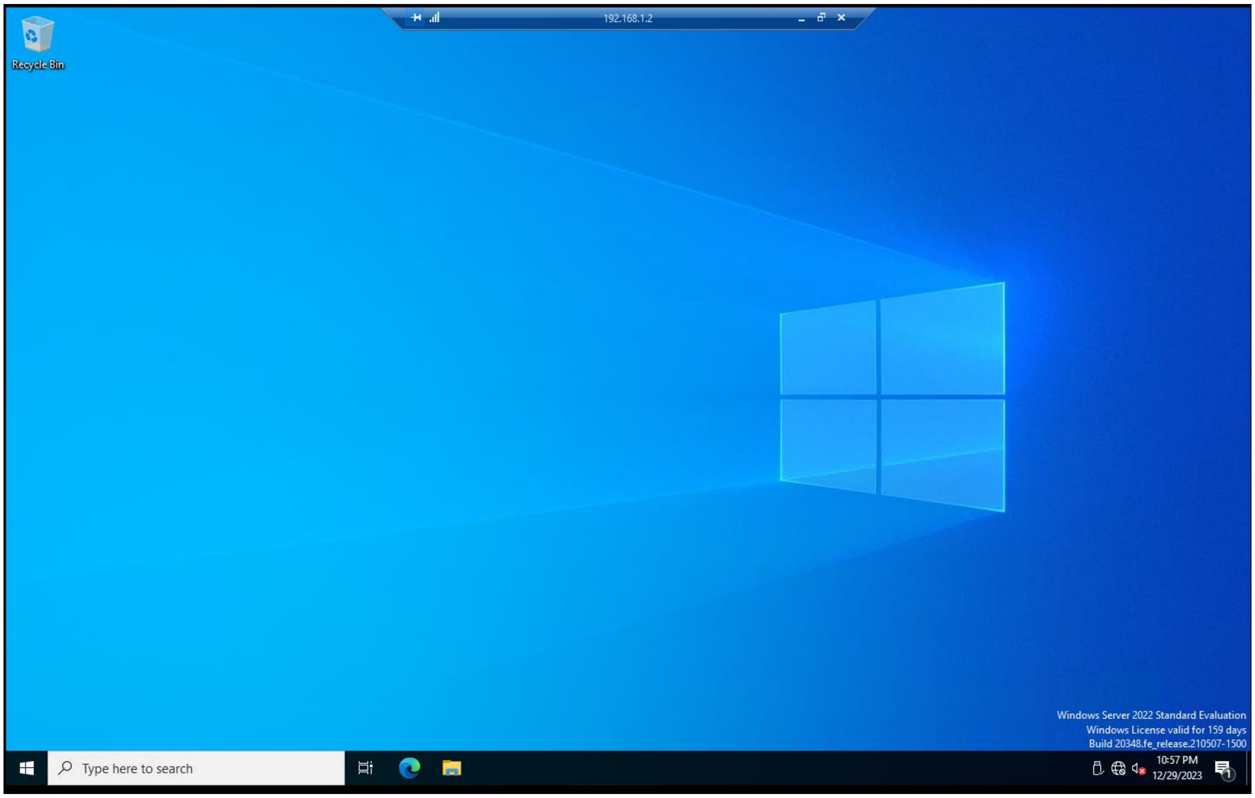
Enter the object names to select (examples):
Remote Desktop Users



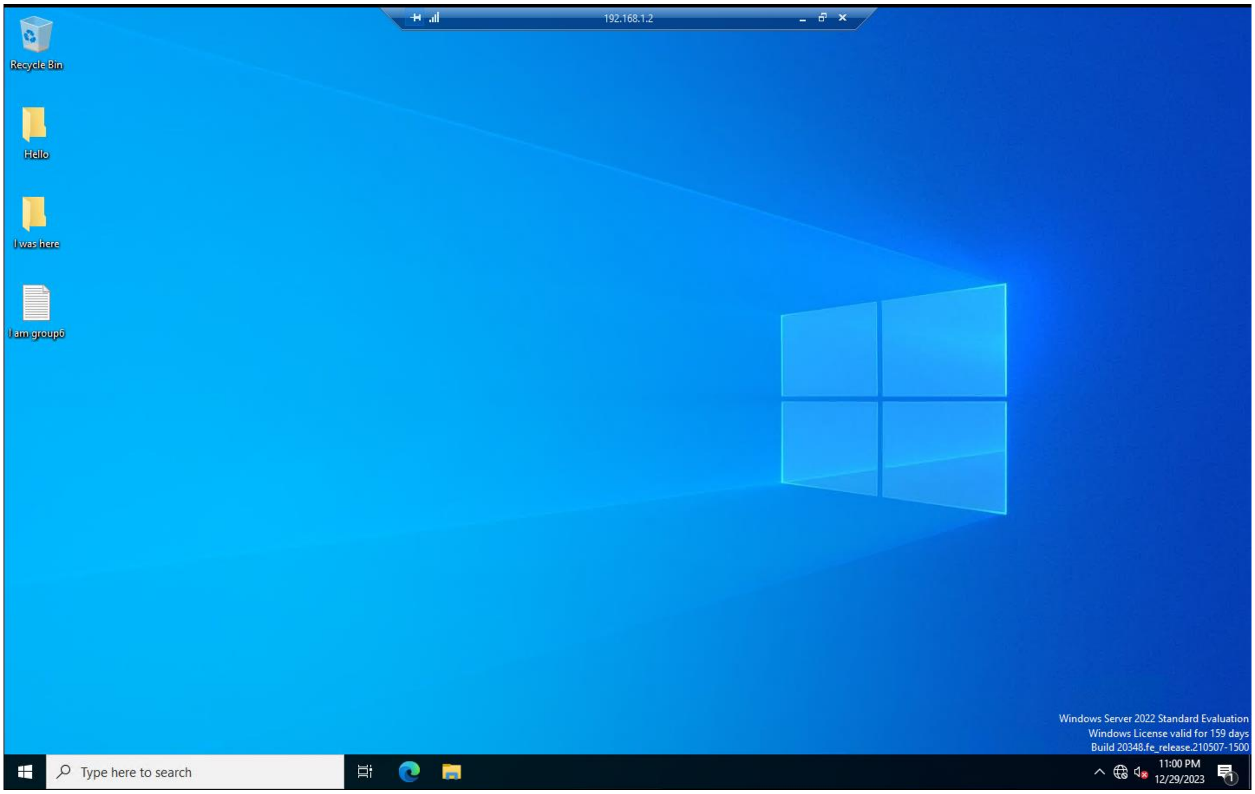
Allow log on through Remote Desktop Services

Administrators
Remote Desktop Users

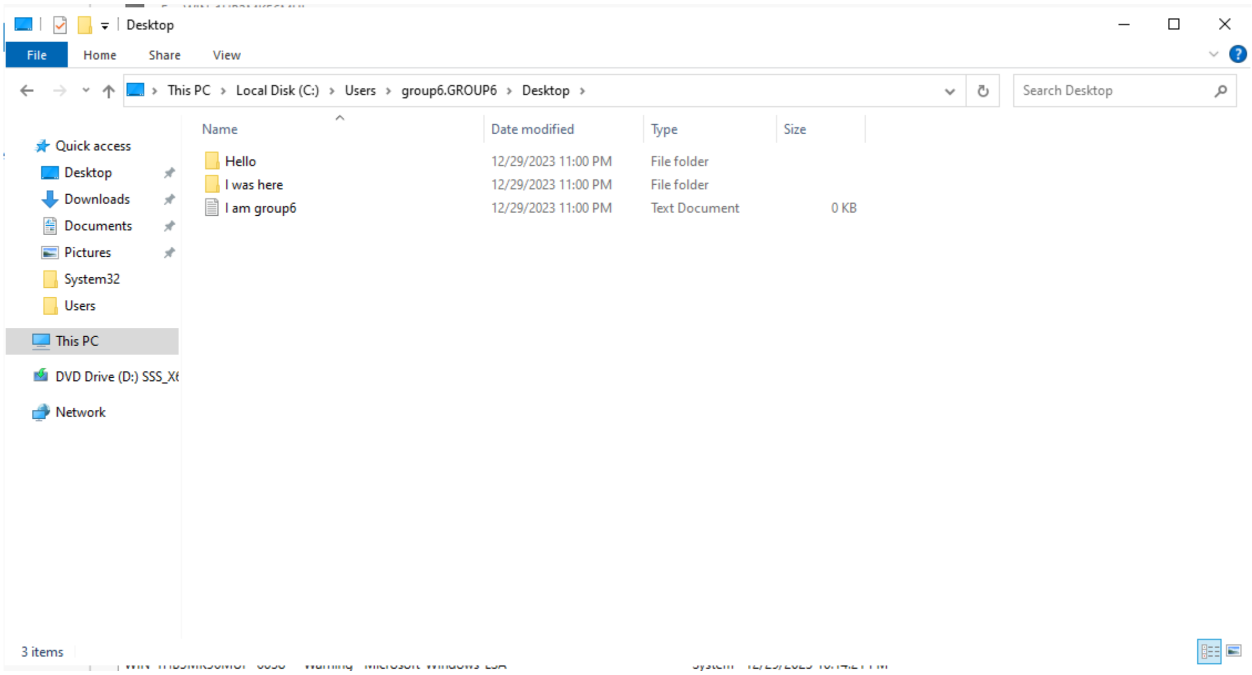
- Now, we will go back to Client's machine and test the Remote Connection.


Recycle Bin
192.168.1.2
Windows Server 2022 Standard Evaluation
Windows License valid for 159 days
Build 20348.fe_release.210507-1500
Type here to search
10:57 PM
12/29/2023

- This time, we successfully connected to the File Server Desktop and started using it.
- Let’s add some folder and .txt file at the desktop.


192.168.1.2
Recycle Bin
Hello
I was here
I am group6
Windows Server 2022 Standard Evaluation
Windows License valid for 159 days
Build 20348.fe_release.210507-1500
Type here to search
11:00 PM
12/29/2023

- Go back to File Server and see if there's any change on user's folder.



Name	Date modified	Type	Size
Hello	12/29/2023 11:00 PM	File folder	
I was here	12/29/2023 11:00 PM	File folder	
I am group6	12/29/2023 11:00 PM	Text Document	0 KB

And that's all we've done regarding setting up a VPN server on a Windows server as well as implementing remote desktop.

IV. APPENDIX

4.1 Self-evaluation

Report format	Presentation	Theory	Demonstration
3	**3**	**2**	**3**

4.2 Task Assignment

Members	Tasks	Percentage of Completing
Lý Thế Nguyên	Report, Theory, Configuration, Demonstration	100%
Trần Phúc Hoàng Duy	Report, Theory, Installation, Configuration	100%
Lê Triệu Vĩ	Report, Theory, Configuration, Advance	100%

4.3 Question and answer

Q: Làm sao để thiết lập và quản lý các kết nối VPN từ xa trên Windows Server để cho phép người dùng truy cập an toàn vào mạng nội bộ?

A:
- Trên window server, thiết lập các giao thức như PPTP, L2TP, OpenVPN,…
- Cấu hình xác thực bao gồm username/password hoặc certificate
- Theo dõi và quản lý các kết nối VPN thông qua Remote Access Mangement.
- Kiểm tra log để theo dõi các hoạt động và vấn đề liên quan đến kết nối VPN

Q: how vpn manage user for specific roles?

A: VPNs can manage user roles and access through a few differents methods like: User Authentication and Authorization, Role-Based Access Control, Network Access Policies

Q: Why can you hide your ip when using vpn, and can any party know your ip when using vpn to access?

A: - When you connect to a VPN, your device establishes a connection with the VPN server. Your internet requests are then forwarded through this server. Any webiste or servie you access sees the IP address of the VPN server instead of your actual IP address.

- Your VPN provider can see your real IP address because they handle the initial connection. An ISP can also see a connections is being made to a VPN server.

Q: Explain the VPN tunnel in your deploy

A: - First of all, any data transmitted from the user's device to the VPN server is encapsulated. A packet header is added to the original data packet, creating an outer packet.

- The outer packet which now includes the original data packet and the additional header is encrypted. This encryption secures the entire packet.
- Upon reaching the VPN server, the encrypted packet is received and decrypted using appropriate keys. The outer packet header is removed, leaving the original data packet intact.
- The packet is now available on the private network and forwarded to its intended destination.