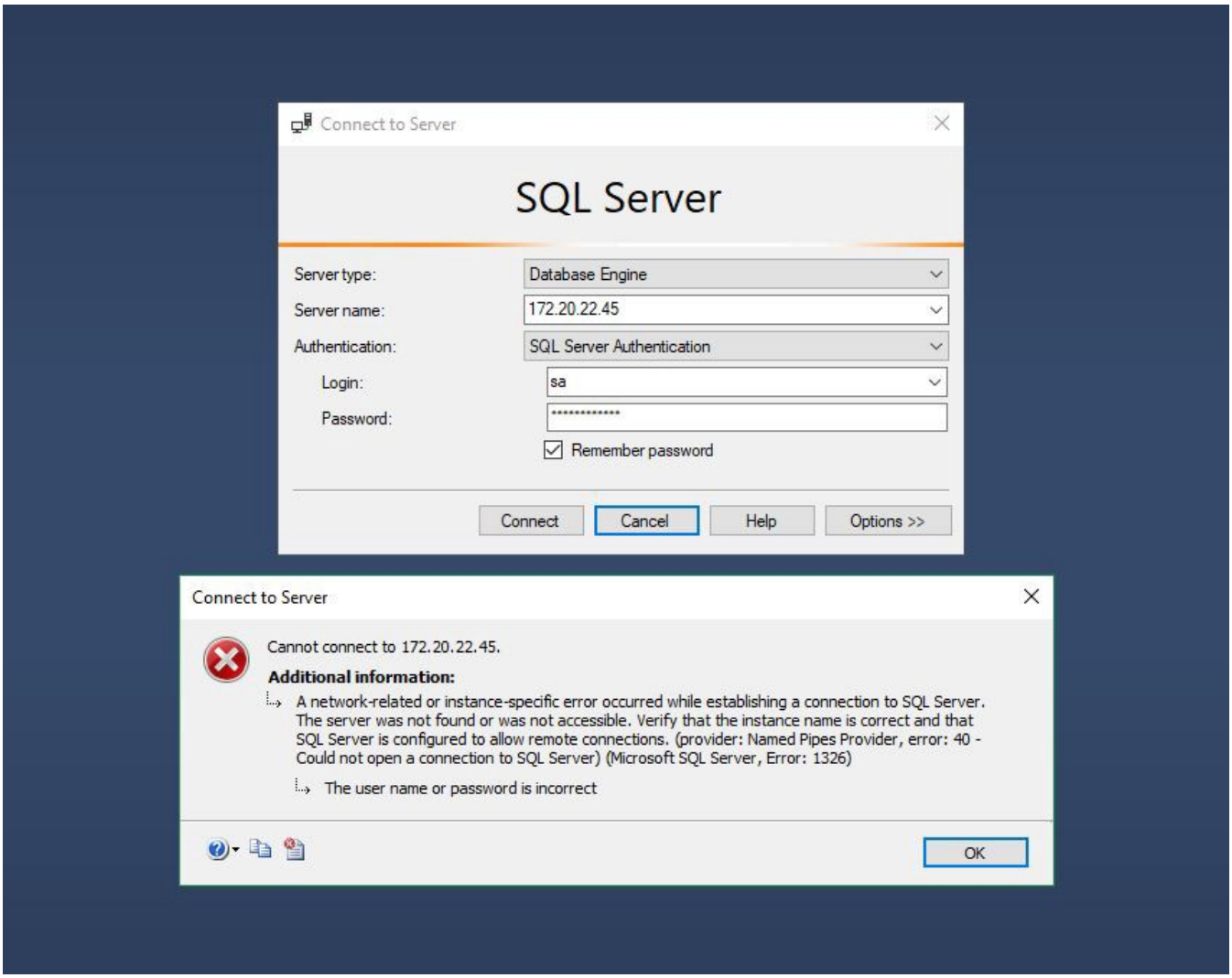
Nishan Chathuranga Wickramarathna

Follow 174 Followers About

How to enable remote connections to SQL Server

Nishan Chathuranga Wickramarathna Feb 4, 2019 · 5 min read



Problem in hand

So you have a VM or a remote server, that you have installed SQL Server, but you also want to connect to SQL Server using SQL Server Management Studio on your local system, but gives you this error.

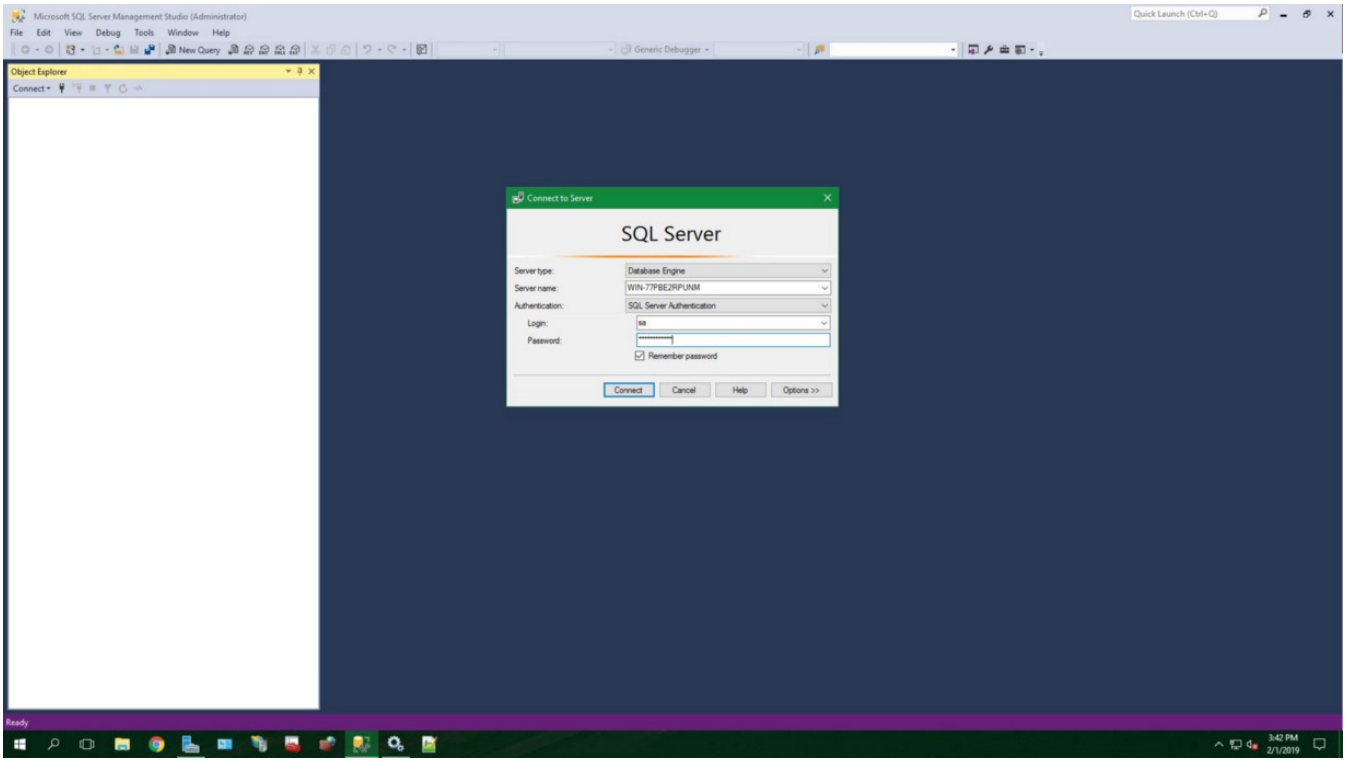
This is because you haven't configured it to allows inbound connections from firewall or from SQL Server itself, could be both.

Prerequisites

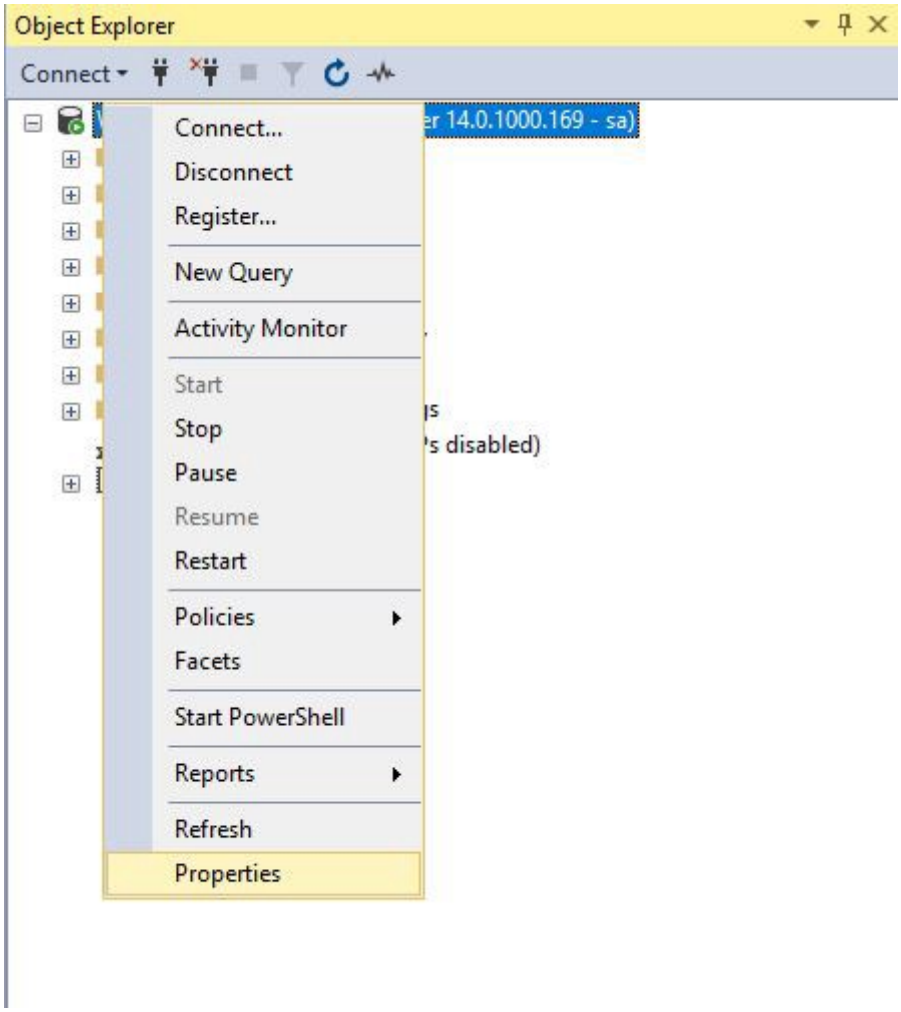
1. Remote server/VM must have SQL Server Management Studio and SQL Server Configuration Manager Installed.
2. Remote SQL Server must have a user that have read and write privileges (Here I'm using **sa** user)

All set, let's start

Connect to the server/VM using *Remote Desktop Connection* and open up SQL Server Management Stdio on remote server, then connect to the SQL Server instance.

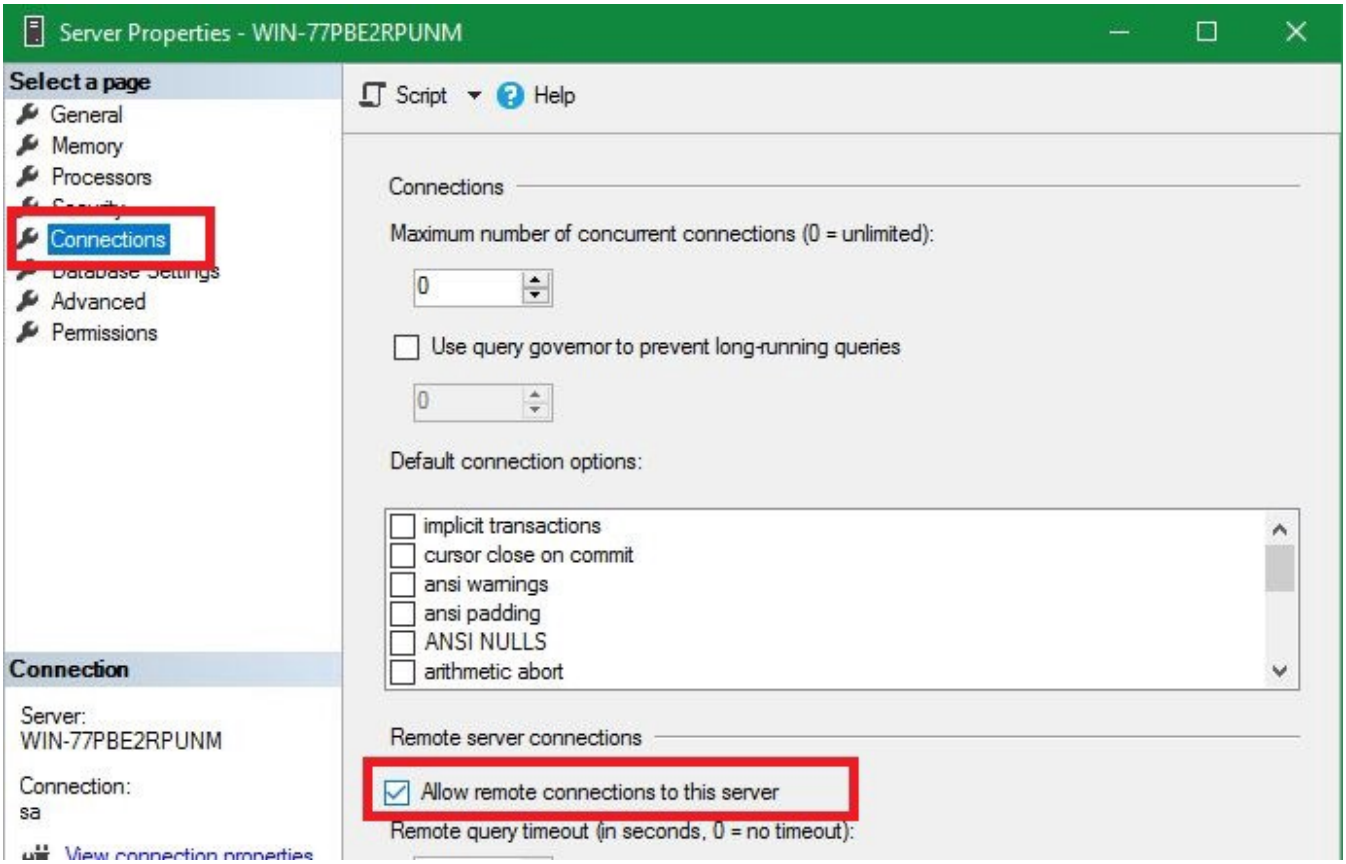


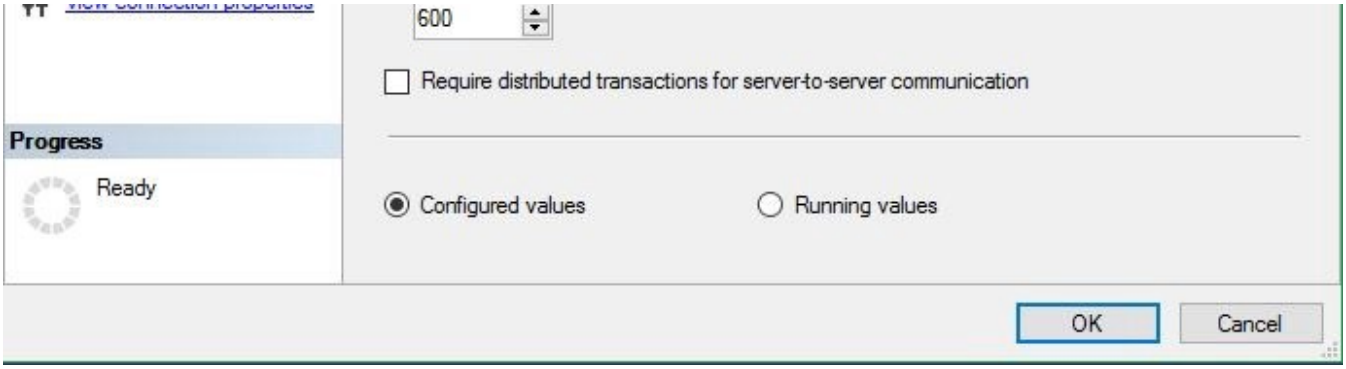
Connect to SQL Server instance from remote server.



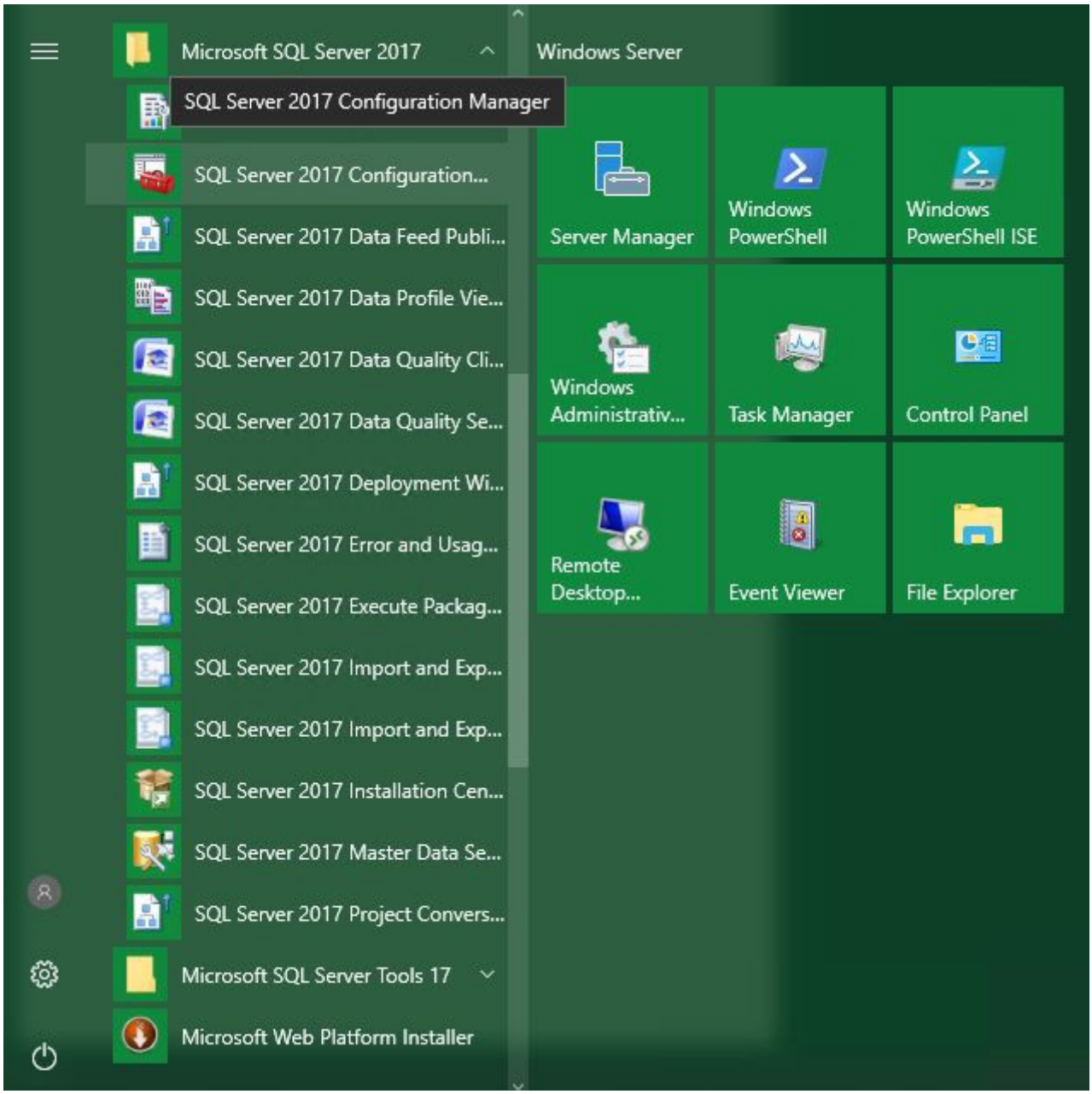
Go to server properties.

Now right click on the server and go to **Properties**.

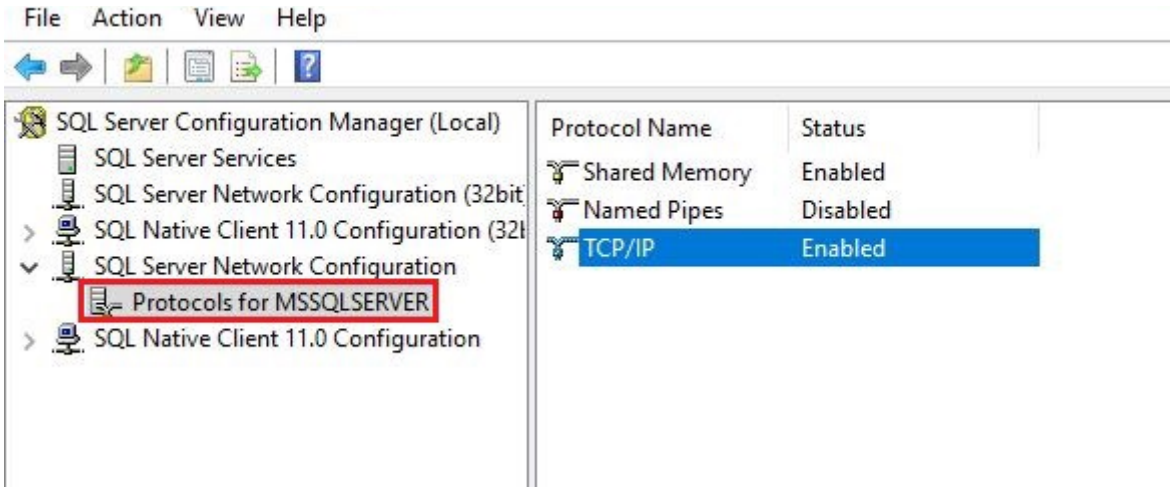




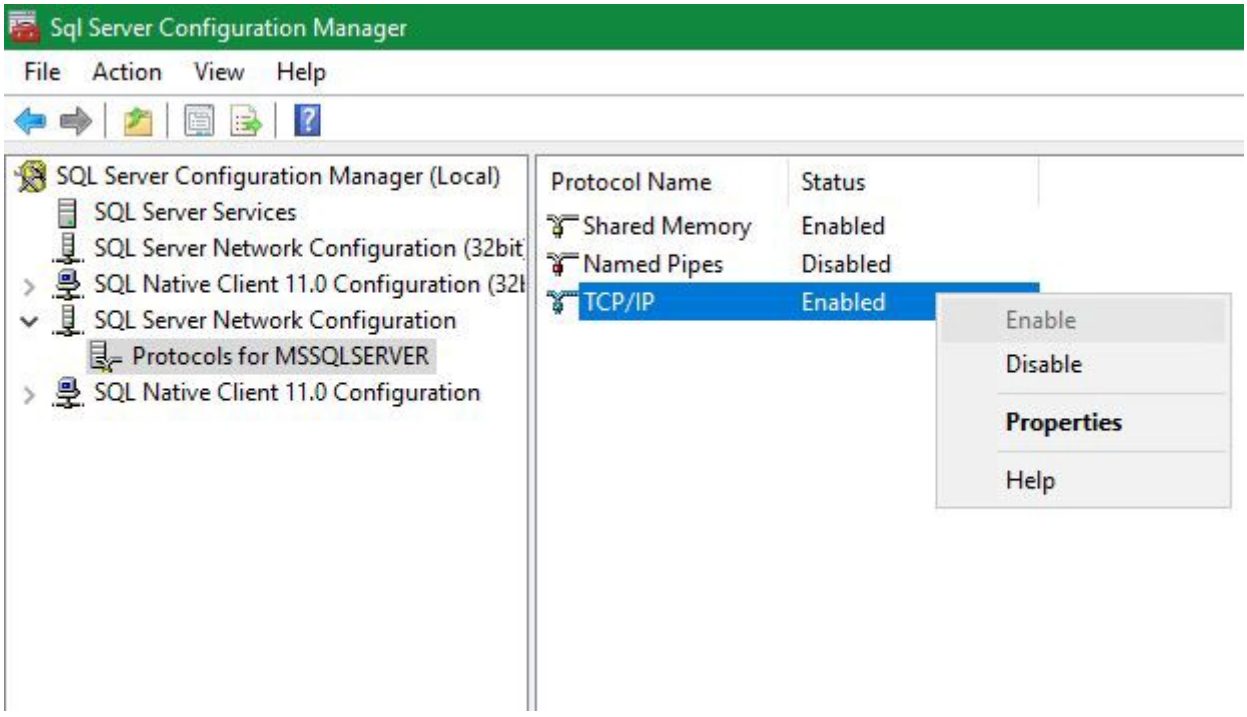
On the **Connections** page under **Remote server connections,** make sure that the **Allow remote connections to this server** is checked.

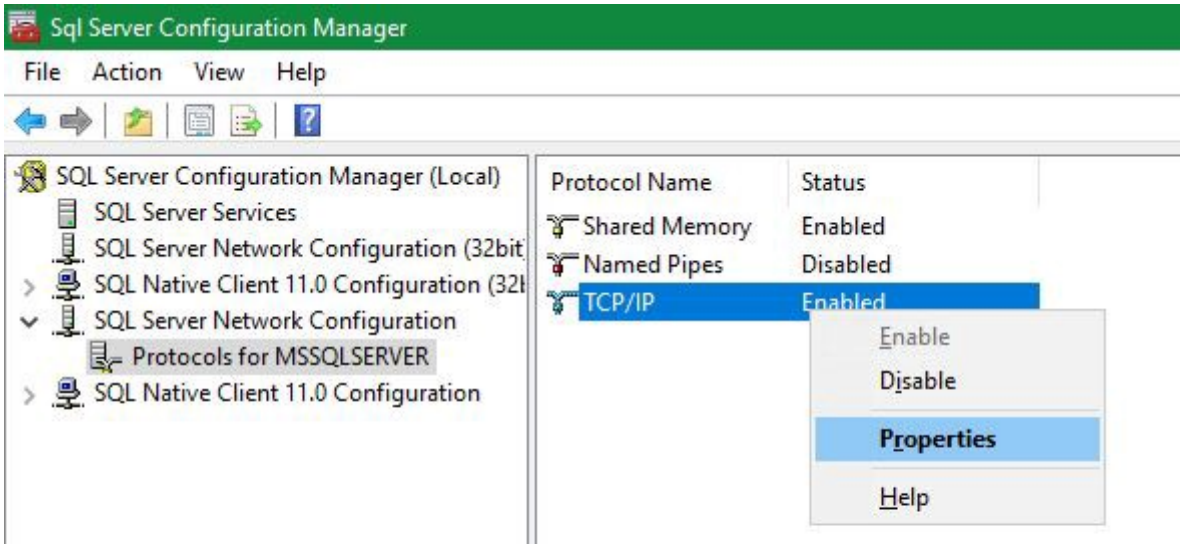


Now open **SQL Server Configuration Manager.**

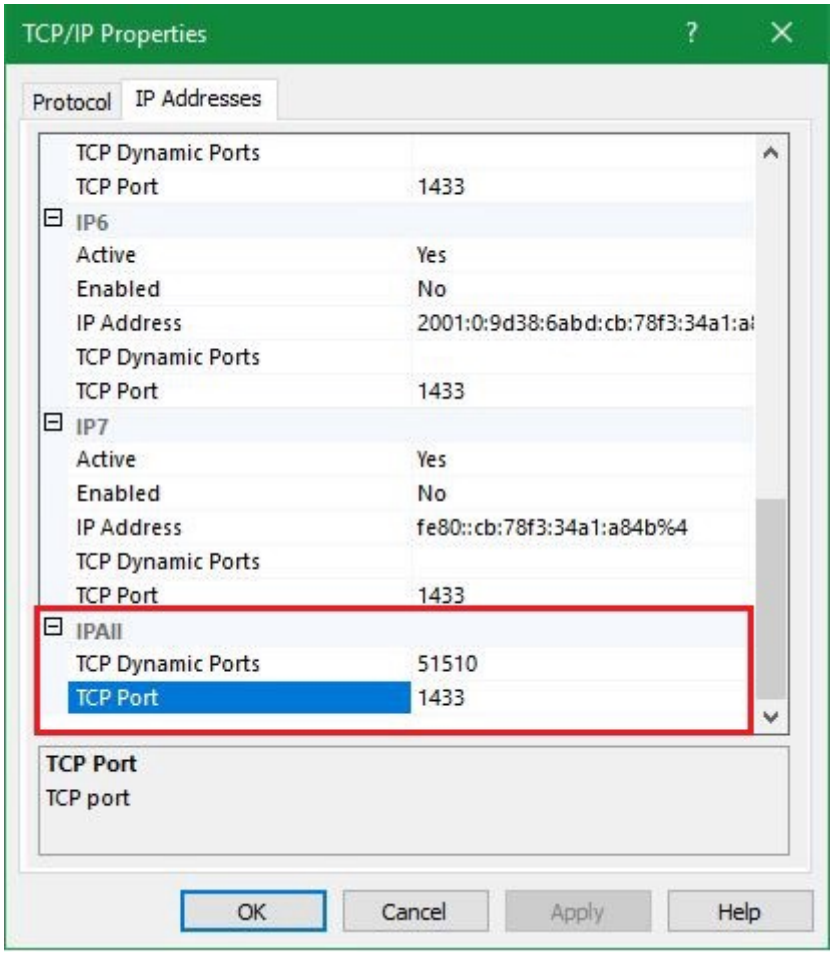


Visit **Protocols for <instance name>,** in my case **Protocols for MSSQLSERVER** under **SQL Server Network Configuration** node, go to **TCP/IP** and make sure the 'Status' is set to **Enabled.** If not, right click and select **Enable**.



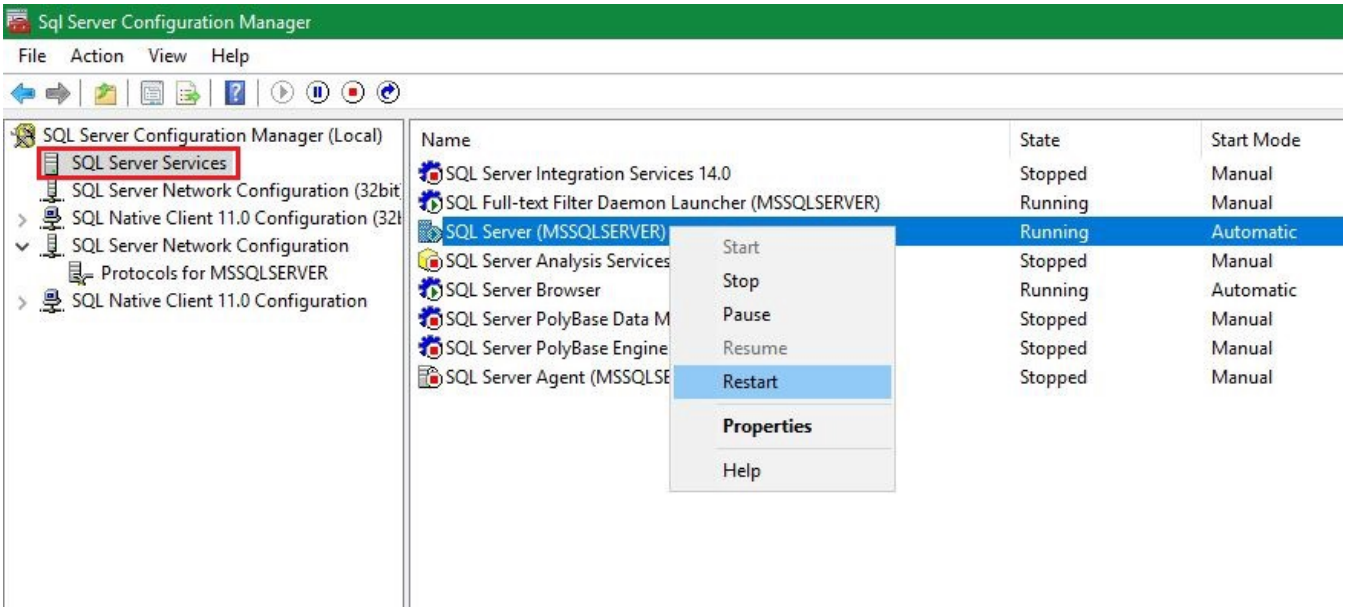


After that, again right click and select **Properties** of **TCP/IP** protocol.



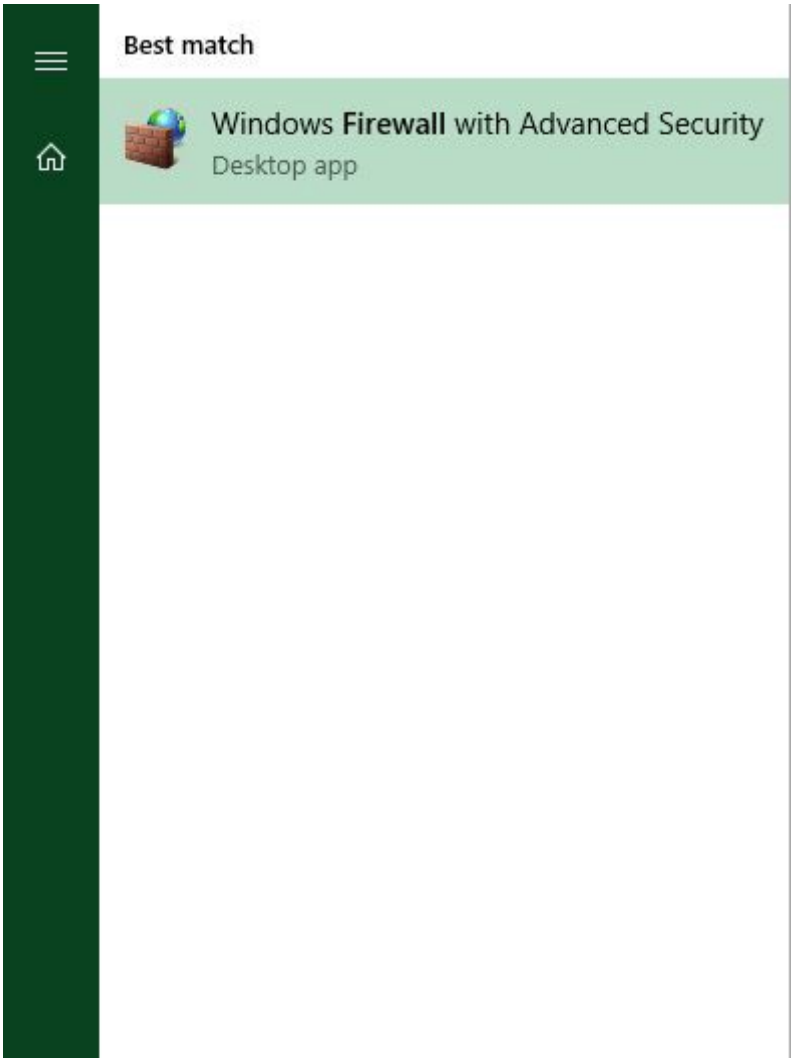
Goto **IP Addresses** tab and go down until you see **IPALL** section. Make sure the TCP Port is set to 1433. If not set it to 1433.

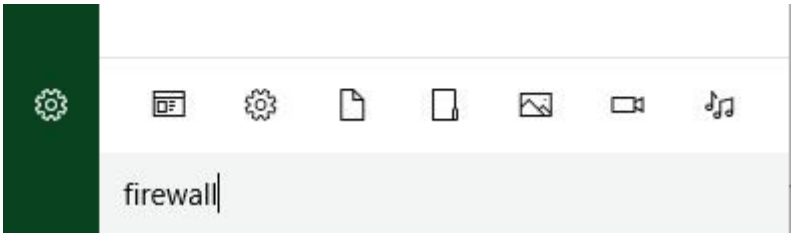
This warning will appear, so we need to restart the server. we can do it by using SQL Server Configuration manager.



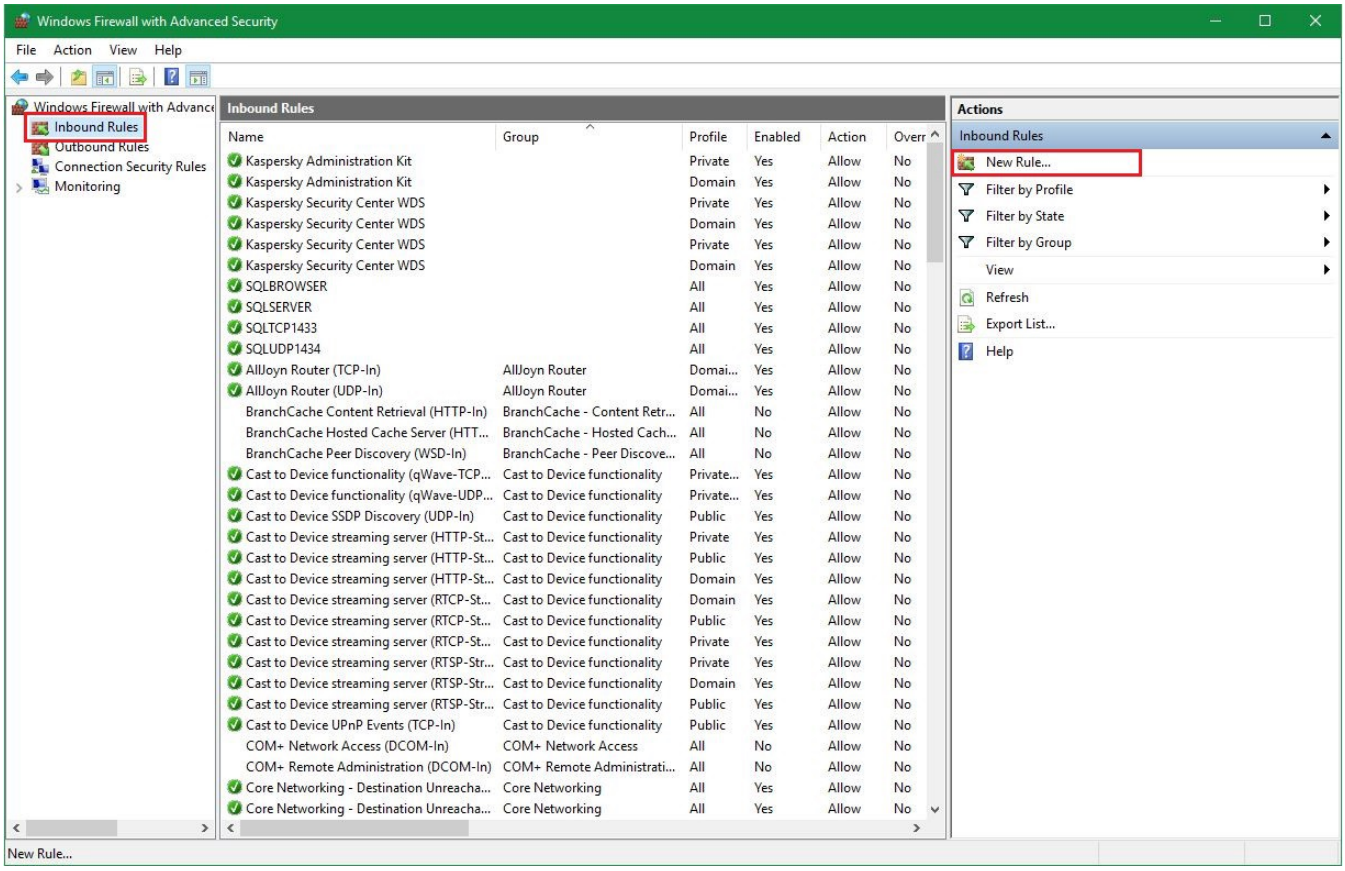
Locate **SQL Server** under SQL Server Services, right click and select **Restart.**

Now lets configure the firewall.





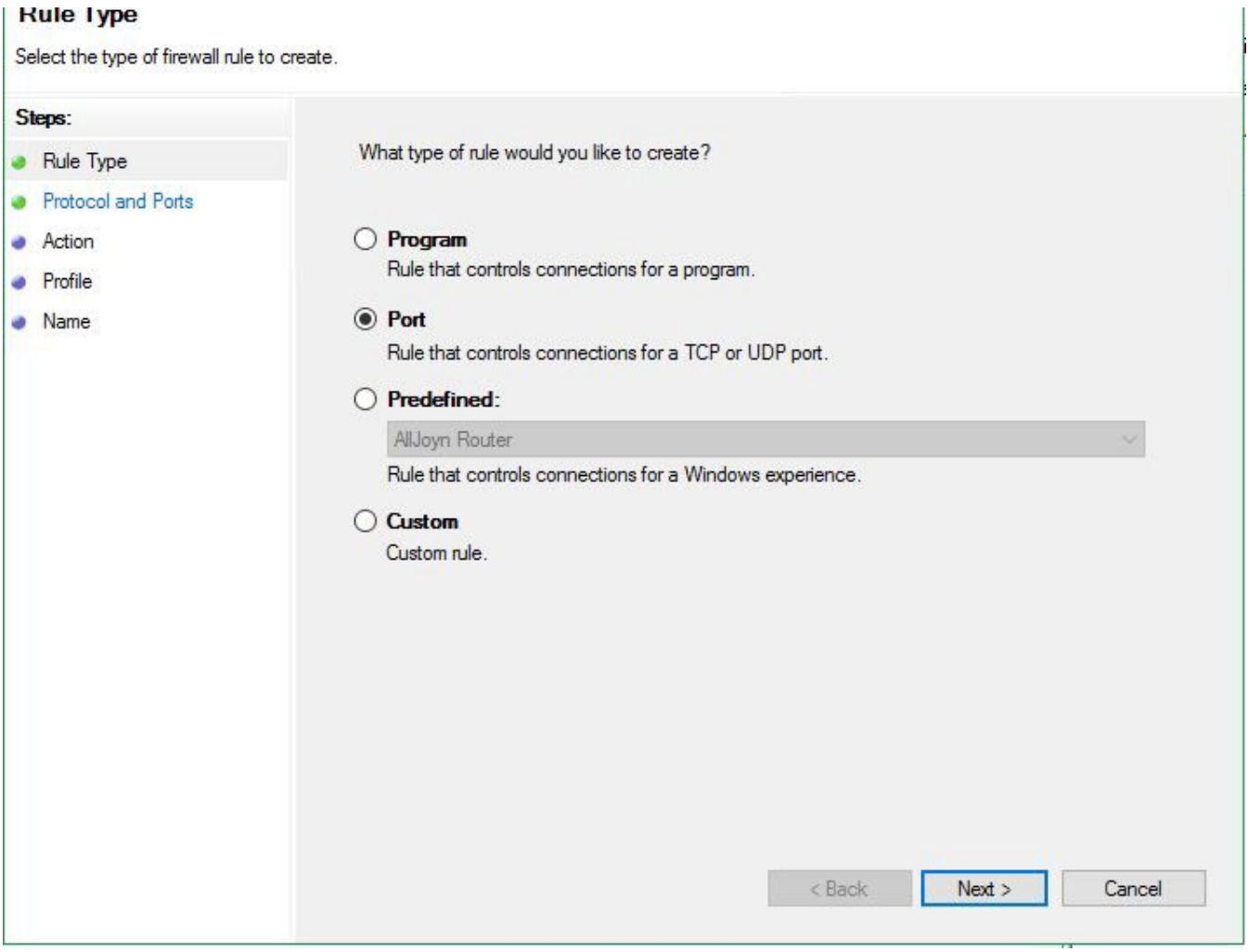
Open up **Windows Firewall.**

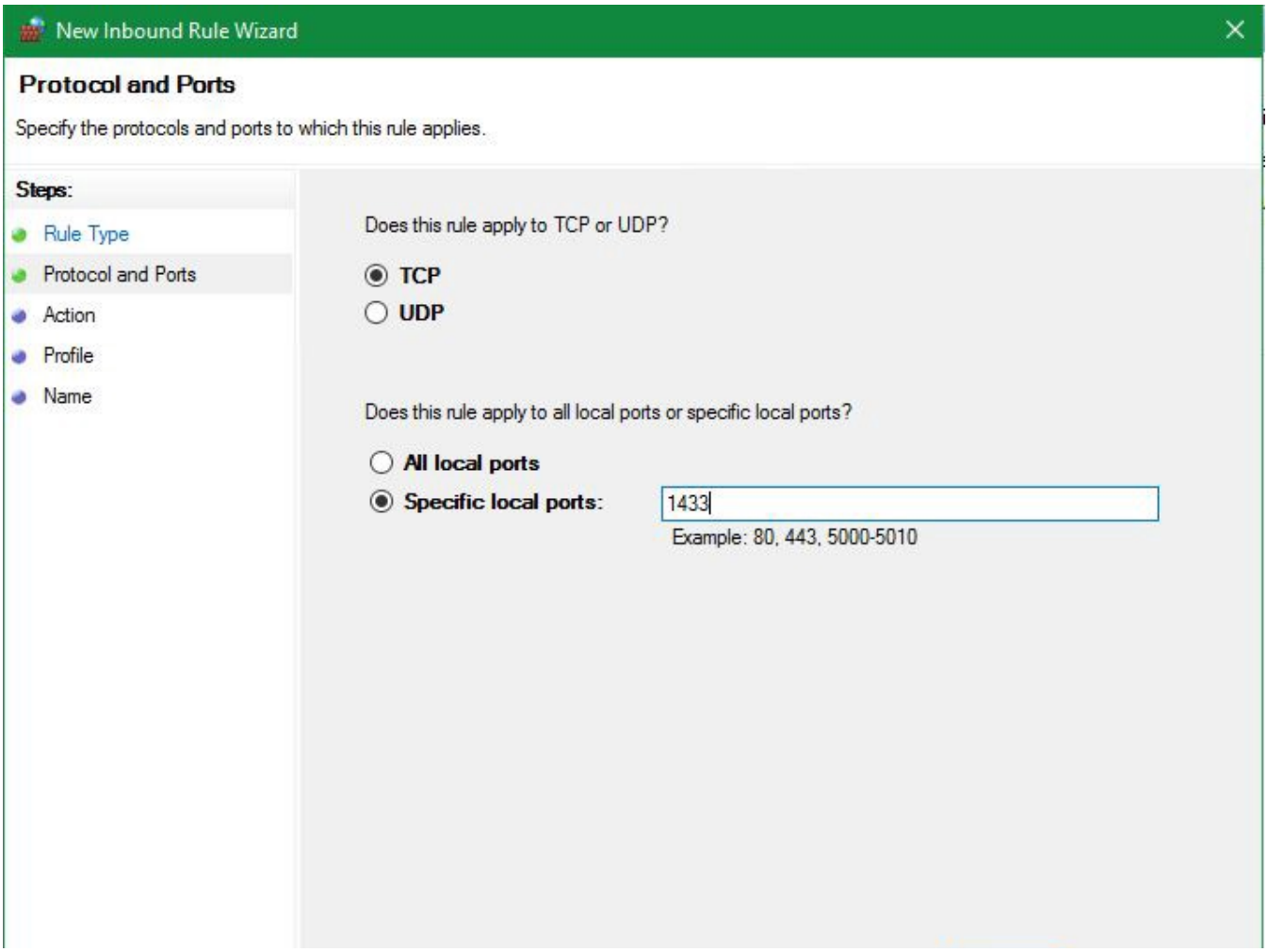


Go to **Inbound Rules** and select **New Rule.**

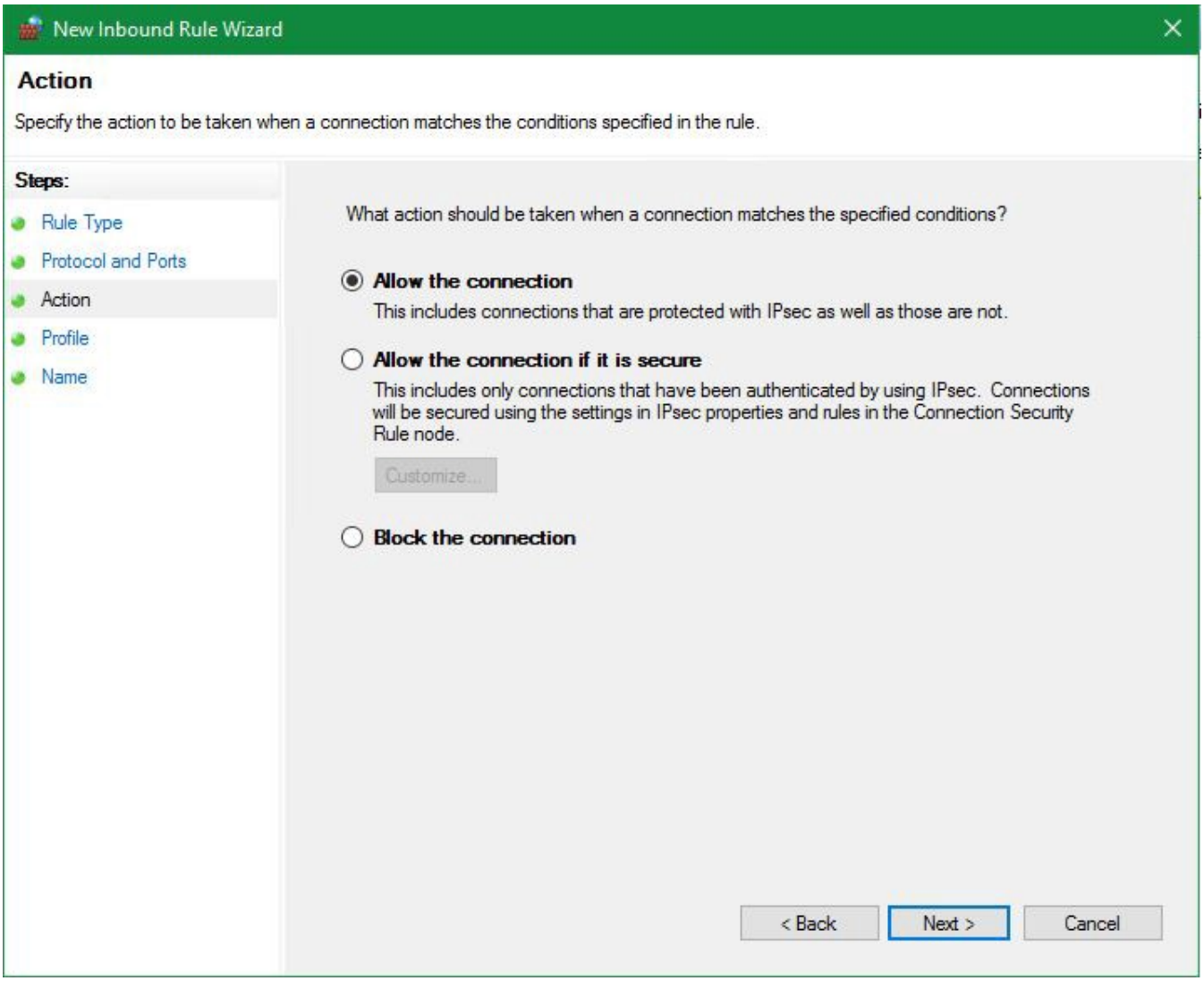
Add the following rule. Follow images if unclear.

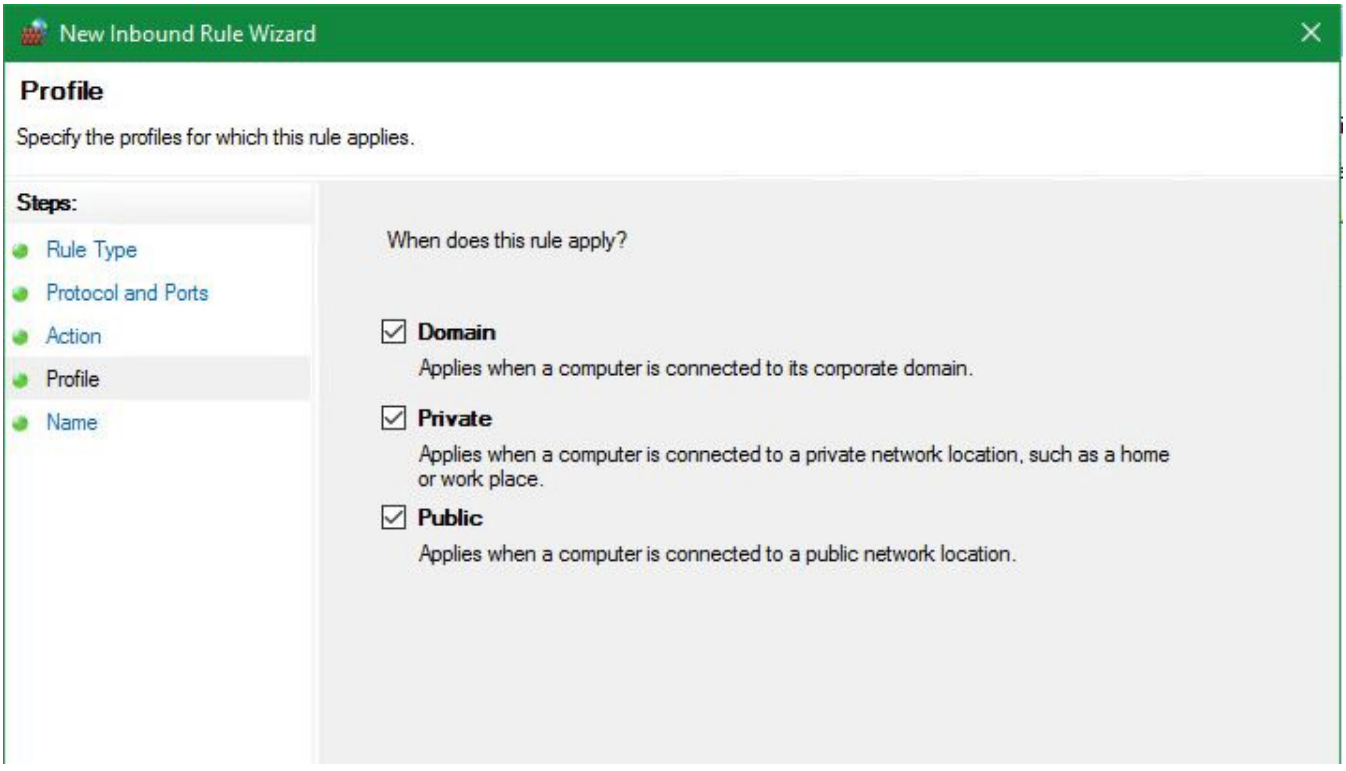
> *Rule Type:* ***Port***
>
> *Protocol and Ports:* ***TCP, 1433***
>
> *Action:* ***Allow the connection***
>
> *Profile:* ***Domain, Private, Public***
>
> *Name:* ***SQLTCP1433***

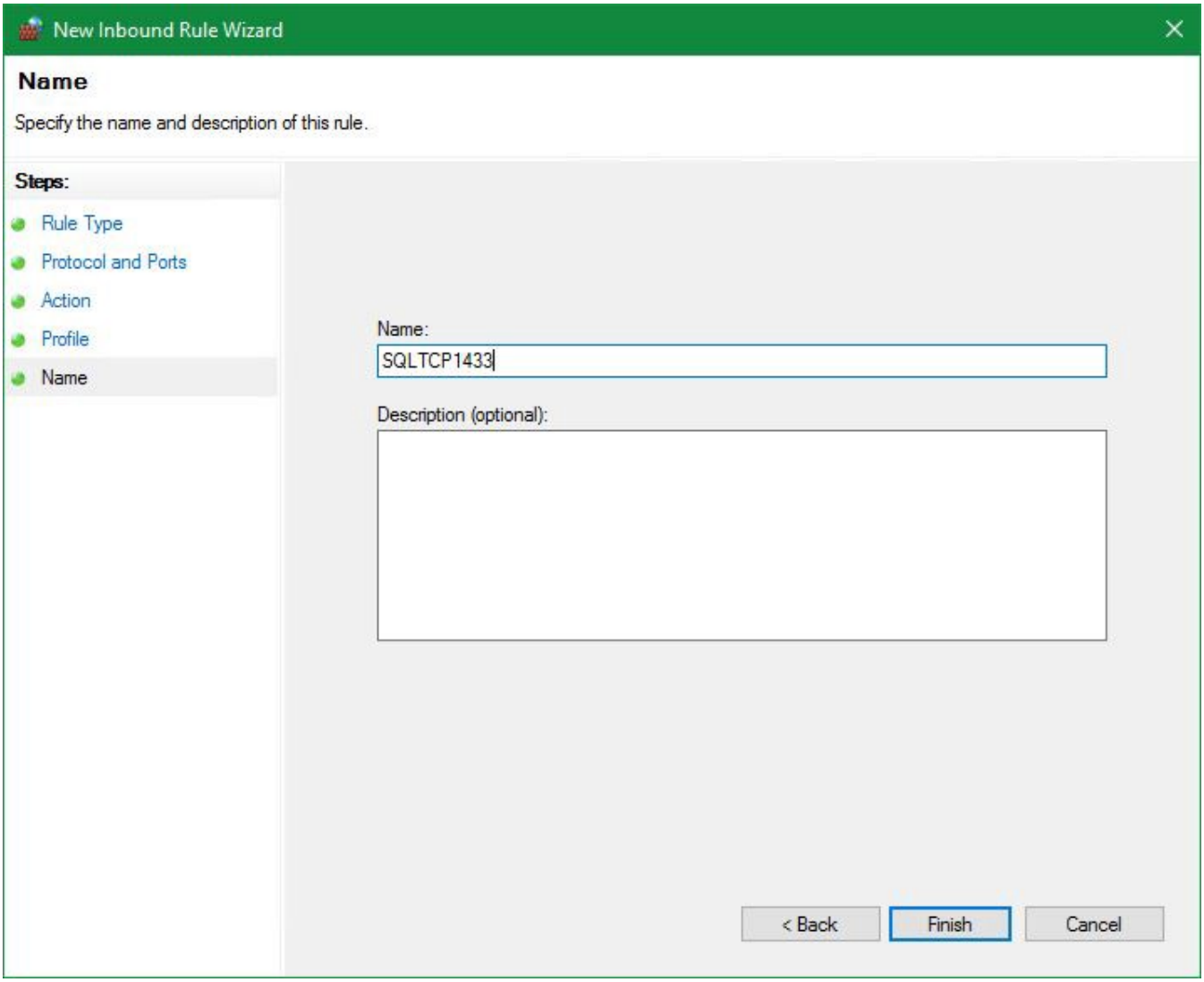

Rule Type
Select the type of firewall rule to create.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
What type of rule would you like to create?
Program
Rule that controls connections for a program.
Port
Rule that controls connections for a TCP or UDP port.
Predefined:
AllJoyn Router
Rule that 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:
1433
Example: 80, 443, 5000-5010


< Back
Next >
Cancel

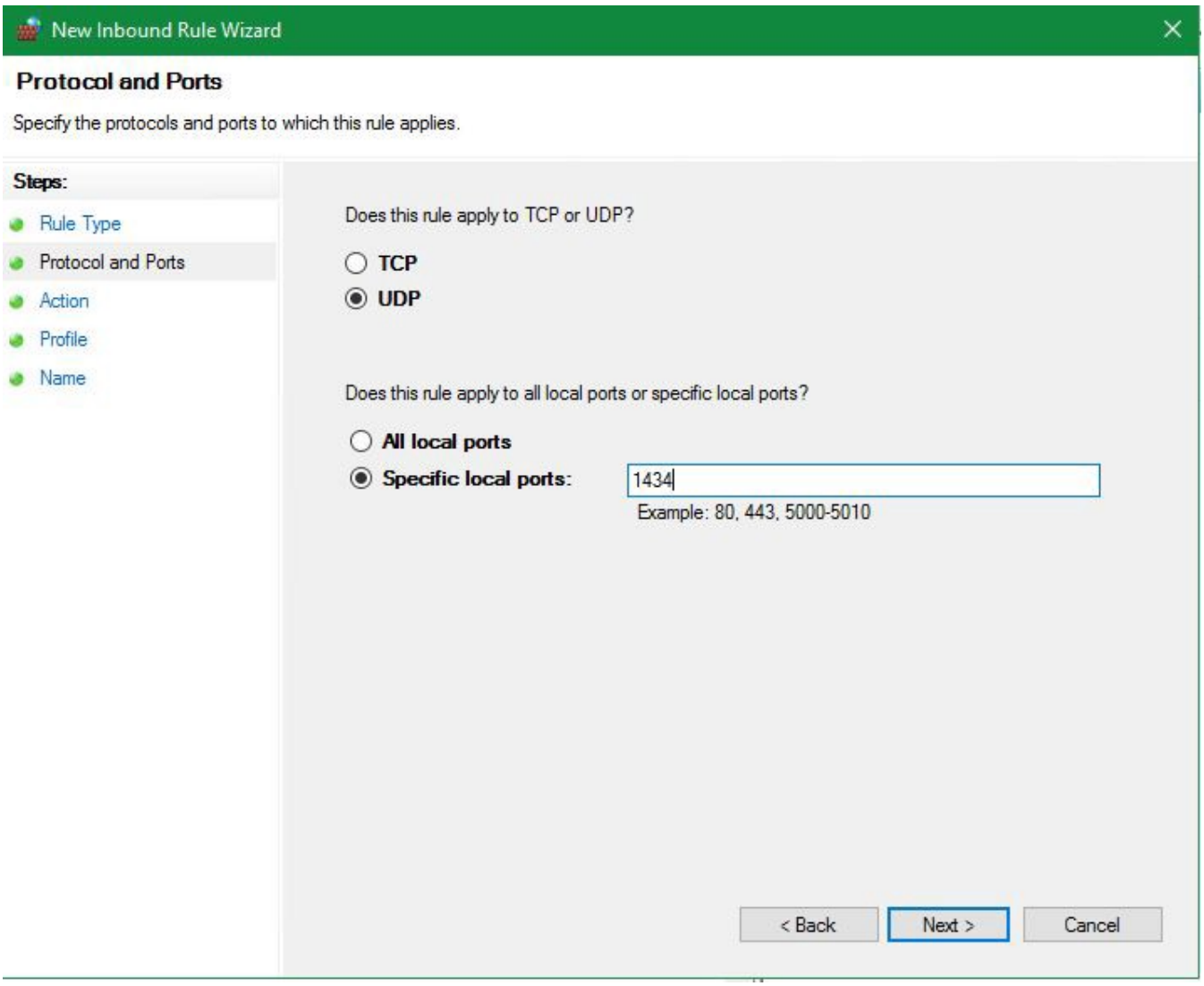

New Inbound Rule Wizard
Action
Specify the action to be taken when a connection matches the conditions specified in the rule.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
What action should be taken when a connection matches the specified conditions?
Allow the connection
This includes connections 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.



Click finish. We need to add another rule for UDP connections as well.

> *Rule Type:* ***Port***
>
> *Protocol and Ports:* ***UDP, 1434***
>
> *Action:* ***Allow the connection***
>
> *Profile:* ***Domain, Private, Public***
>
> *Name:* ***SQLUDP1434***

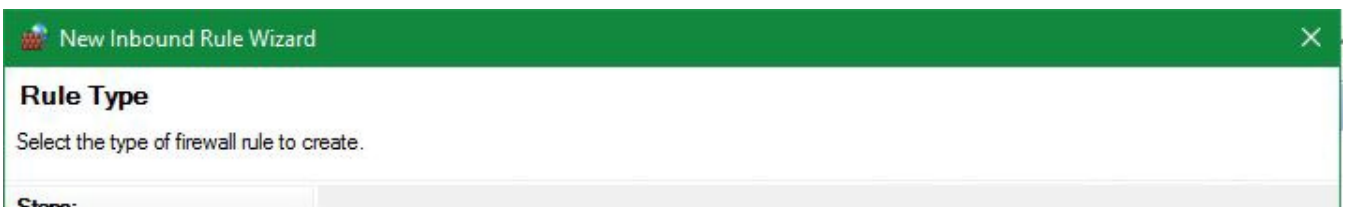


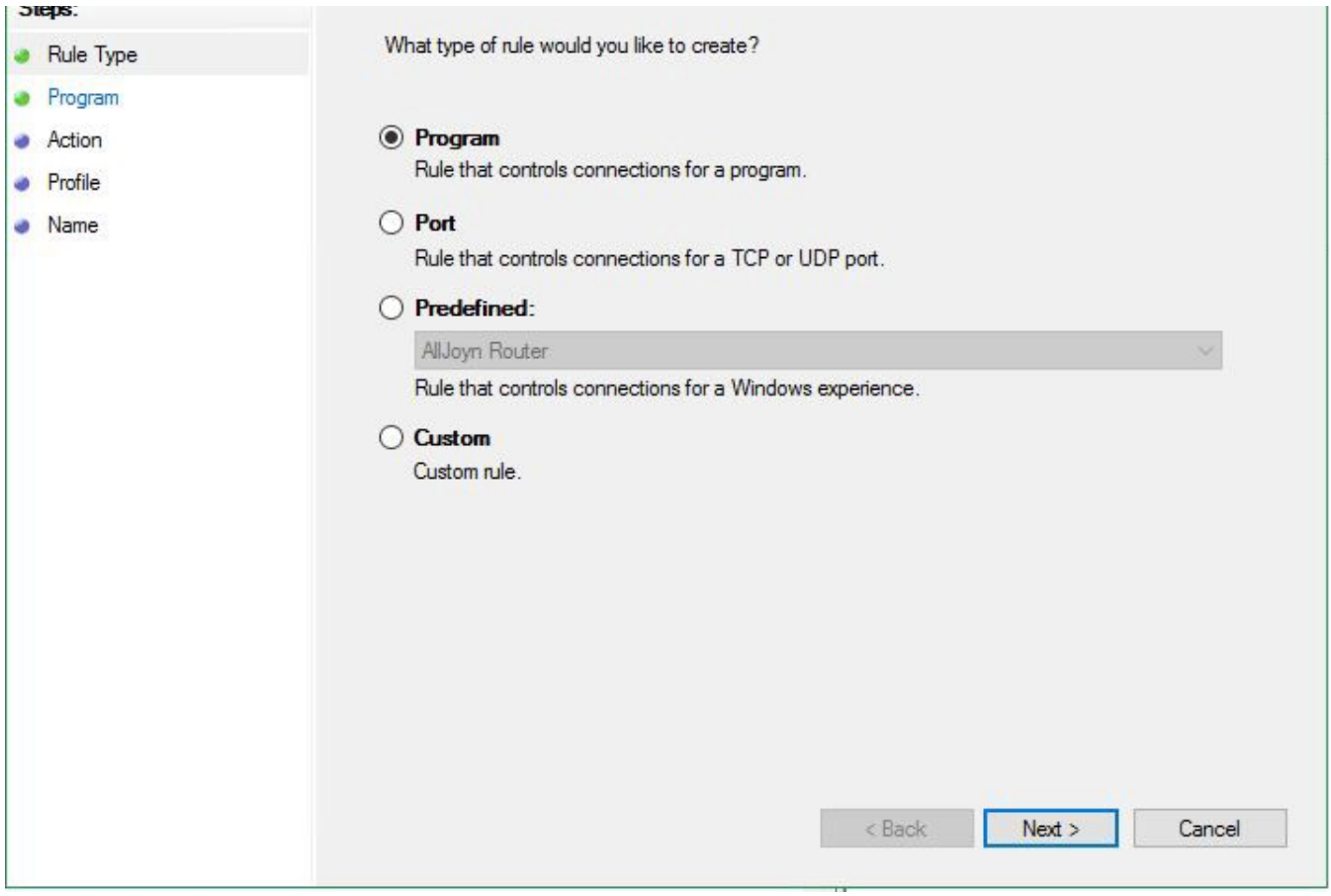
Let' make **SQL Server** and **SQL Server Browser** accessible through firewall.

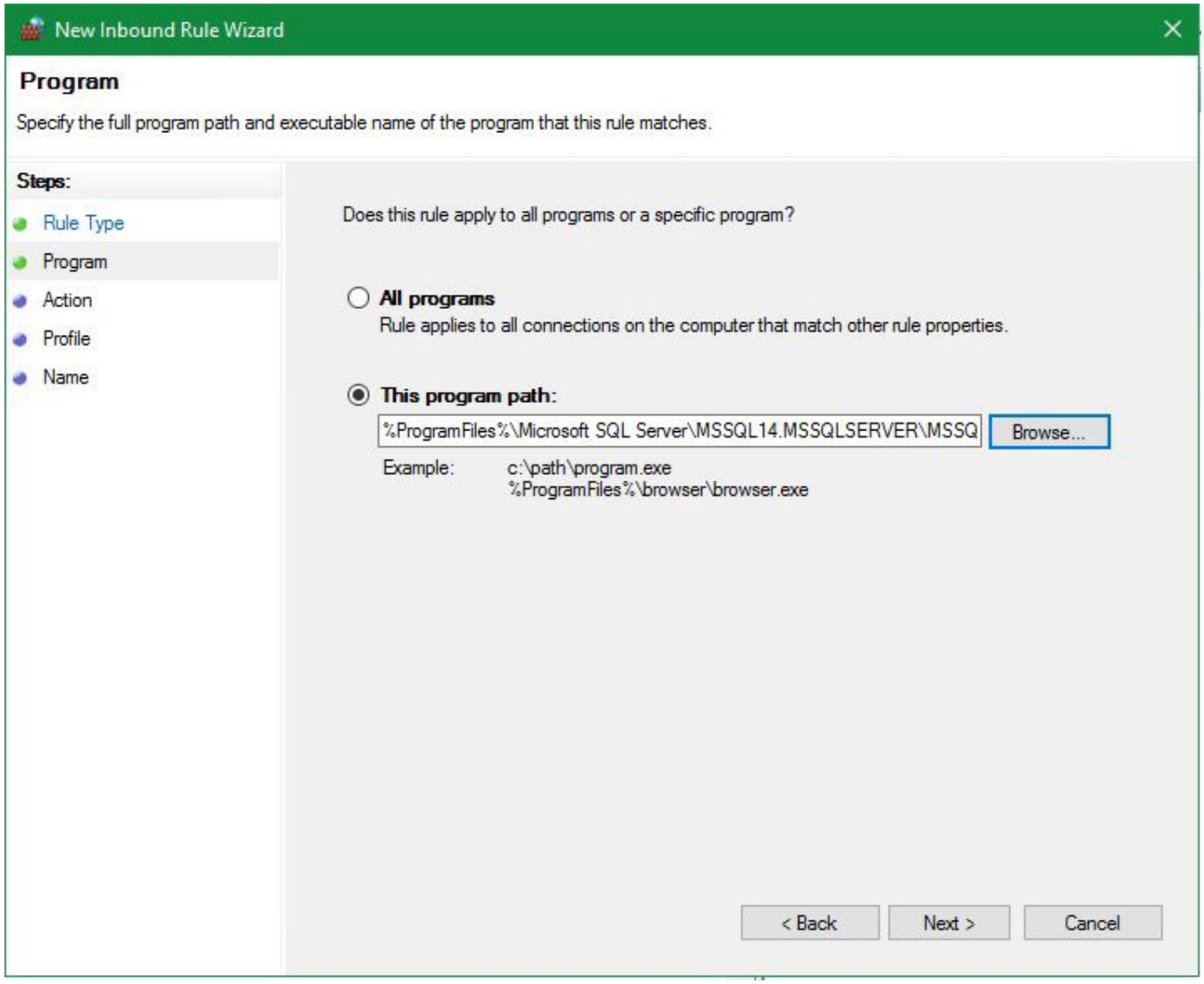
> *Rule Type:* ***Program***
>
> *Program:* ***C:\Program Files\Microsoft SQL Server\<Server version>.<Instance name>\MSSQL\Binn\sqlservr.exe***

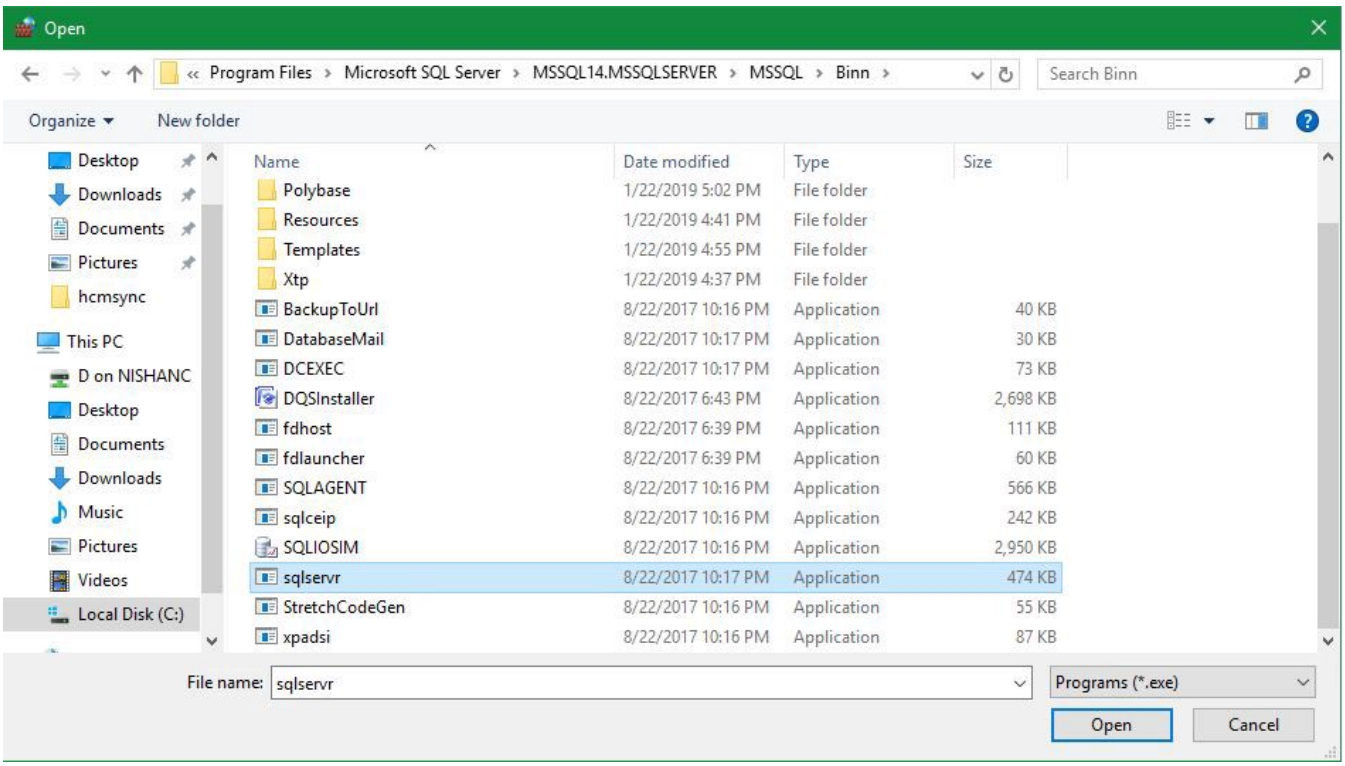
e.g. C:\Program Files\Microsoft SQL Server\MSSQL14.MSSQLSERVER\MSSQL\Binn

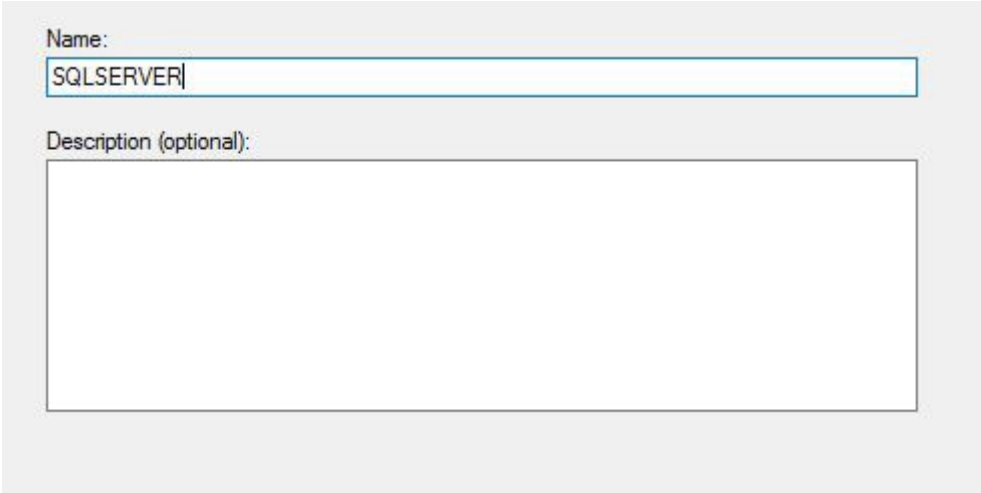
> *Action:* ***Allow the connection***
>
> *Profile:* ***Domain, Private, Public***
>
> *Name:* ***SQLSERVER***




Steps:
Rule Type
Program
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:
AllJoyn Router
Rule that controls connections for a Windows experience.
Custom
Custom rule.
< Back
Next >
Cancel

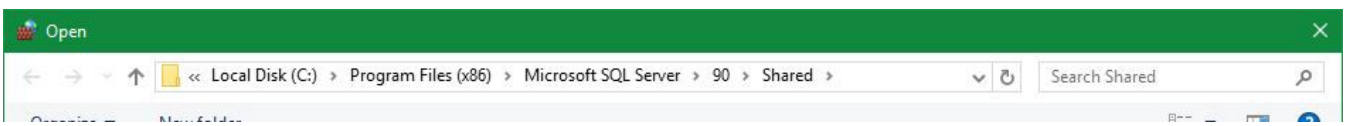

New Inbound Rule Wizard
Program
Specify the full program path and executable name of the program that this rule matches.
Steps:
Rule Type
Program
Action
Profile
Name
Does this rule apply to all programs or a specific program?
All programs
Rule applies to all connections on the computer that match other rule properties.
This program path:
%ProgramFiles%\Microsoft SQL Server\MSSQL14.MSSQLSERVER\MSSQ
Browse...
Example: c:\path\program.exe
%ProgramFiles%\browser\browser.exe
< Back
Next >
Cancel

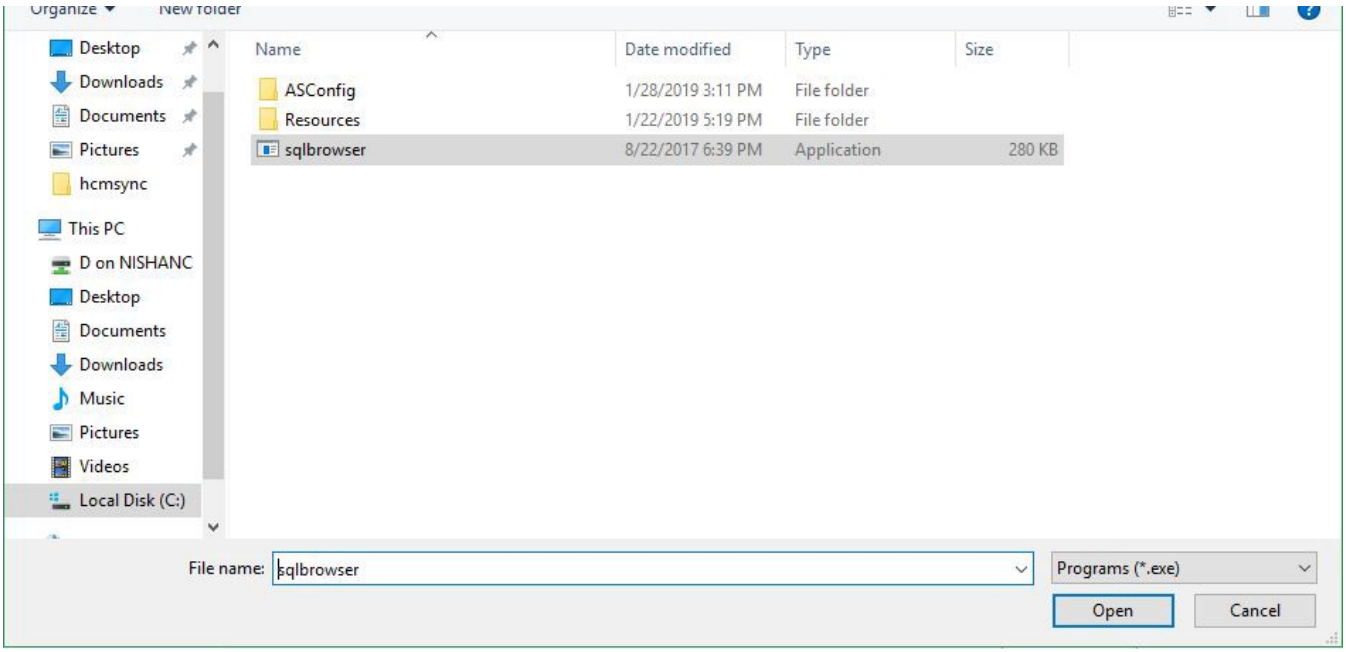


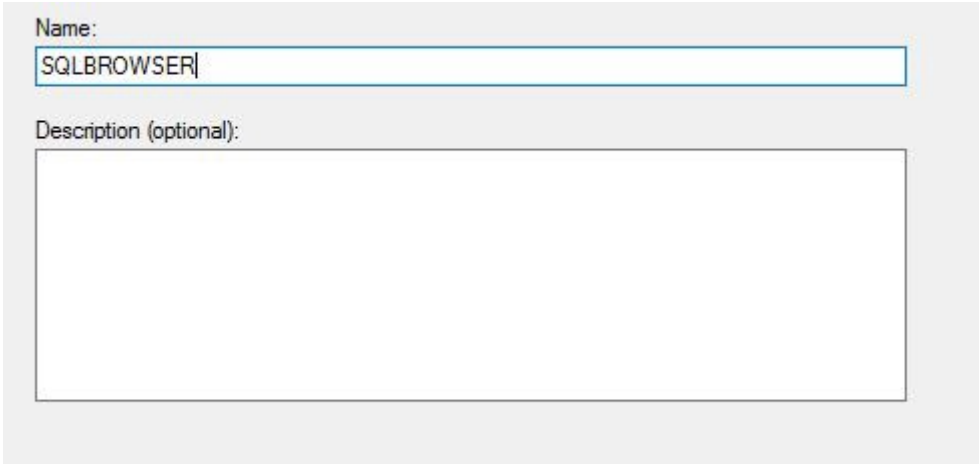


One more rule for the **SQL Server Browser.**

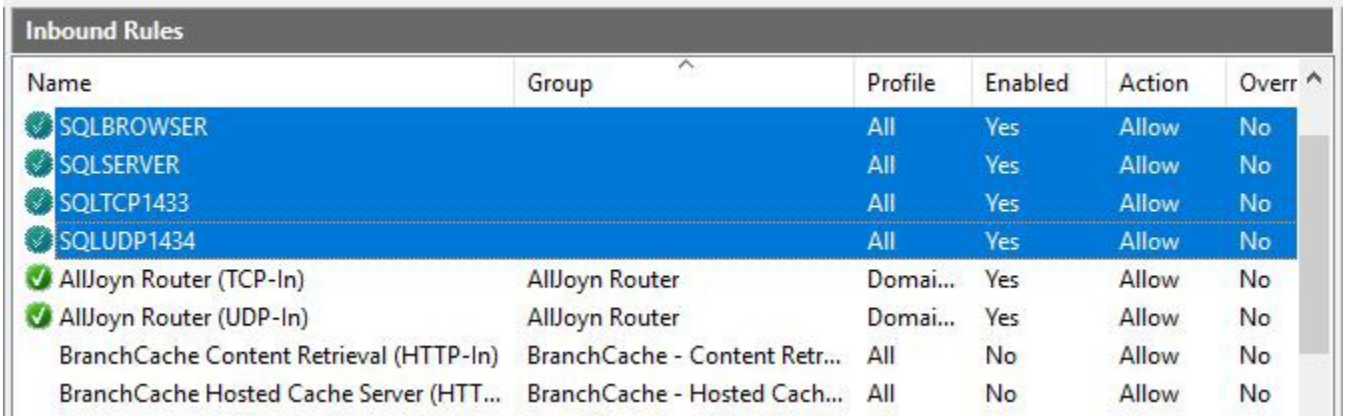
> *Rule Type:* ***Program***
>
> *Program:* ***C:\Program Files (x86)\Microsoft SQL Server\90\Shared\sqlbrowser.exe***
>
> *Action:* ***Allow the connection***
>
> *Profile:* ***Domain, Private, Public***
>
> *Name:* ***SQLBROWSER***



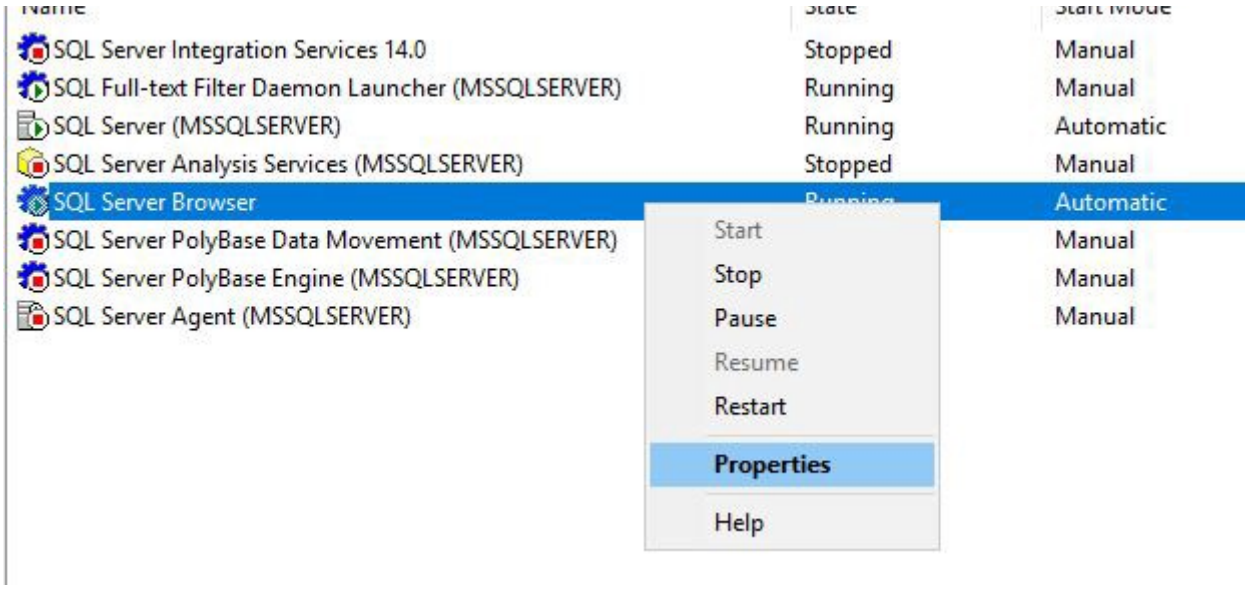




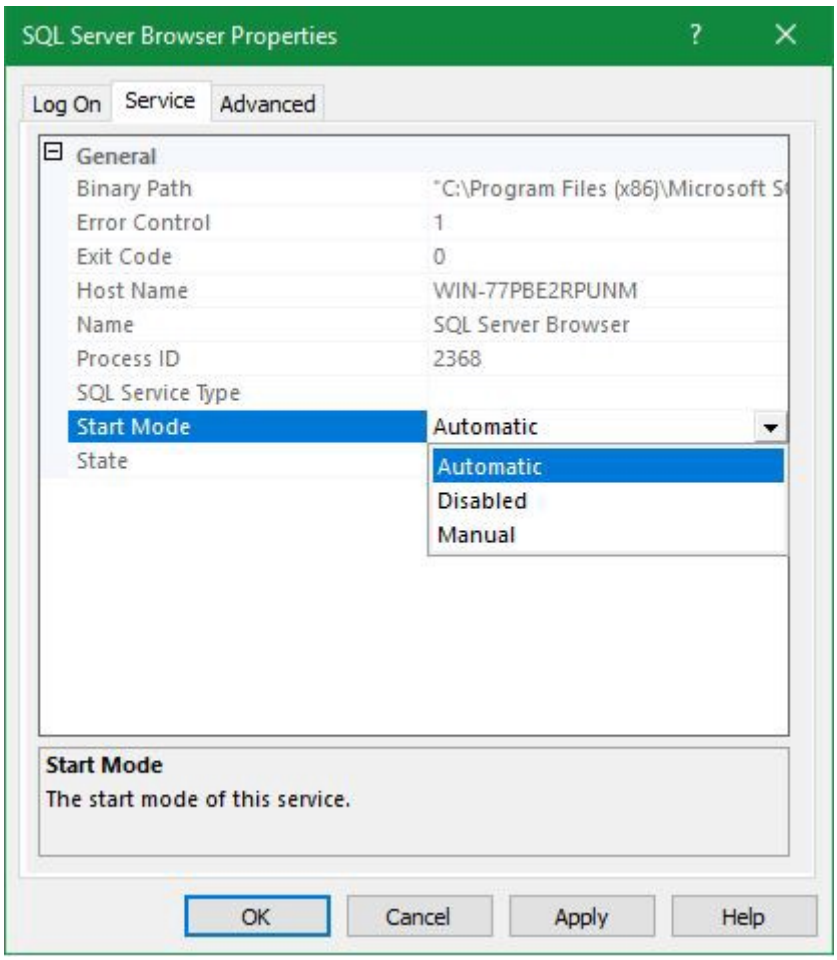
Now all four rules are setup.



Make sure the **SQL Server Browser** and **SQL Server** is set to start automatically. Go back to **SQL Server Configuration Manager** and right click on **SQL Server Browser** under **SQL Server Services,** click **Properties.**

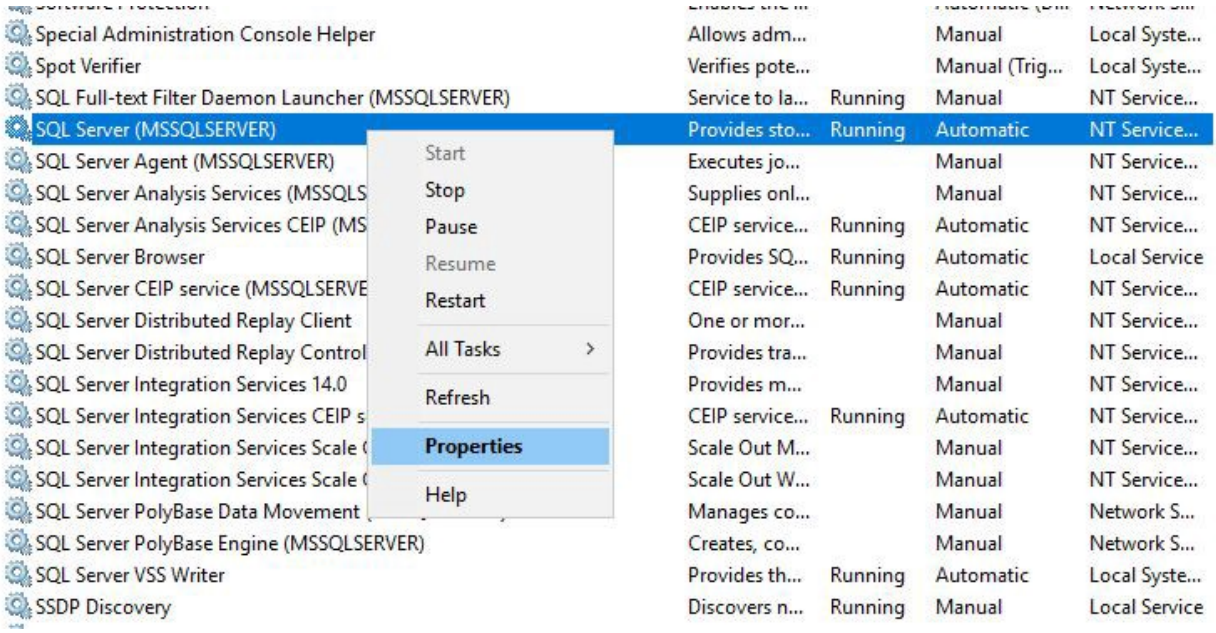


Under **Service** tab, select **Automatic** for **Start mode.**

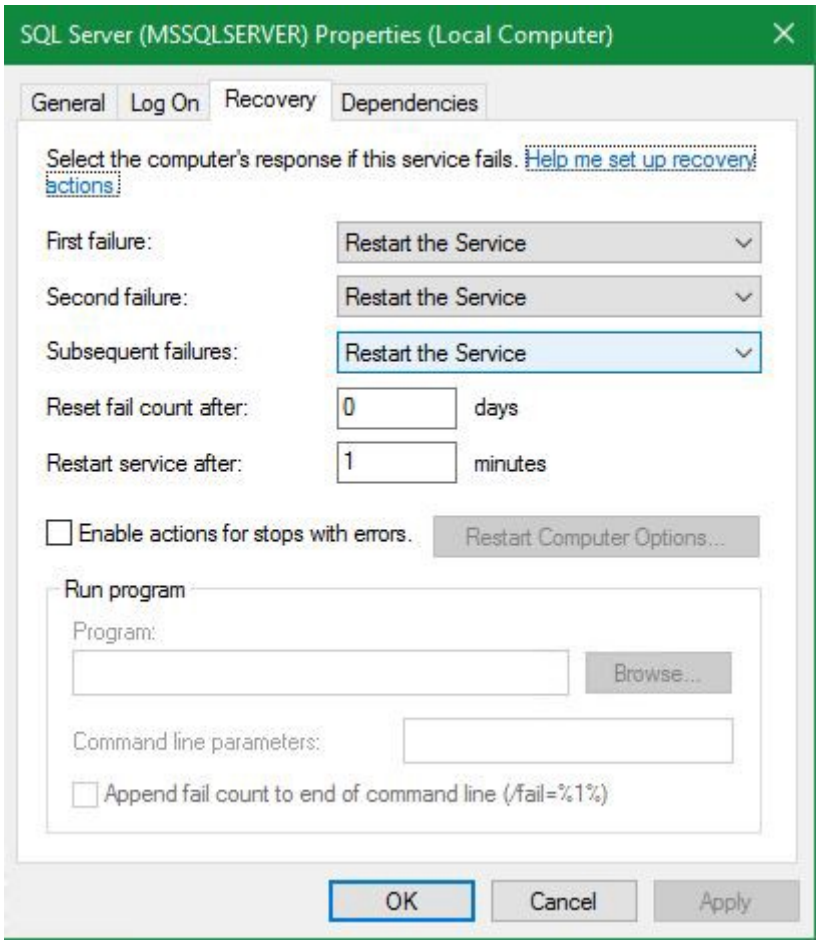


Click **Apply.** Now let's make sure that we keep the service failures to minimum.

1. Click the Windows key + R to **open** the Run window.
2. Type services.msc in the **Open:** box.
3. Click **OK.**



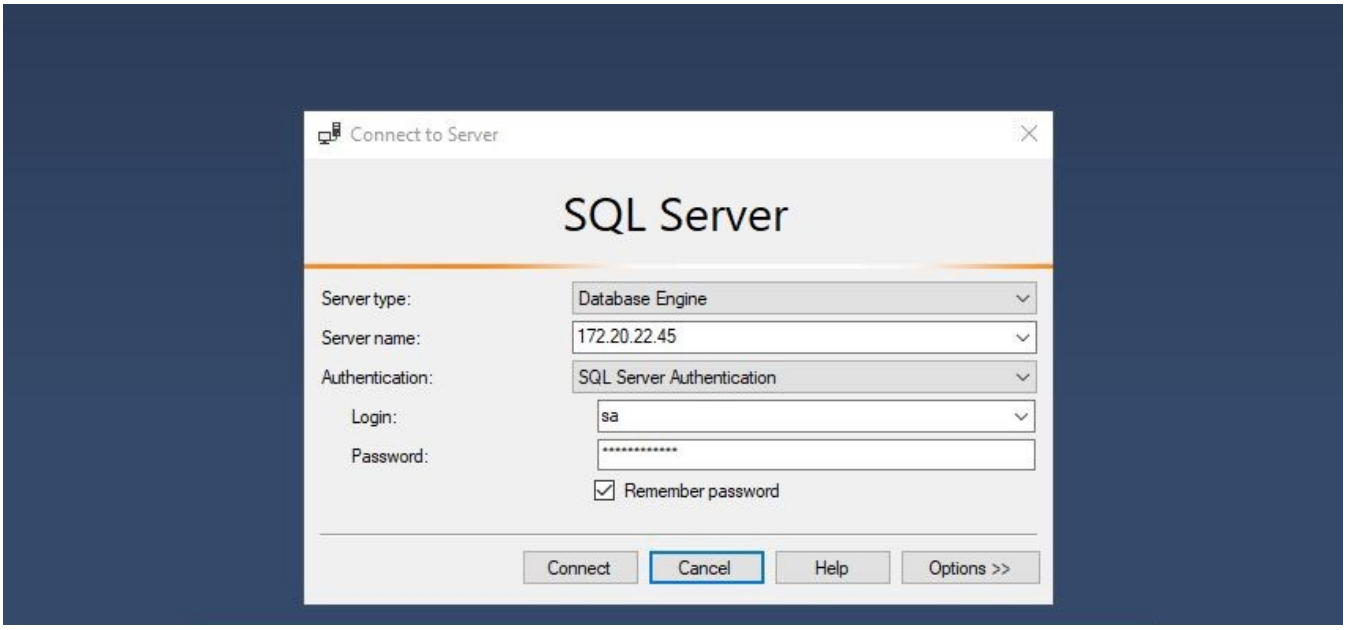
Find the **SQL Server** service, right click and select Properties.

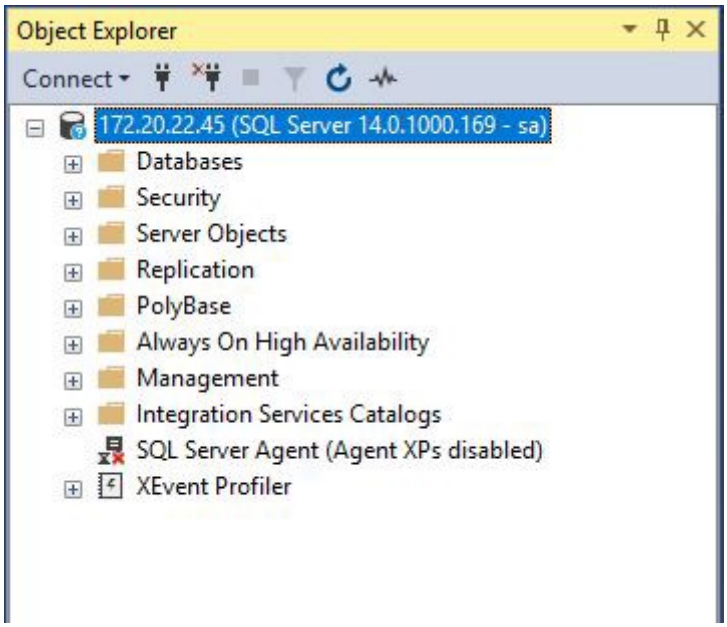


On the **Recovery** tab select **Restart the Service** for **First failure, Second failure, Subsequent failures.**

...and Done!.

Try again to connect.





Awesome! You did it. :)

Microsoft Sql Server Remote Server