Sri Lanka Institute of Information Technology

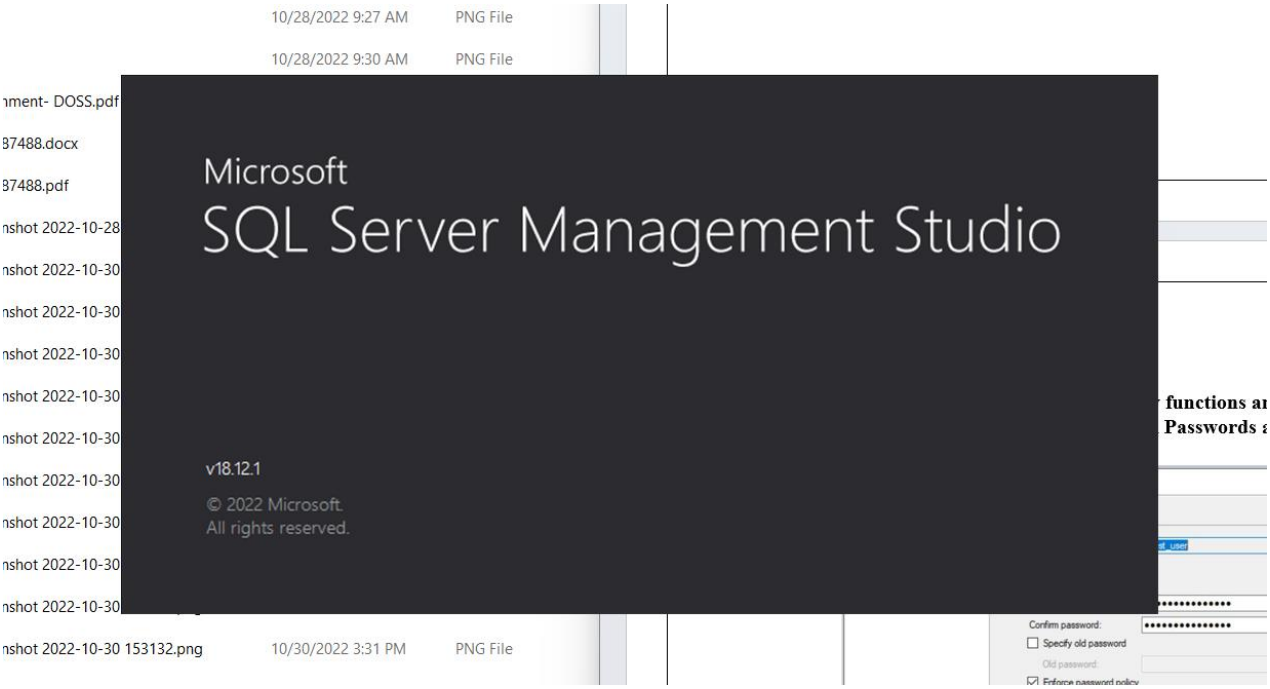
Assignment – Implementing Security features in OS and DB

Data and Operating System Security

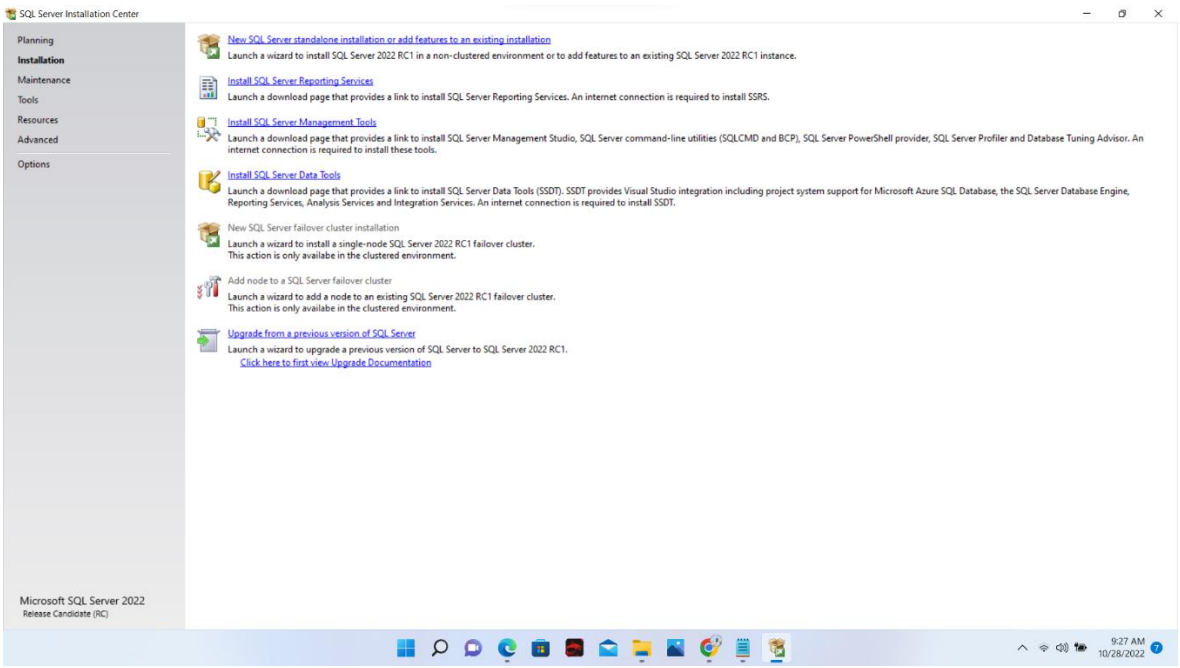
- IE3062

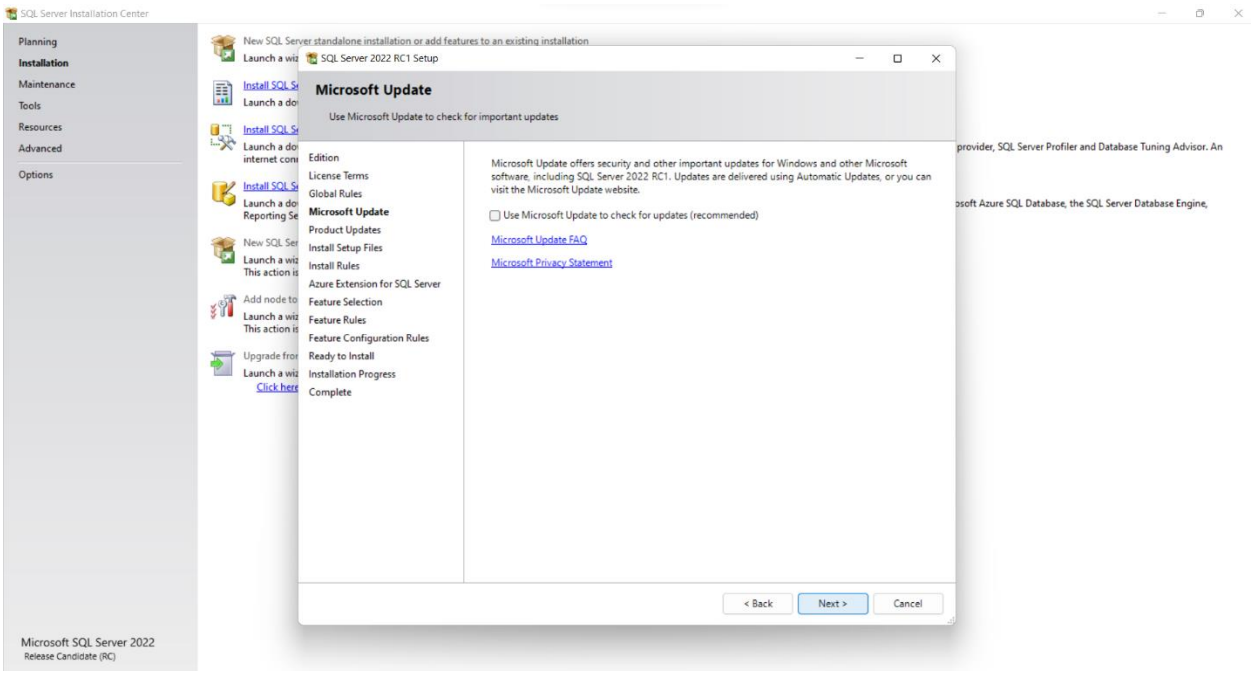
–

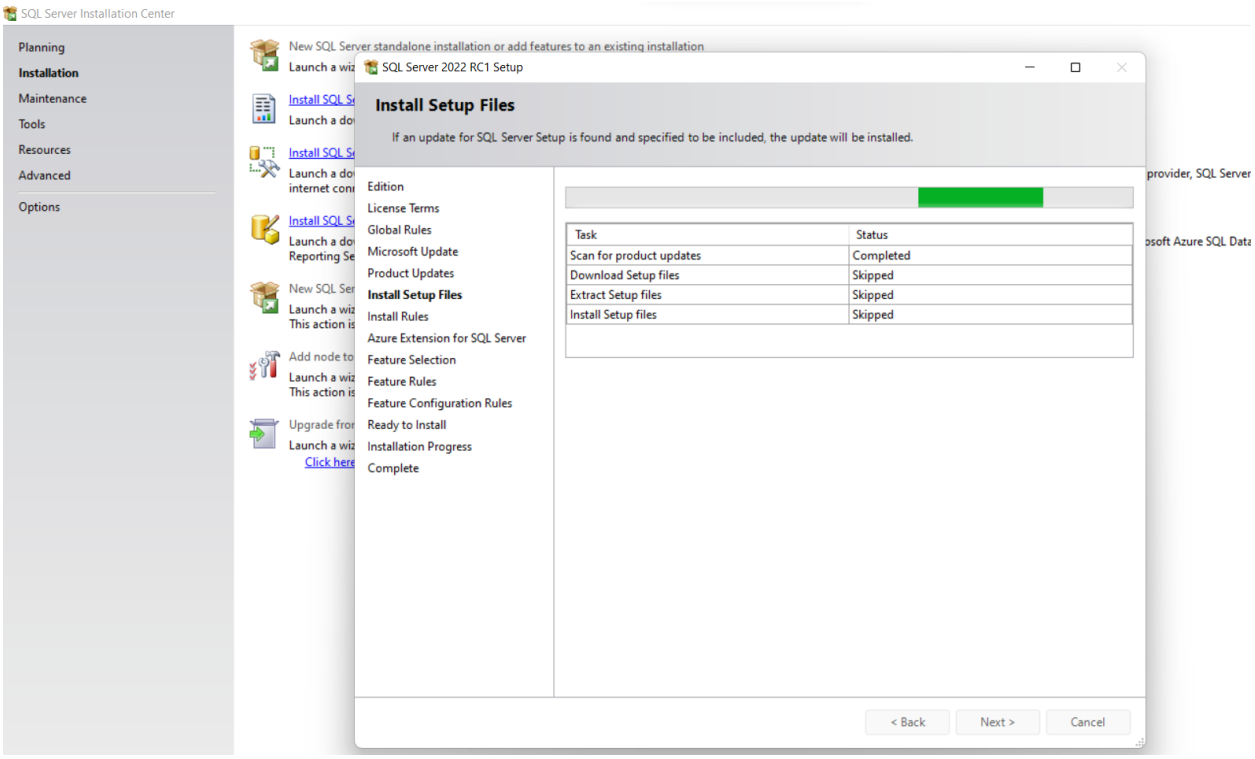
Student Registration Number	Student Name
IT20627928	Herath H.M.T. D
IT20618872	Thisitha K.L. D



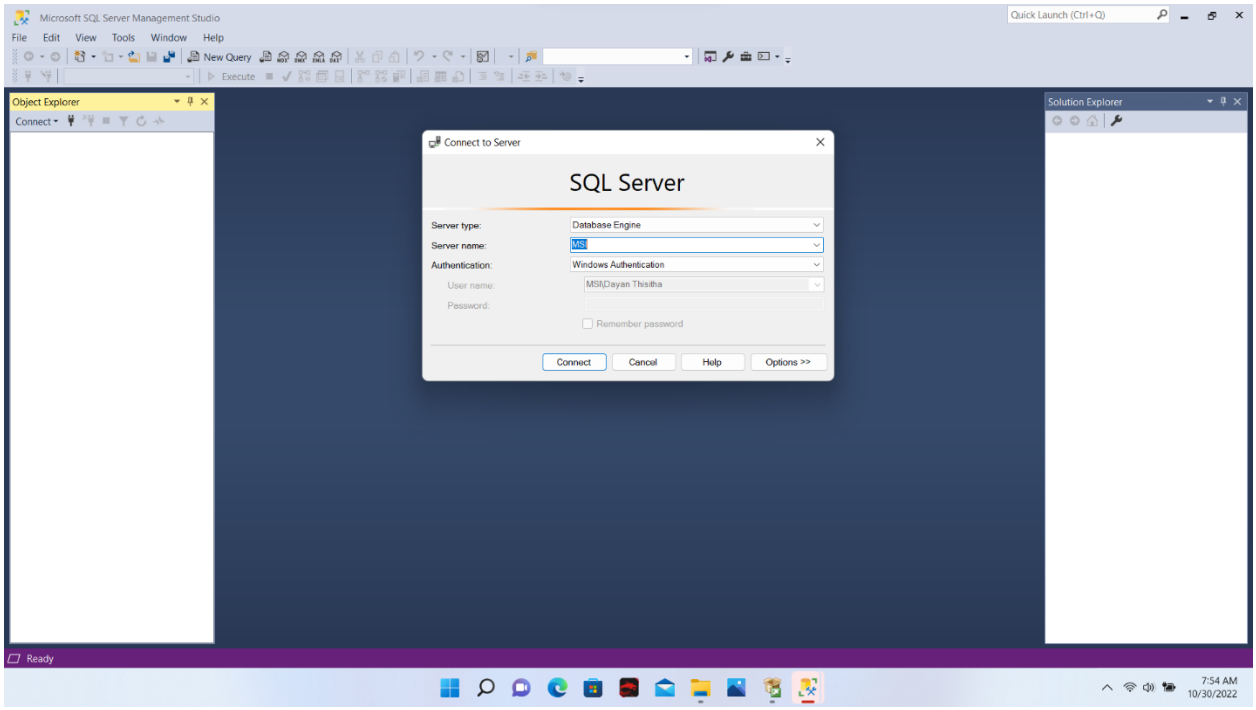
1. Install SQL server

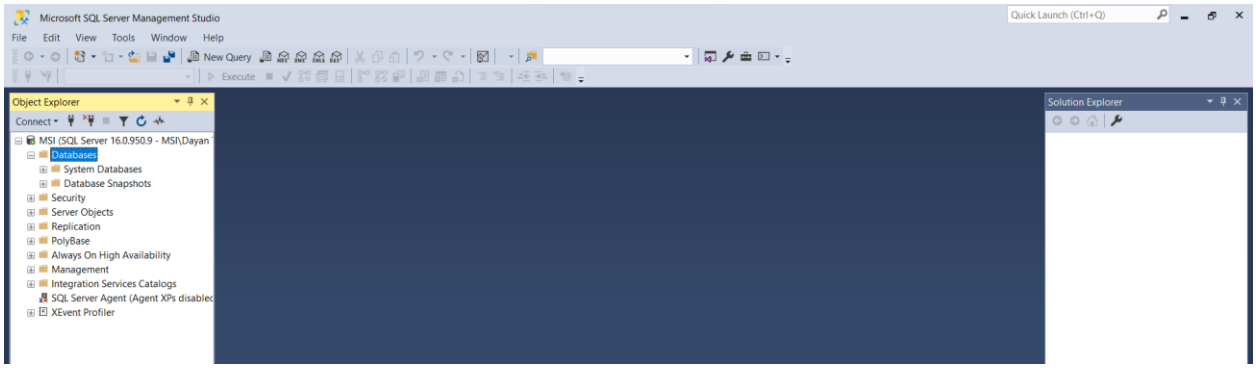



SQL Server Installation Center
Planning
Installation
Maintenance
Tools
Resources
Advanced
Options
New SQL Server standalone installation or add features to an existing installation
SQL Server 2022 RC1 Setup
Microsoft Update
Use Microsoft Update to check for important updates
Edition
License Terms
Global Rules
Microsoft Update
Product Updates
Install Setup Files
Install Rules
Azure Extension for SQL Server
Feature Selection
Feature Rules
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Microsoft Update offers security and other important updates for Windows and other Microsoft software, including SQL Server 2022 RC1. Updates are delivered using Automatic Updates, or you can visit the Microsoft Update website.
Use Microsoft Update to check for updates (recommended)
Microsoft Update FAQ
Microsoft Privacy Statement
< Back
Next >
Cancel
Microsoft SQL Server 2022
Release Candidate (RC)

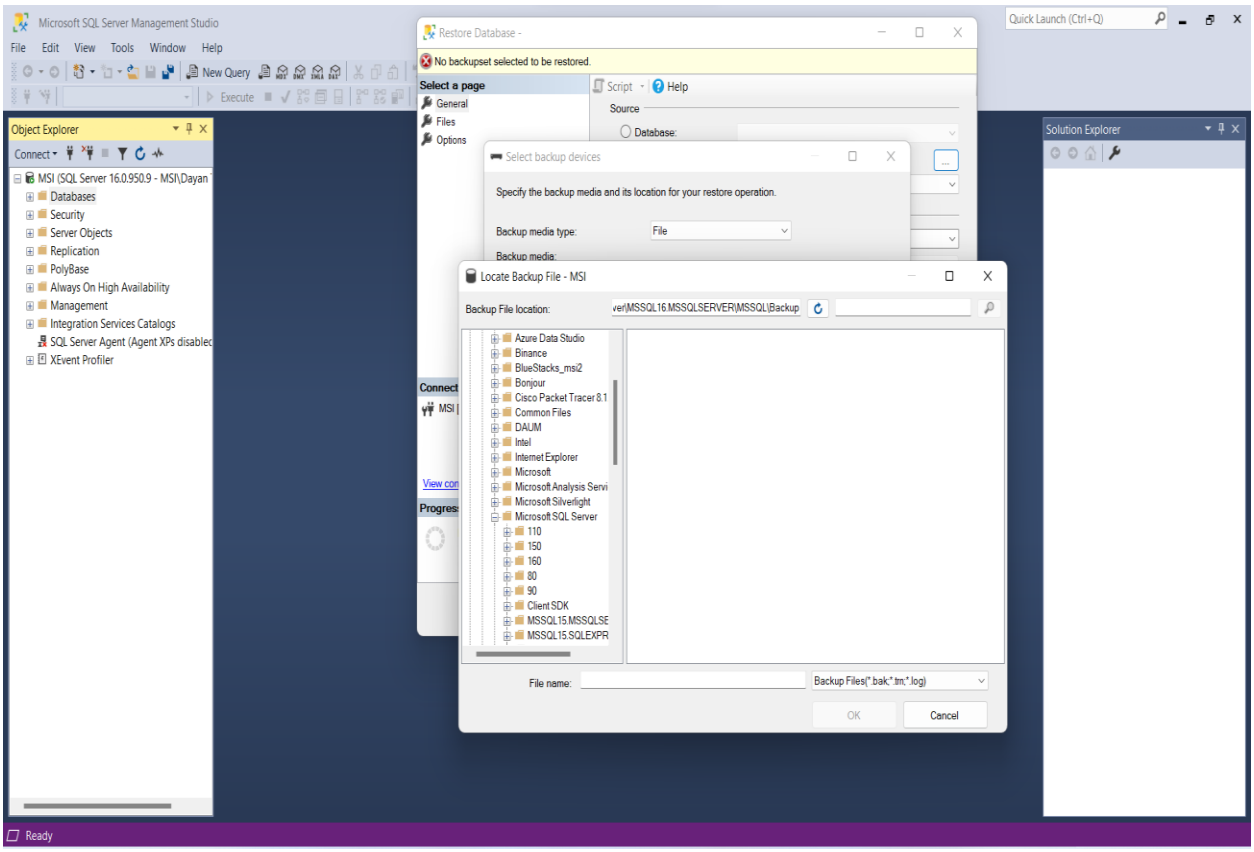

SQL Server Installation Center
Planning
Installation
Maintenance
Tools
Resources
Advanced
Options
New SQL Server standalone installation or add features to an existing installation
SQL Server 2022 RC1 Setup
Install Setup Files
If an update for SQL Server Setup is found and specified to be included, the update will be installed.
Edition
License Terms
Global Rules
Microsoft Update
Product Updates
Install Setup Files
Install Rules
Azure Extension for SQL Server
Feature Selection
Feature Rules
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Task
Status
Scan for product updates
Completed
Download Setup files
Skipped
Extract Setup files
Skipped
Install Setup files
Skipped
< Back
Next >
Cancel

2. Connect to server





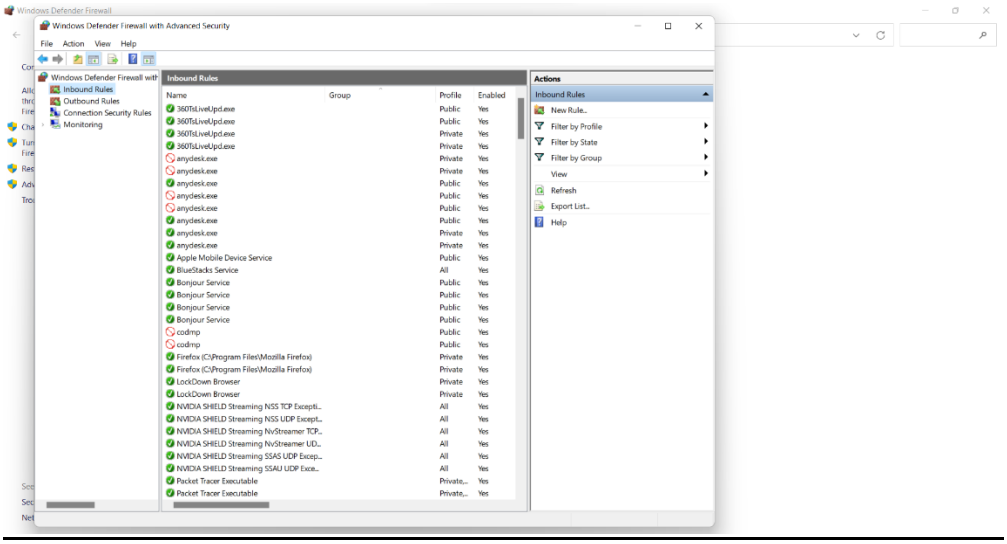
3. Restore / Import database

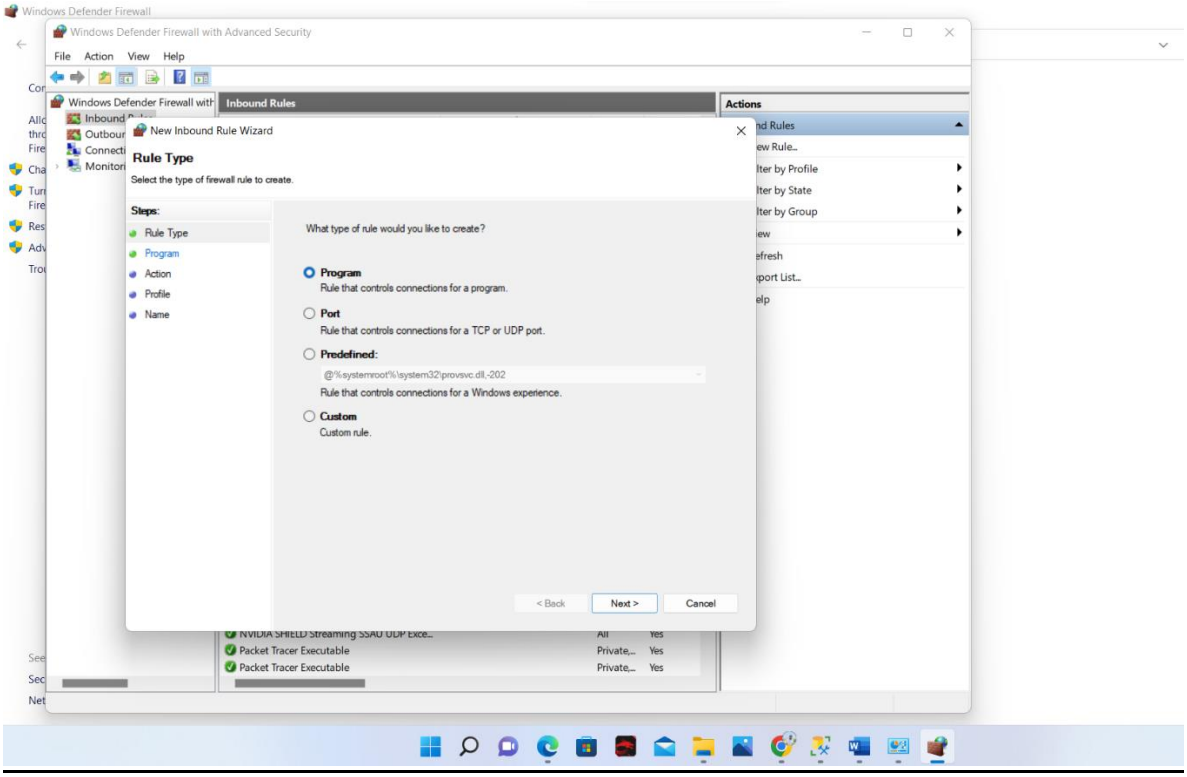


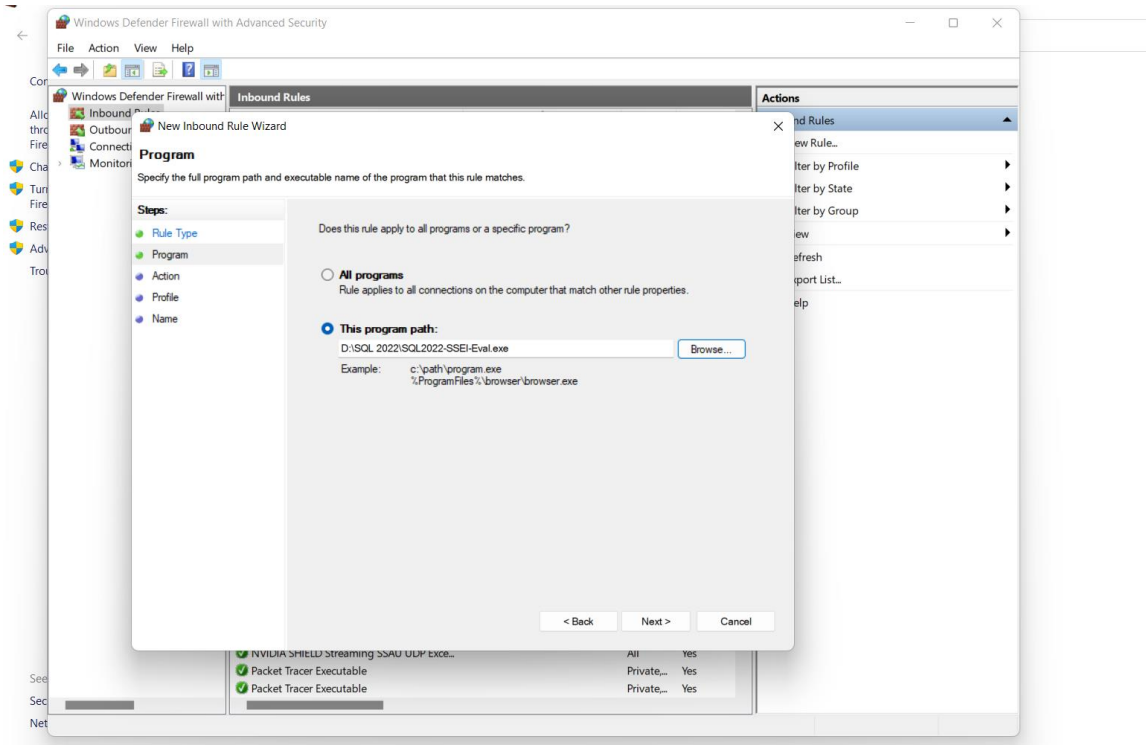
The Security Check list to be implemented

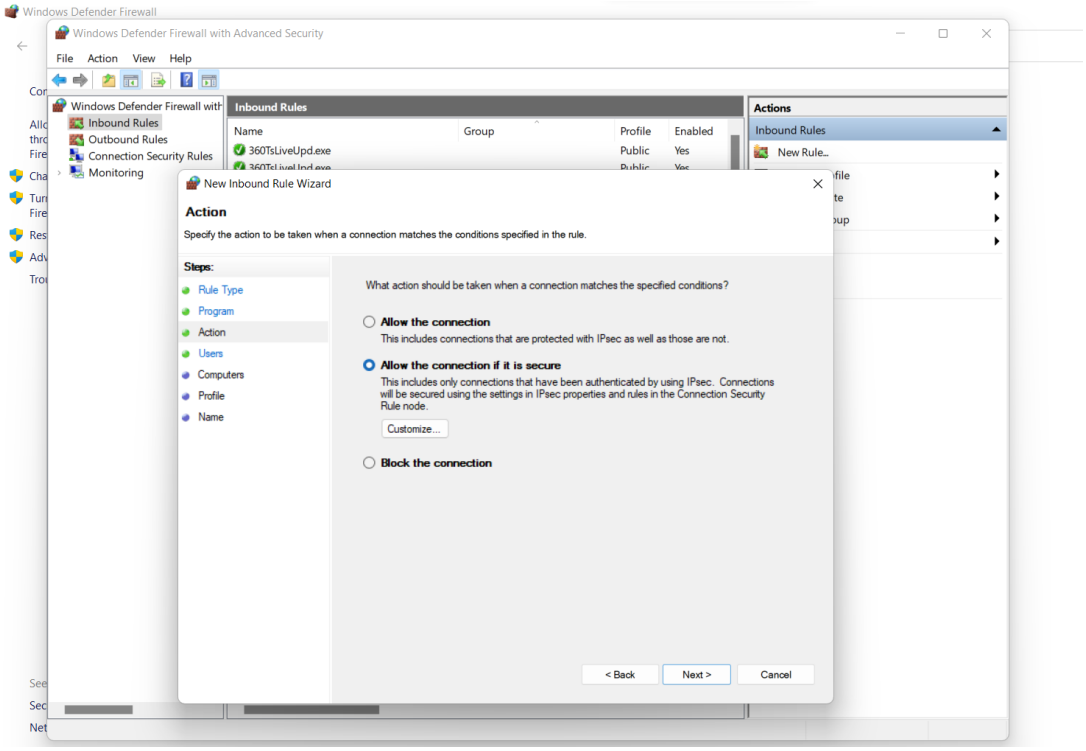
1. Firewall for database servers

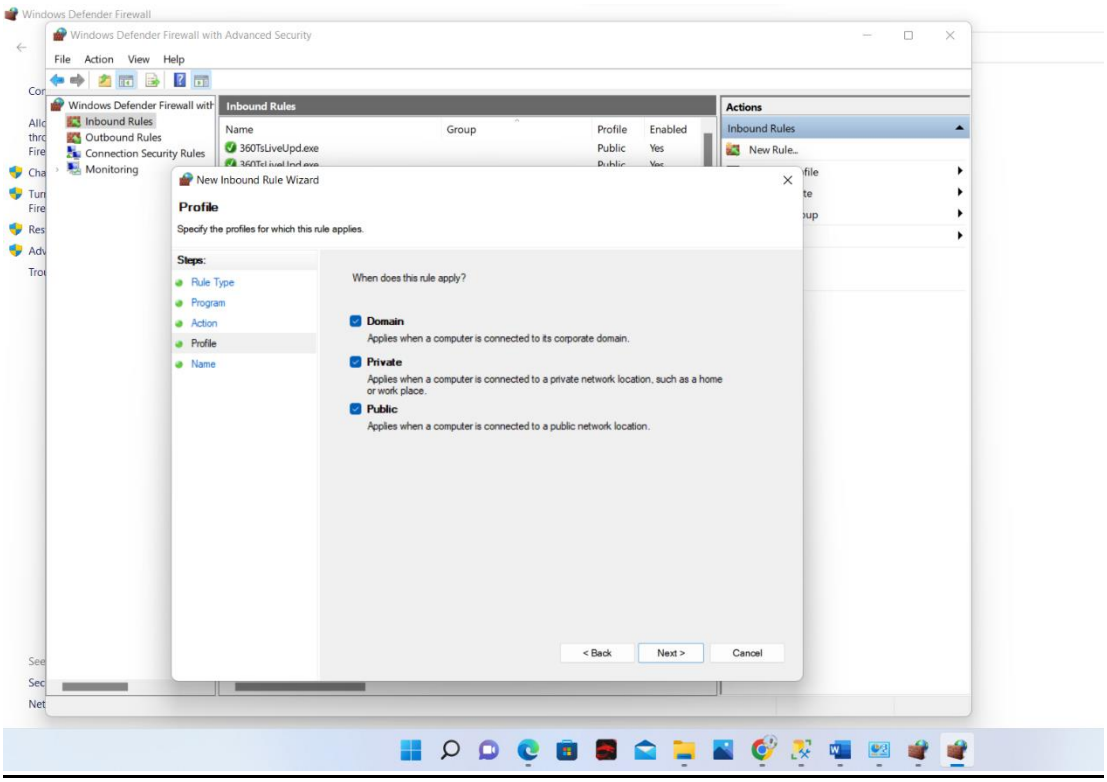
- New inbound rule for program

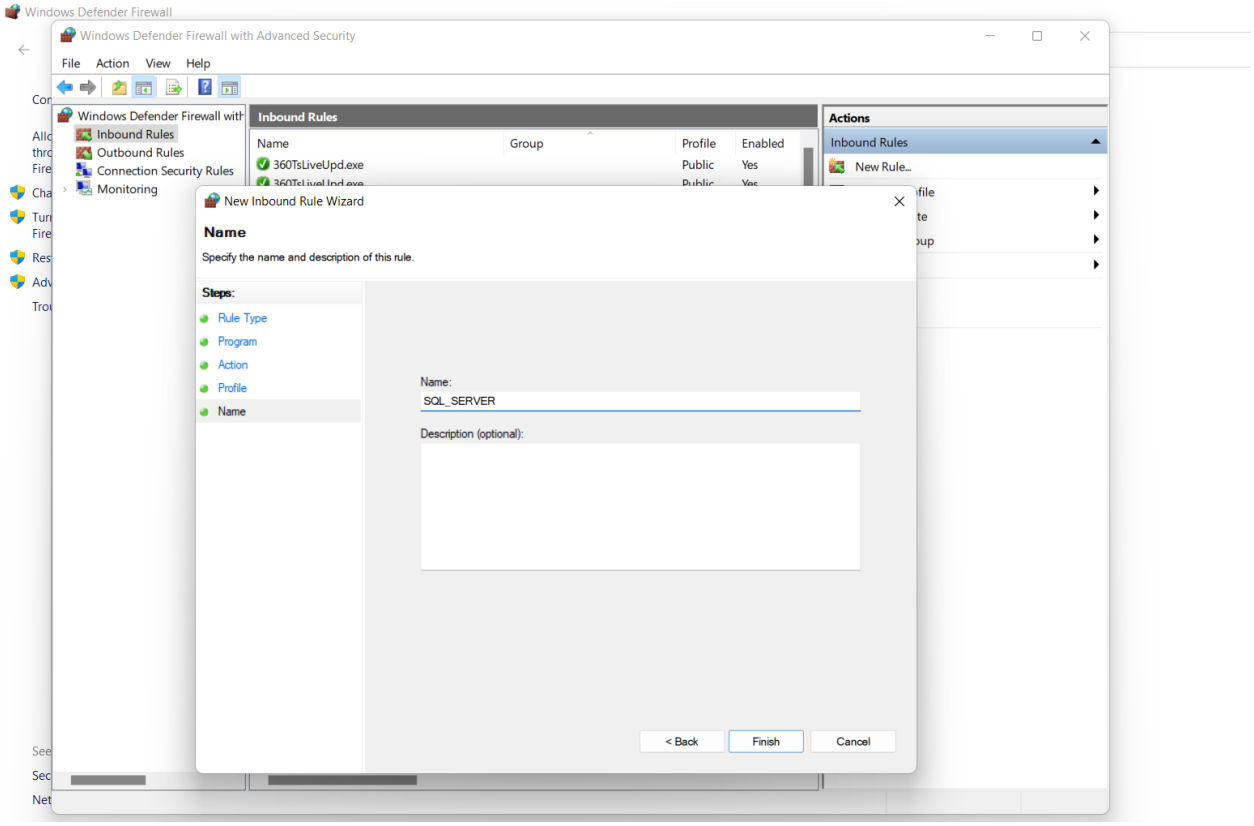




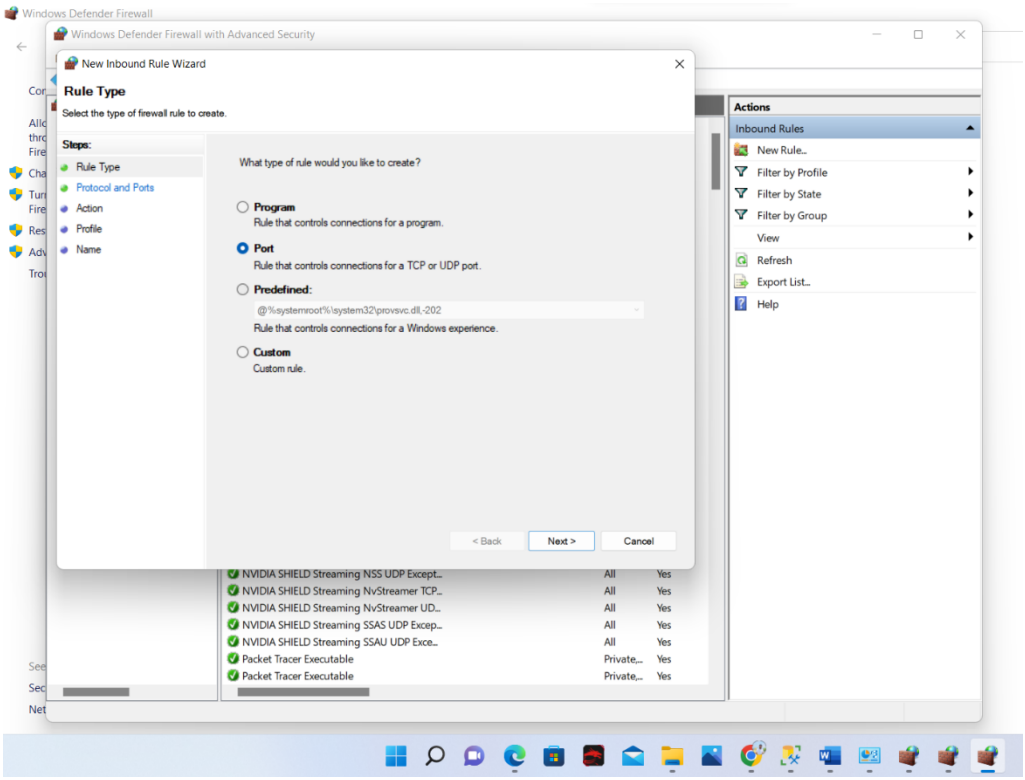

Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall with
Inbound Rules
Actions
New Inbound Rule Wizard
Program
Specify the full program path and executable name of the program that this rule matches.
Steps:
Rule Type
Program
Action
Profile
Name
Does this rule 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:
D:\SQL 2022\SQL2022-SSEI-Eval.exe
Browse...
Example: c:\path\program.exe
%ProgramFiles%\browser\browser.exe
< Back
Next >
Cancel
Packet Tracer Executable
Packet Tracer Executable

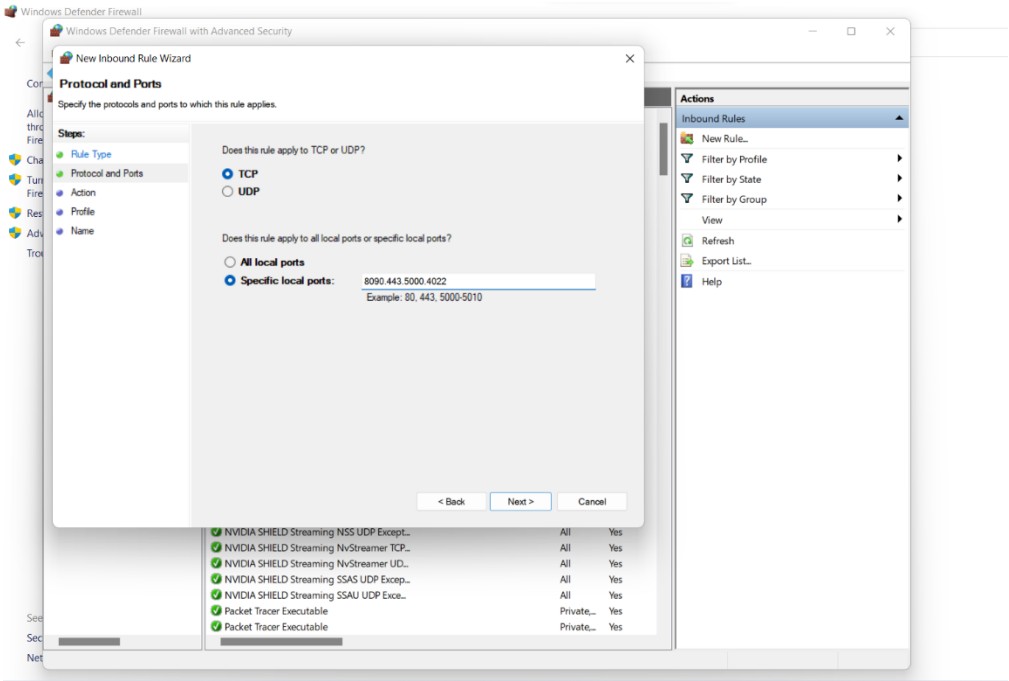

Windows Defender Firewall
Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name
Group
Profile
Enabled
360TsLiveUpd.exe
Public
Yes
Actions
Inbound Rules
New Rule...
New Inbound Rule Wizard
Action
Specify the action to be taken when a connection matches the conditions specified in the rule.
Steps:
Rule Type
Program
Action
Users
Computers
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

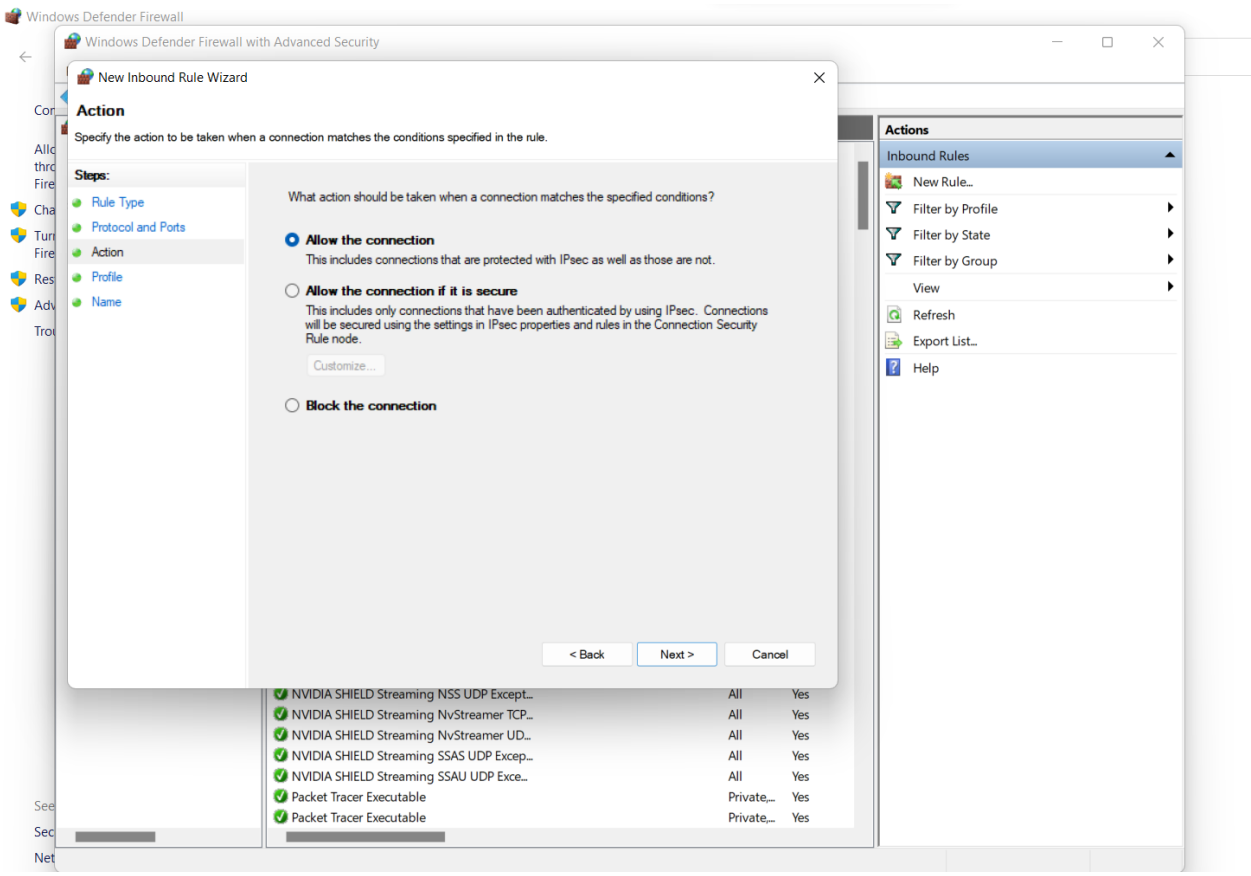

Windows Defender Firewall
Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name
Group
Profile
Enabled
360TsLiveUpd.exe
Public
Yes
Actions
Inbound Rules
New Rule...
New Inbound Rule Wizard
Profile
Specify the profiles for which this rule applies.
Steps:
Rule Type
Program
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

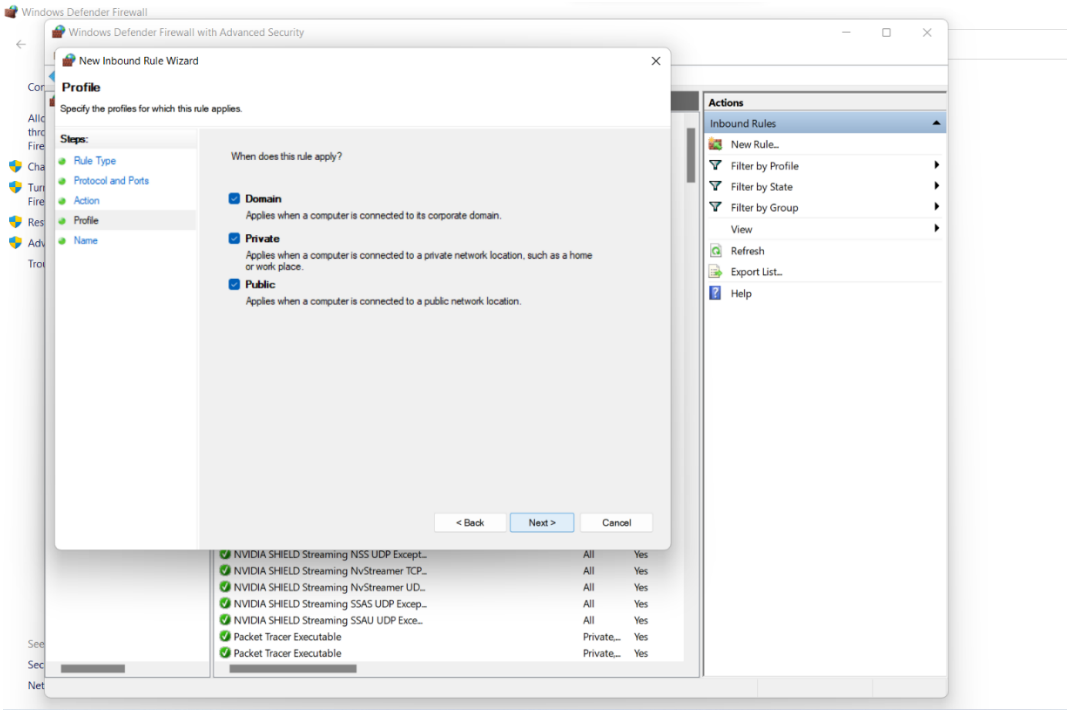

Windows Defender Firewall
Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name
Group
Profile
Enabled
360TsLiveUpd.exe
Public
Yes
Actions
Inbound Rules
New Rule...
New Inbound Rule Wizard
Name
Specify the name and description of this rule.
Steps:
Rule Type
Program
Action
Profile
Name
Name:
SQL_SERVER
Description (optional):
< Back
Finish
Cancel

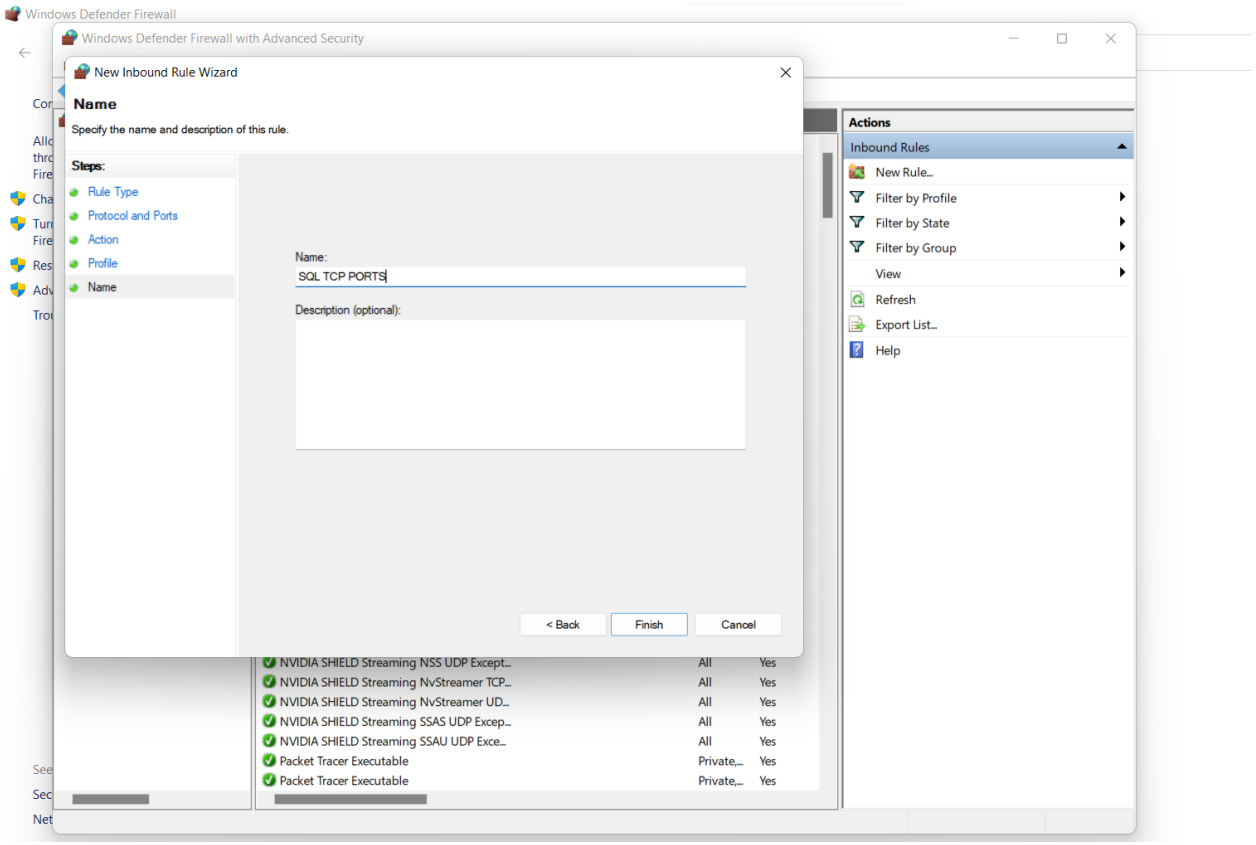
❖ New inbound rule for port security



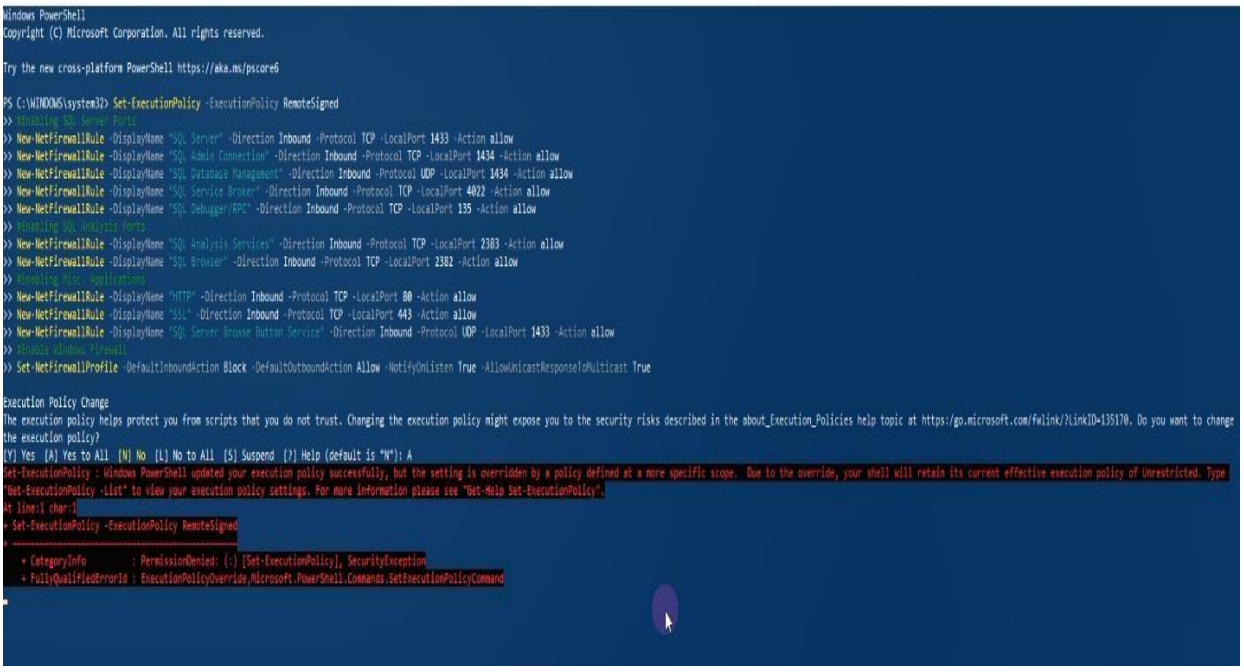



Windows Defender Firewall
Windows Defender Firewall with Advanced Security
New Inbound Rule Wizard
Action
Specify the action to be taken when a connection matches the conditions specified in the rule.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
What action should be taken when a connection 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
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
NVIDIA SHIELD Streaming NSS UDP Except... All Yes
NVIDIA SHIELD Streaming NvStreamer TCP... All Yes
NVIDIA SHIELD Streaming NvStreamer UD... All Yes
NVIDIA SHIELD Streaming SSAS UDP Excep... All Yes
NVIDIA SHIELD Streaming SSAU UDP Exce... All Yes
Packet Tracer Executable Private,... Yes
Packet Tracer Executable Private,... Yes

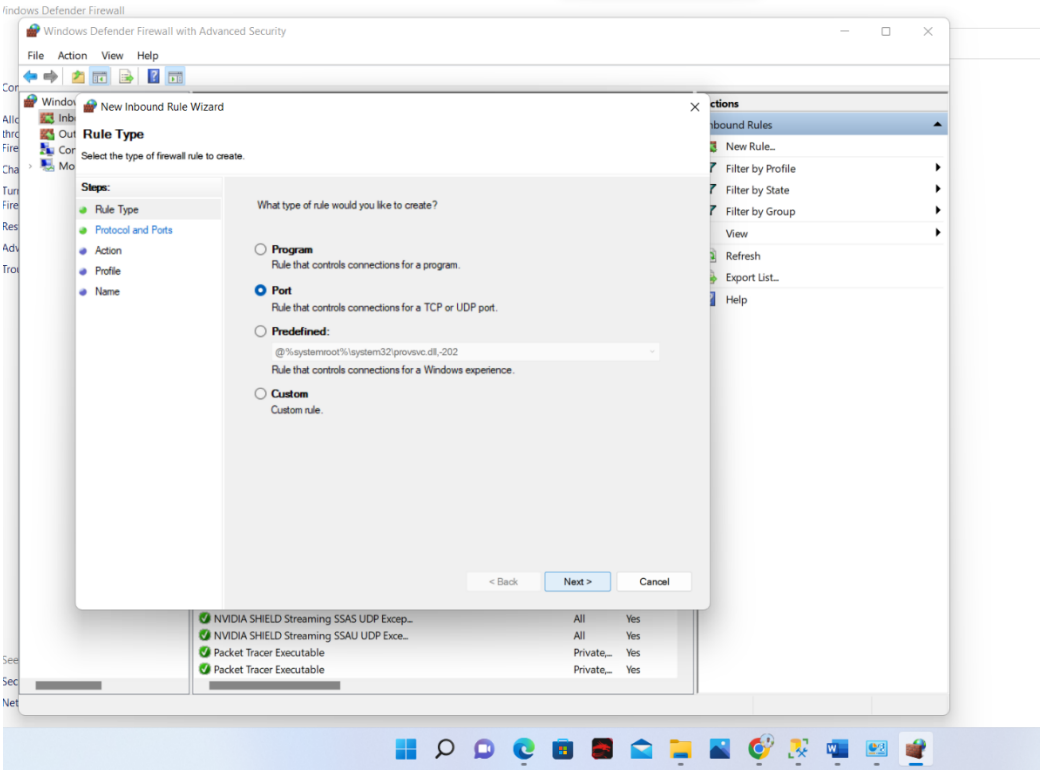

Windows Defender Firewall
Windows Defender Firewall with Advanced Security
New Inbound Rule Wizard
Profile
Specify the profiles for which this rule applies.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
When does this rule apply?
Domain
Applies when a computer is connected to its corporate 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
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
NVIDIA SHIELD Streaming NSS UDP Except... All Yes
NVIDIA SHIELD Streaming NvStreamer TCP... All Yes
NVIDIA SHIELD Streaming NvStreamer UD... All Yes
NVIDIA SHIELD Streaming SSAS UDP Excep... All Yes
NVIDIA SHIELD Streaming SSAU UDP Exce... All Yes
Packet Tracer Executable Private,... Yes
Packet Tracer Executable Private,... Yes

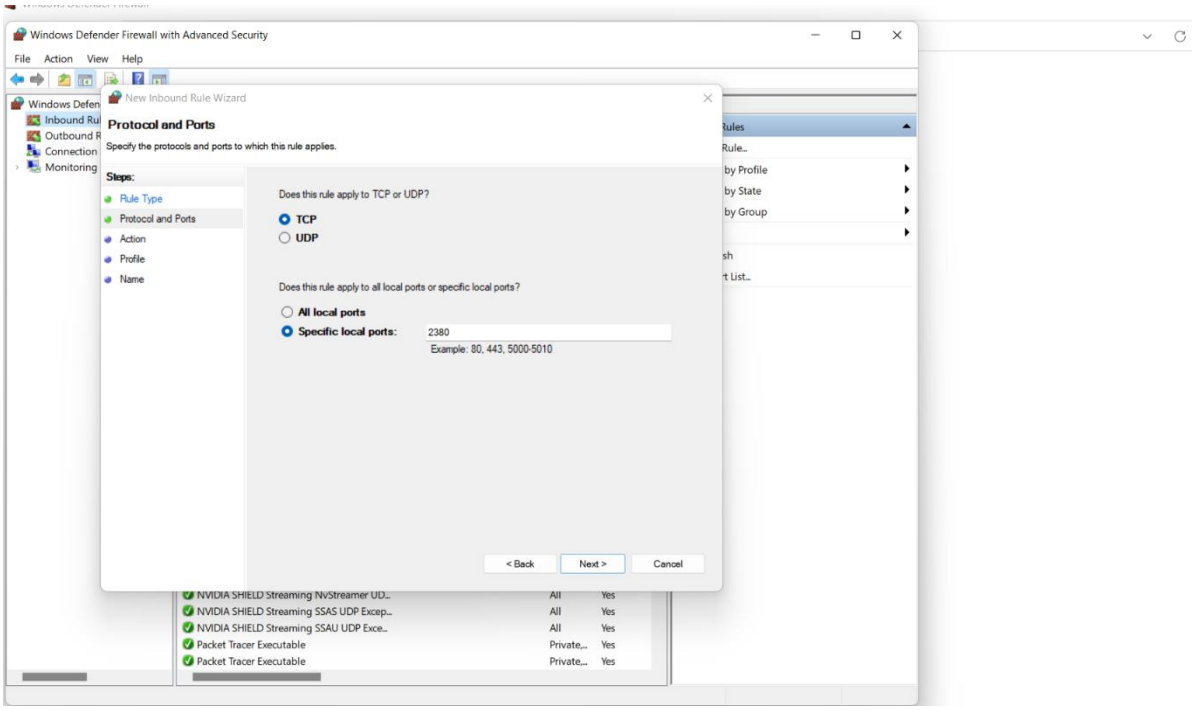


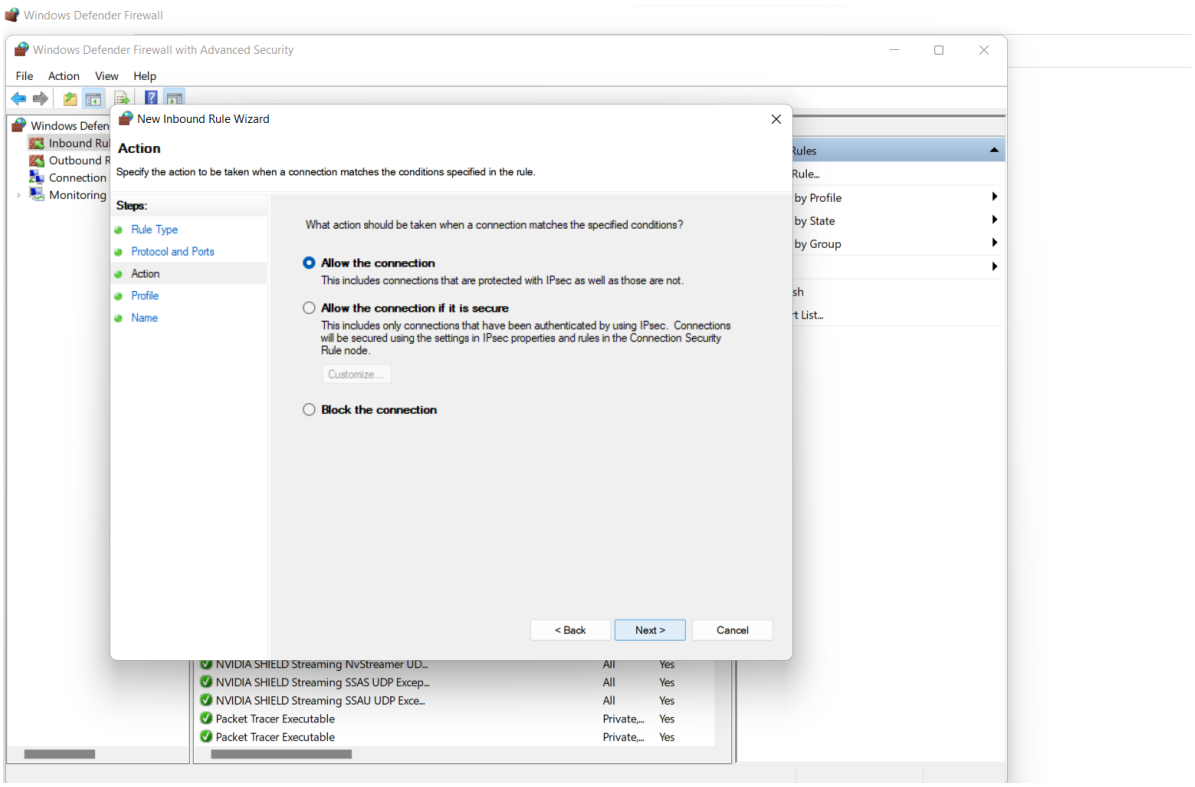
❖ Run firewall rules in the PowerShell

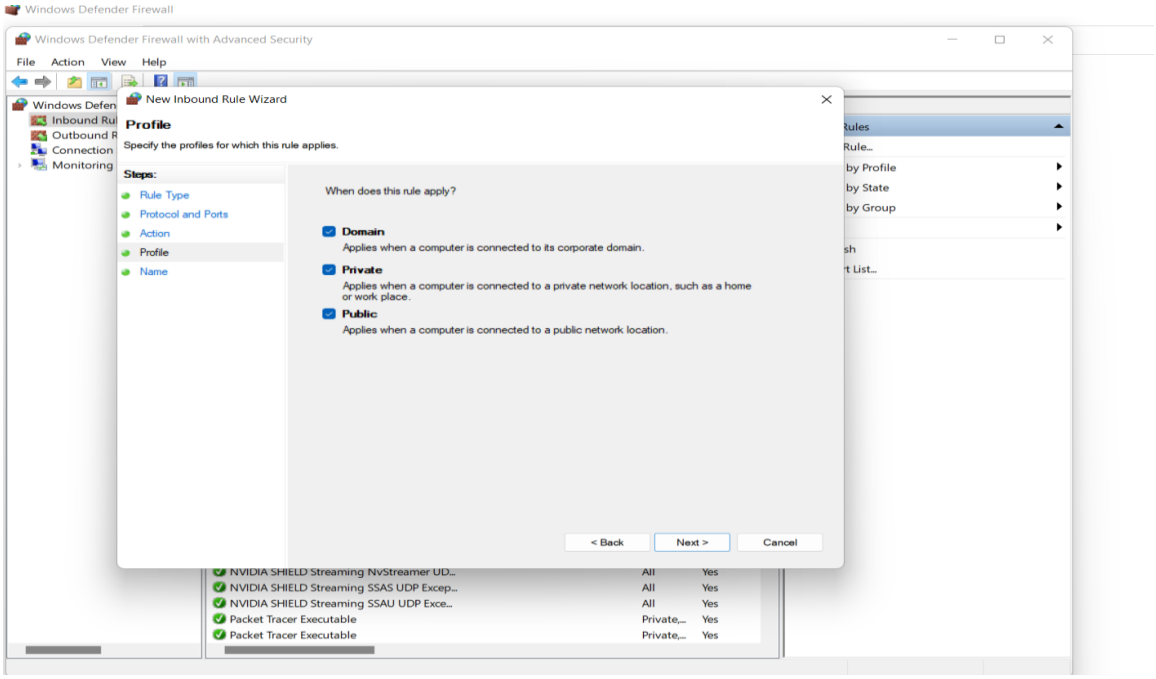


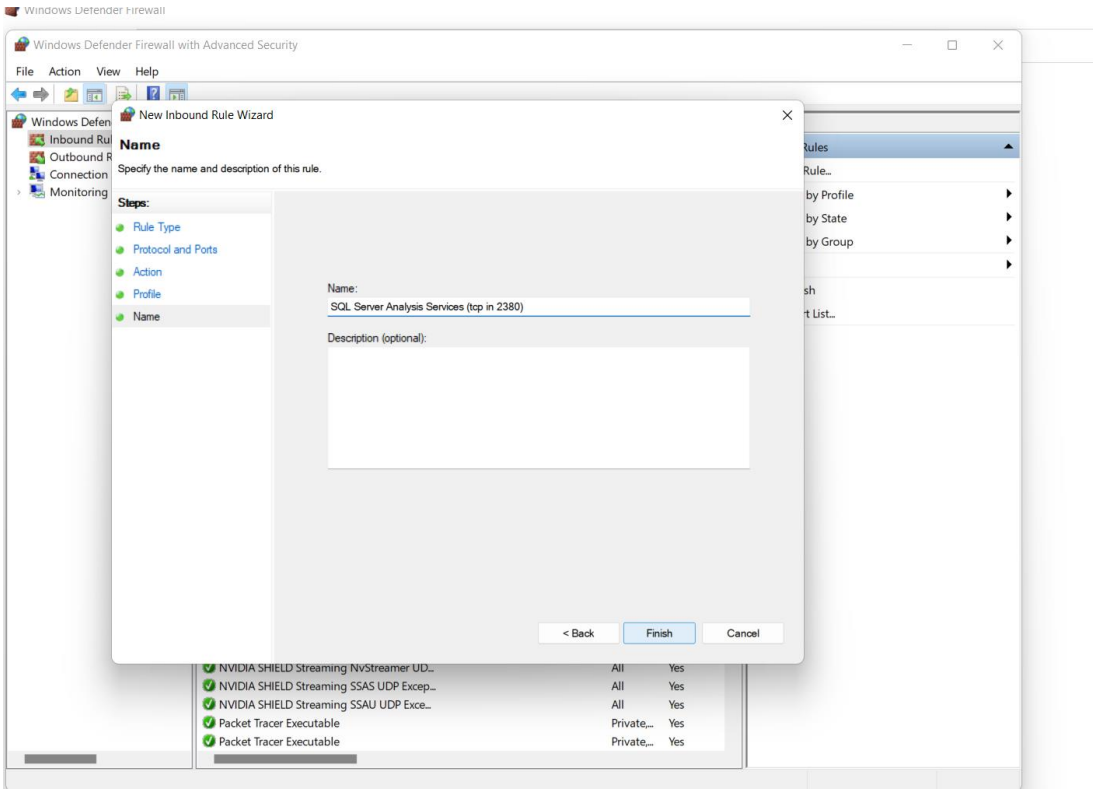
❖ Activating SQL Server Analysis Services (tcp-in 2380)



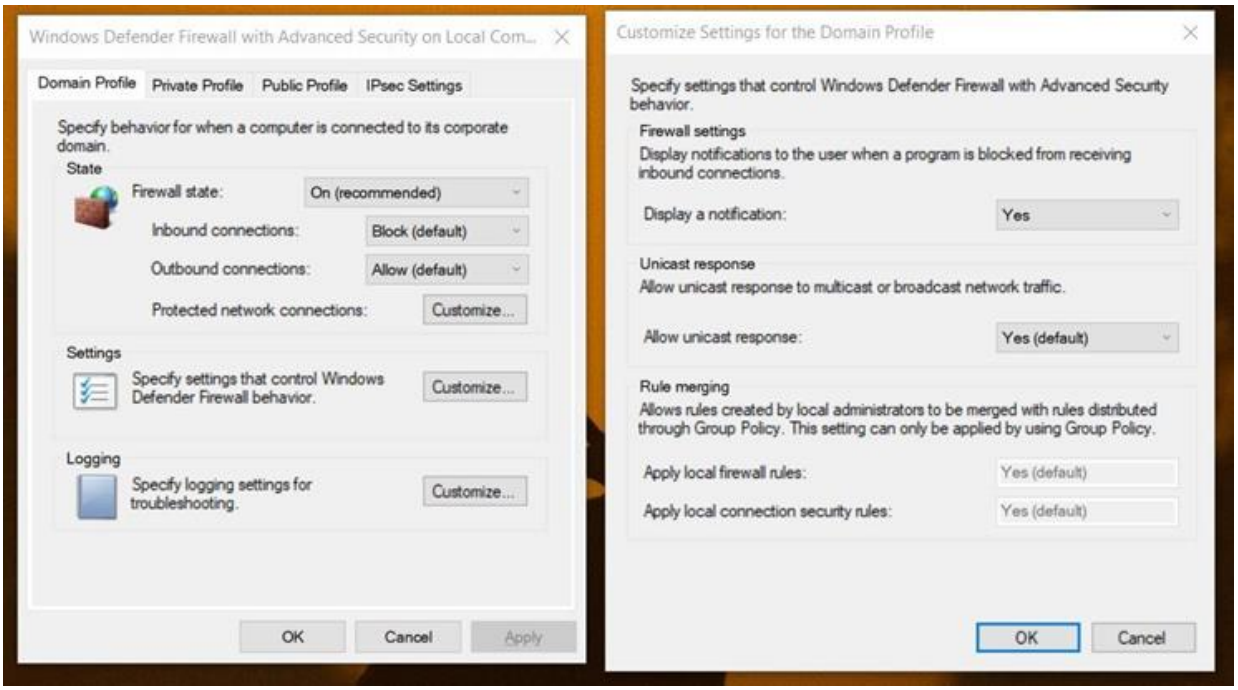



Windows Defender Firewall
Windows Defender Firewall with Advanced Security
File Action View Help
New Inbound Rule Wizard
Action
Specify the action to be taken when a connection matches the conditions specified in the rule.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
What action should be 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

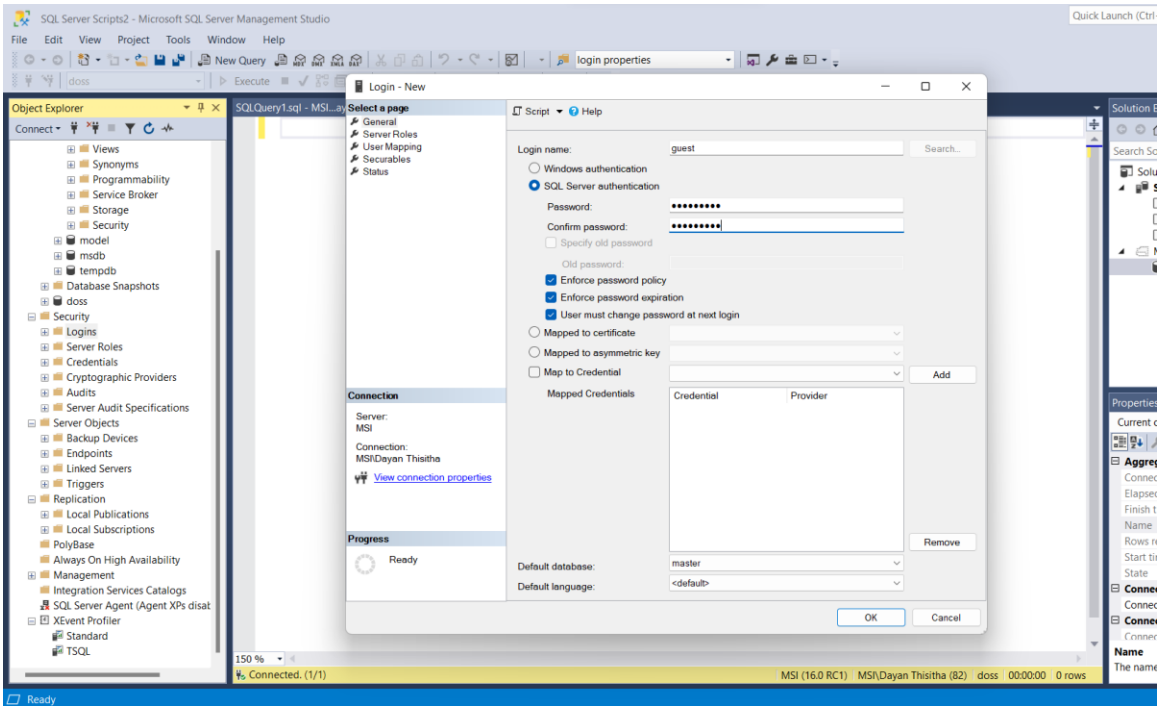

Windows Defender Firewall
Windows Defender Firewall with Advanced Security
File Action View Help
New Inbound Rule Wizard
Profile
Specify the profiles for which this rule applies.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
When does this rule apply?
Domain
Applies when a computer is connected 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

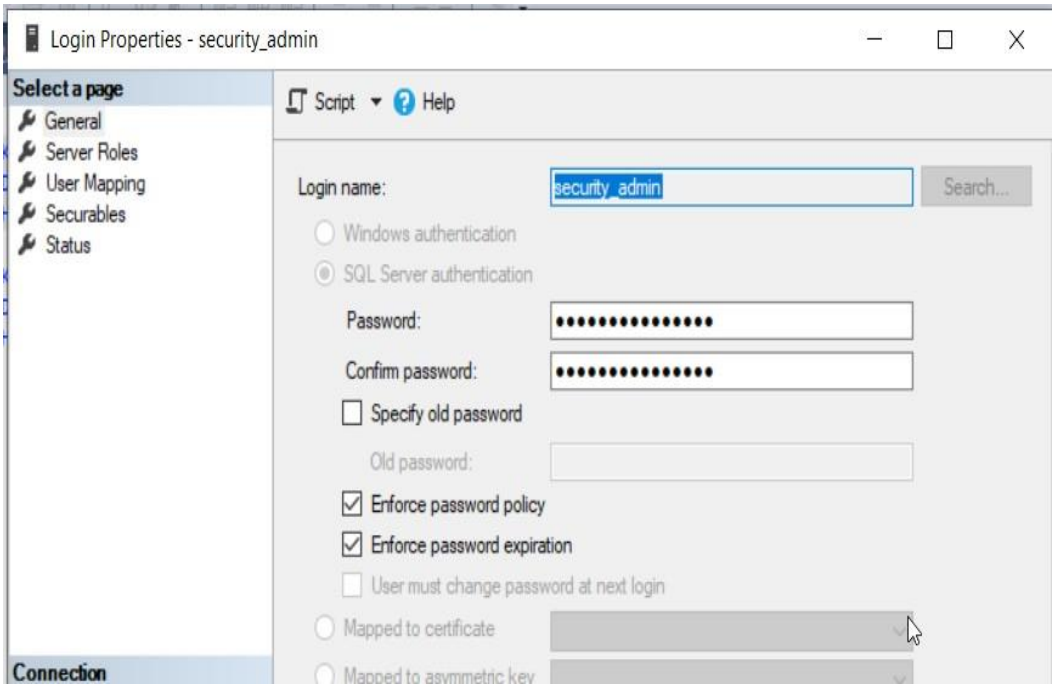


- Enable the notifications when rule is modified in the firewall

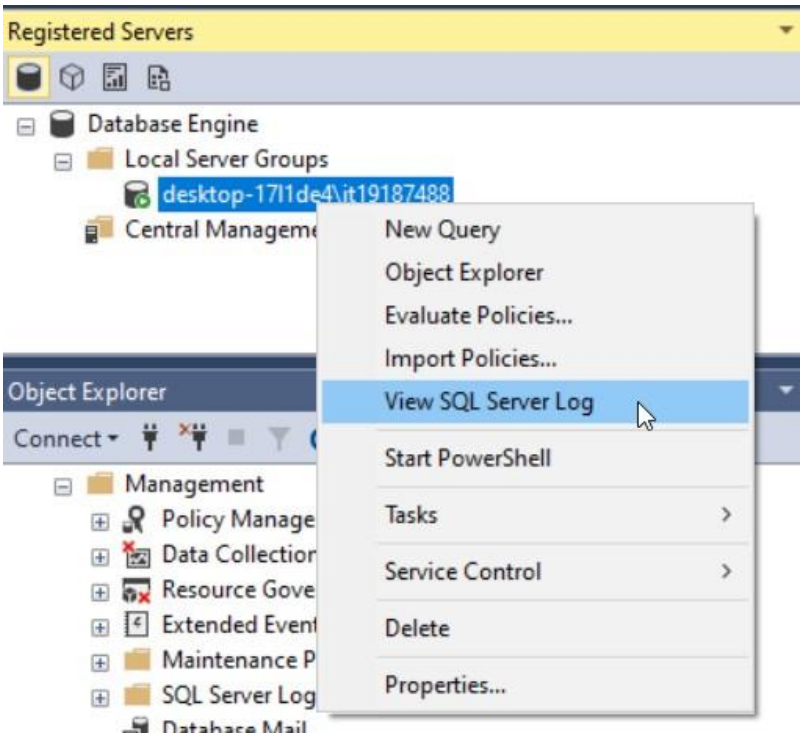


❖ **Database Software (All Unnecessary functions and accounts are removed, default passwords are changed)**

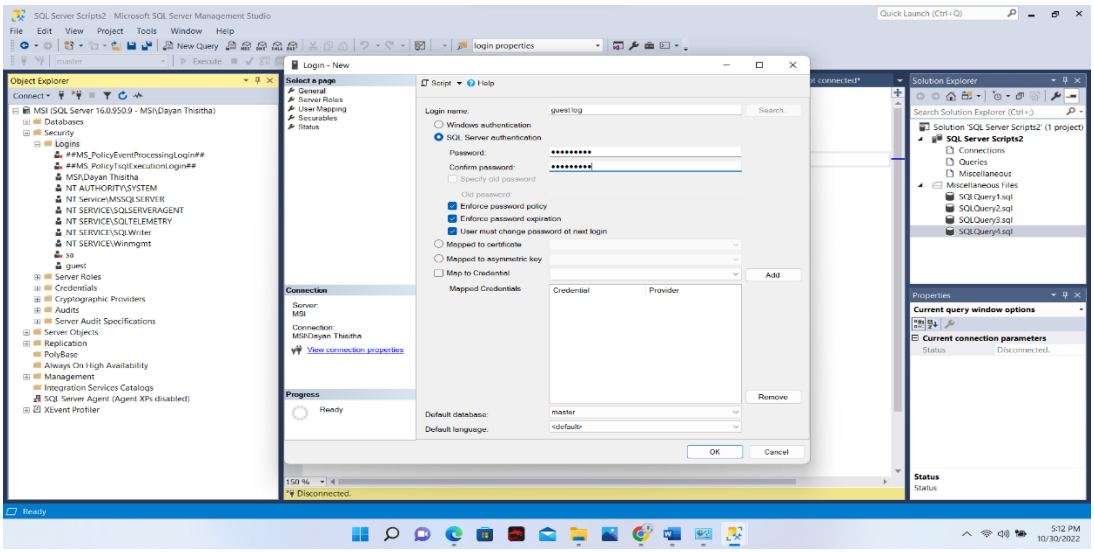


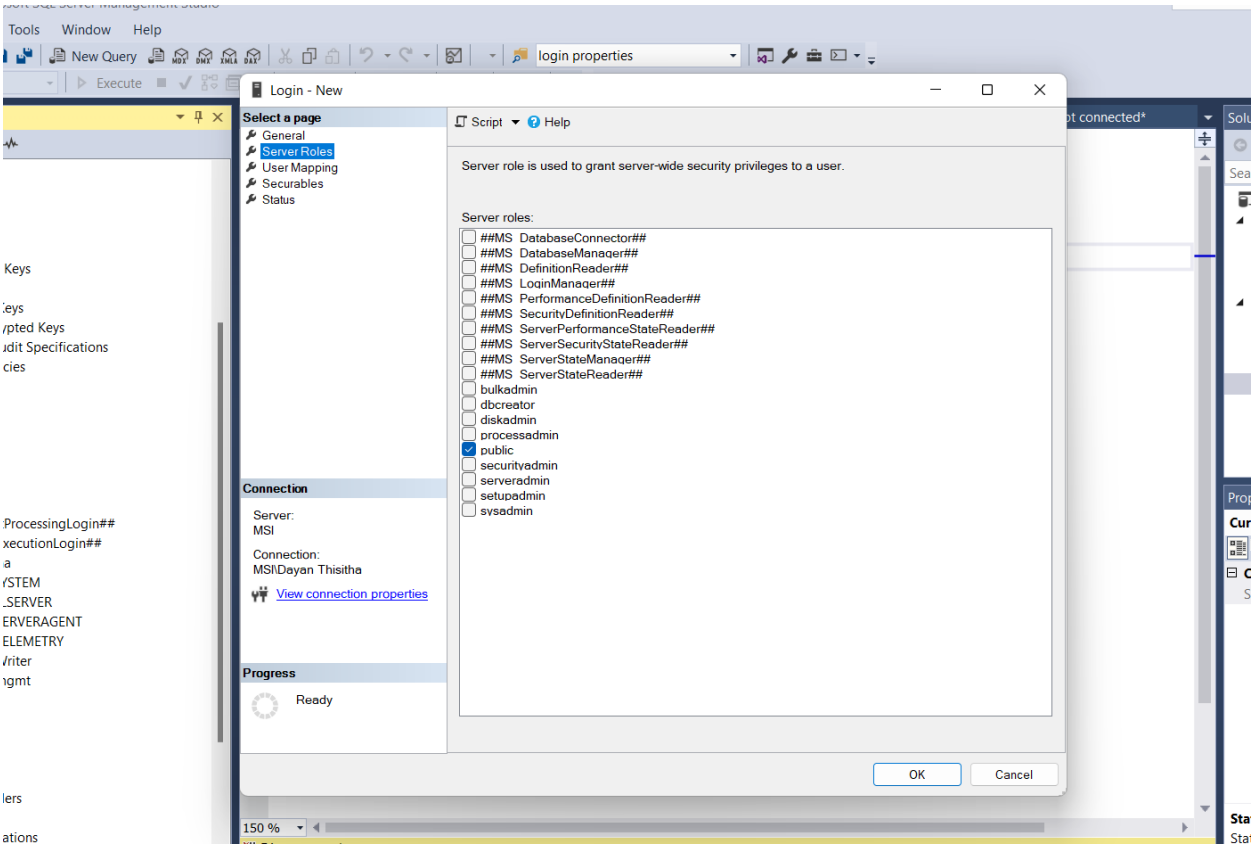


- **Maintain the log records of accessing to the database and maintain the minimum access privileges to the servers and applications.**



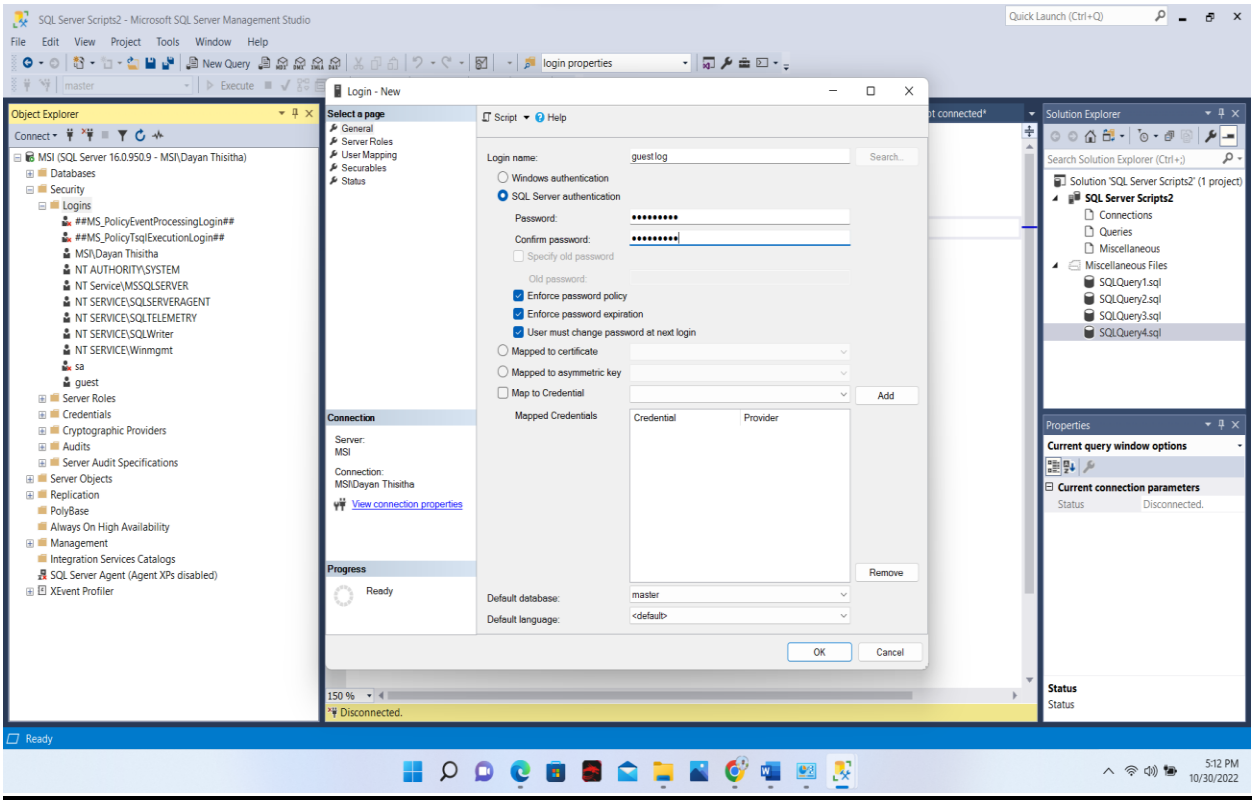
- **Maintain individual login credentials for the people who access the workstation and to perform administrative tasks of the database.**

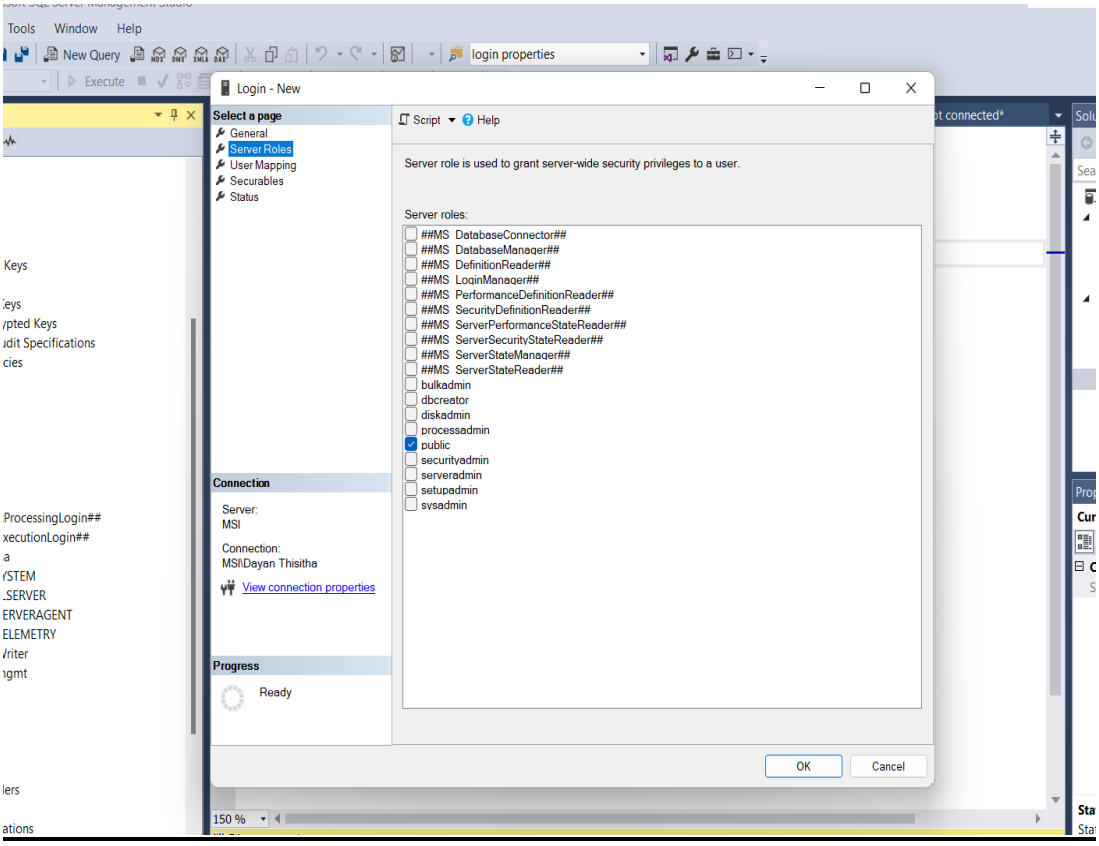


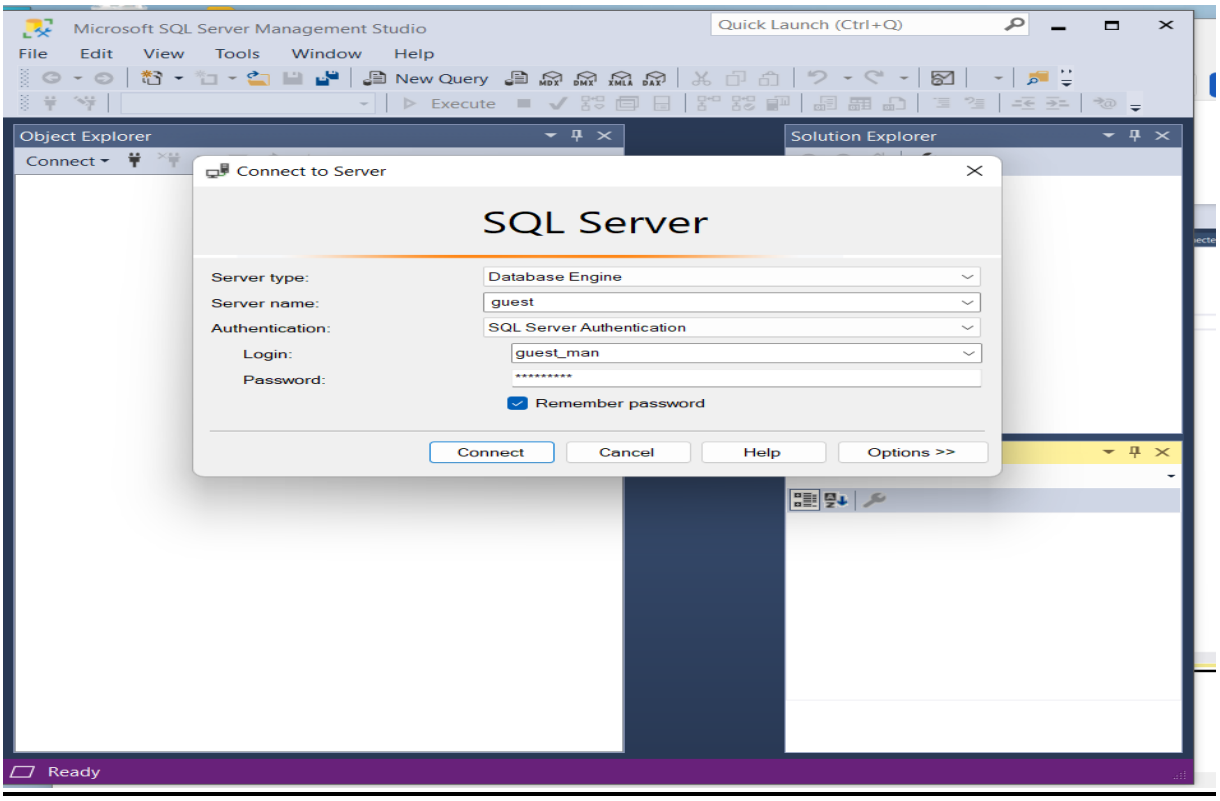

Tools
Window
Help
New Query
Execute
login properties
Login - New
Select a page
General
Server Roles
User Mapping
Securables
Status
Script
Help
Server role is used to grant server-wide security privileges to a user.
Server roles:
##MS_DatabaseConnector##
##MS_DatabaseManager##
##MS_DefinitionReader##
##MS_LoginManager##
##MS_PerformanceDefinitionReader##
##MS_SecurityDefinitionReader##
##MS_ServerPerformanceStateReader##
##MS_ServerSecurityStateReader##
##MS_ServerStateManager##
##MS_ServerStateReader##
bulkadmin
dbcreator
diskadmin
processadmin
public
securityadmin
serveradmin
setupadmin
sysadmin
Connection
Server:
MSI
Connection:
MSI\Dayan Thisitha
View connection properties
Progress
Ready
OK
Cancel
150 %

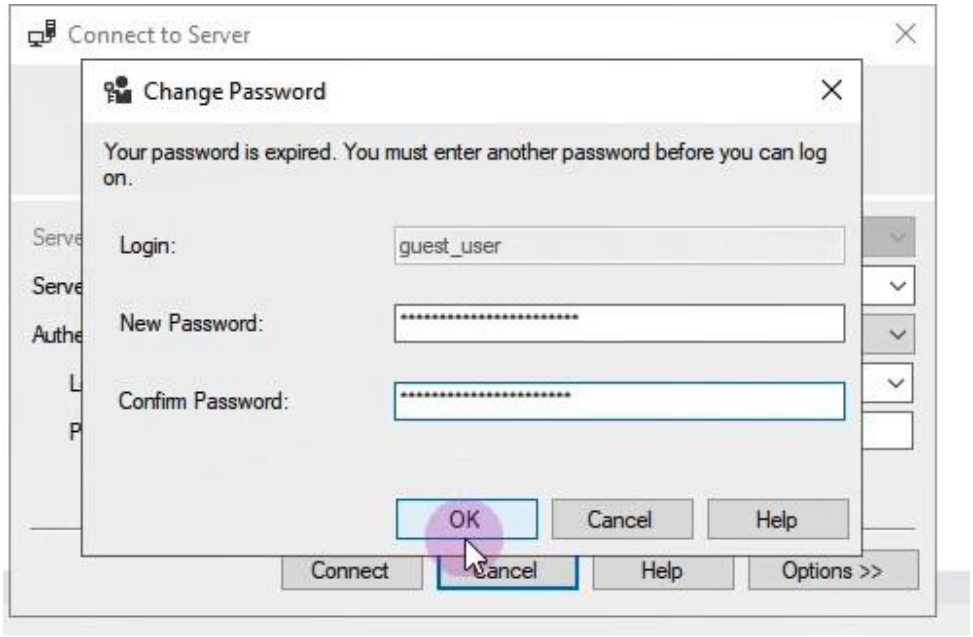

Connect to Server
SQL Server
Server type:
Database Engine
Server name:
LAPTOP-9GH53O0P\IT18211160
Authentication:
SQL Server Authentication
Login:
server_security_admin
Password:
Remember password
Connect
Cancel
Help
Options >>

❖ Create login for guest user and testing login



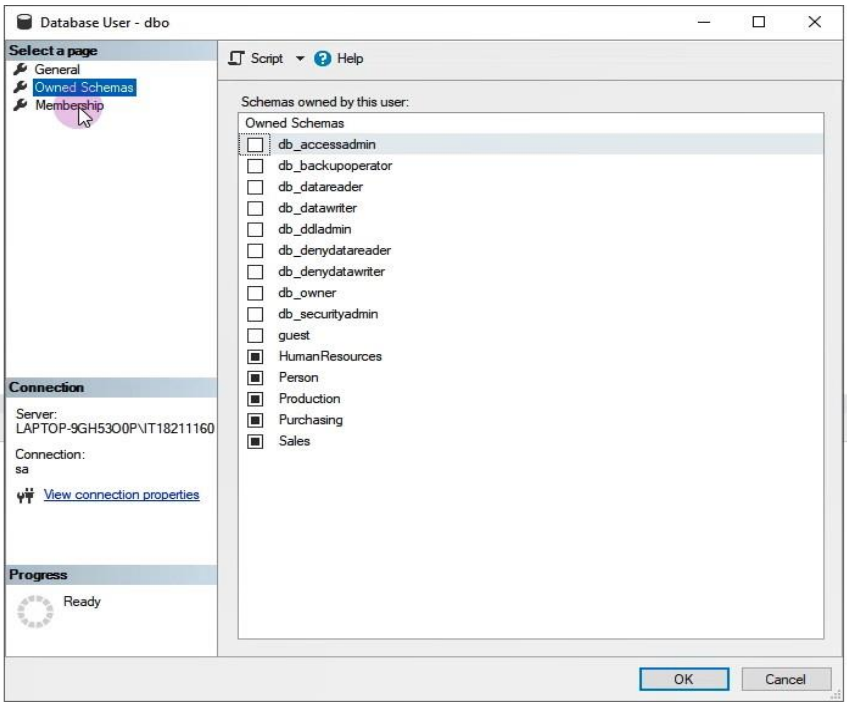

Tools
Window
Help
New Query
Execute
login properties
Login - New
Select a page
General
Server Roles
User Mapping
Securables
Status
Script
Help
Server role is used to grant server-wide security privileges to a user.
Server roles:
##MS_DatabaseConnector##
##MS_DatabaseManager##
##MS_DefinitionReader##
##MS_LoginManager##
##MS_PerformanceDefinitionReader##
##MS_SecurityDefinitionReader##
##MS_ServerPerformanceStateReader##
##MS_ServerSecurityStateReader##
##MS_ServerStateManager##
##MS_ServerStateReader##
bulkadmin
dbcreator
diskadmin
processadmin
public
securityadmin
serveradmin
setupadmin
sysadmin
Connection
Server:
MSI
Connection:
MSI\Dayan Thisitha
View connection properties
Progress
Ready
OK
Cancel
150 %

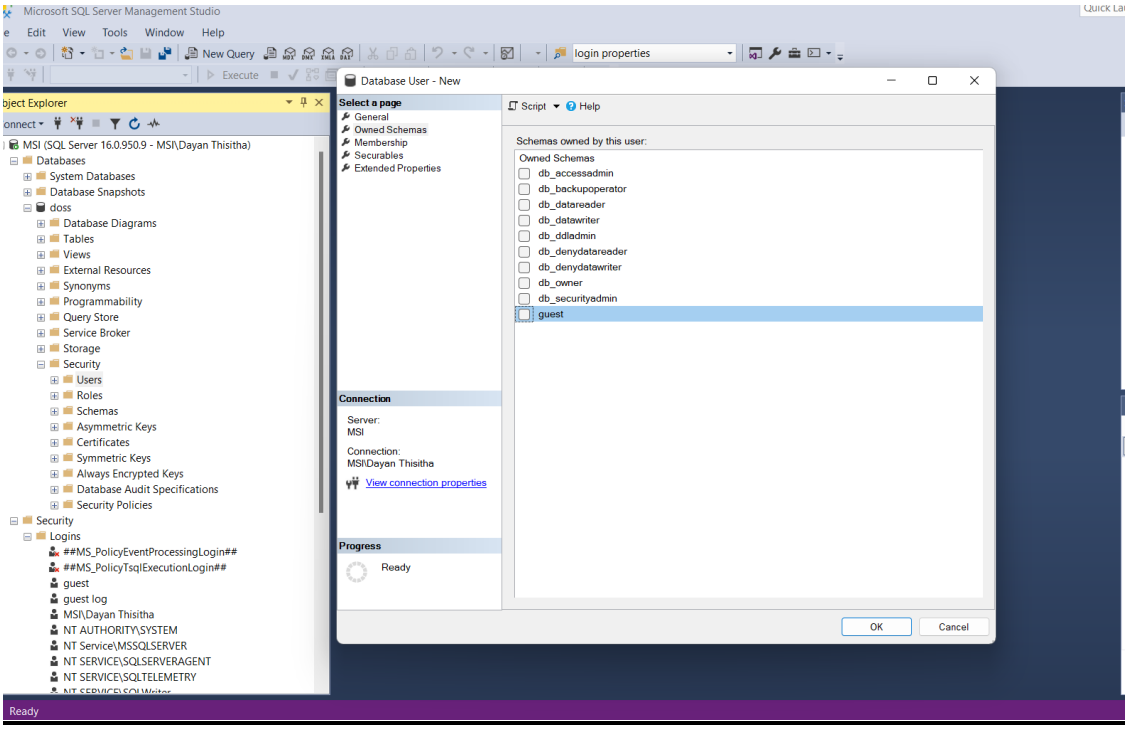

Microsoft SQL Server Management Studio
Quick Launch (Ctrl+Q)
File
Edit
View
Tools
Window
Help
New Query
Execute
Object Explorer
Connect
Solution Explorer
Connect to Server
SQL Server
Server type:
Database Engine
Server name:
guest
Authentication:
SQL Server Authentication
Login:
guest_man
Password:
Remember password
Connect
Cancel
Help
Options >>
Ready


Connect to Server
Change Password
Your password is expired. You must enter another password before you can log on.
Login:
guest_user
New Password:
Confirm Password:
OK
Cancel
Help
Connect
Cancel
Help
Options >>

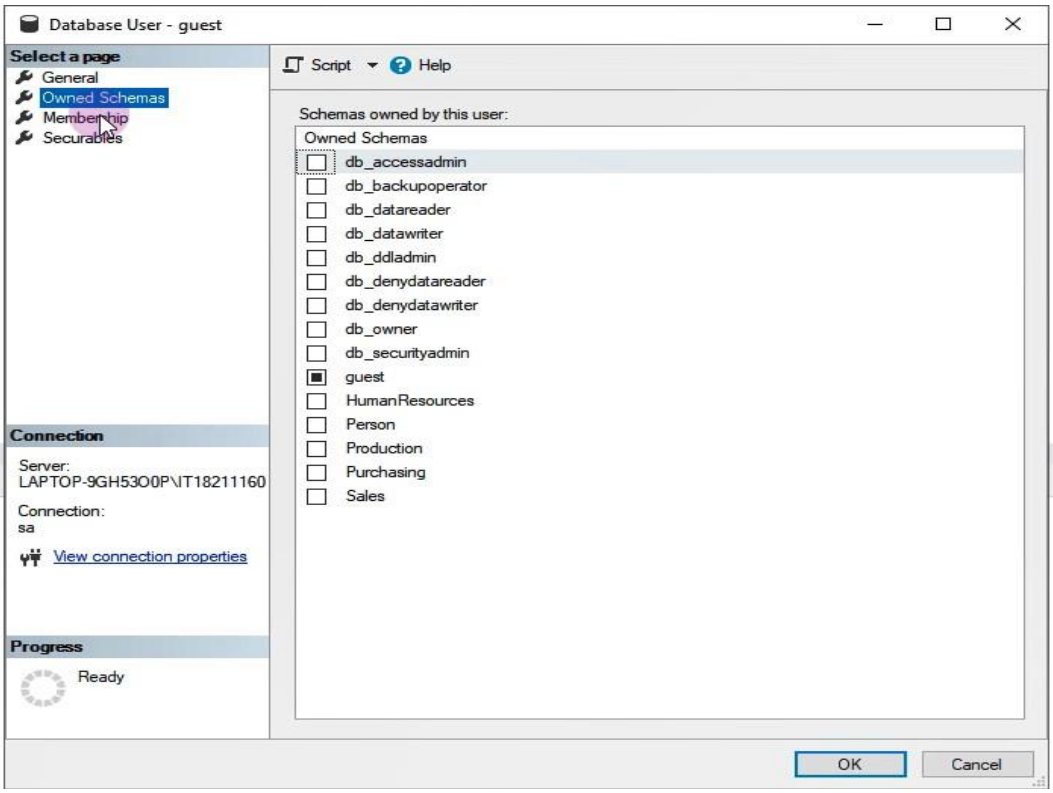
❖ **Grant minimal permissions that necessary for the people according to their job role in the database.**

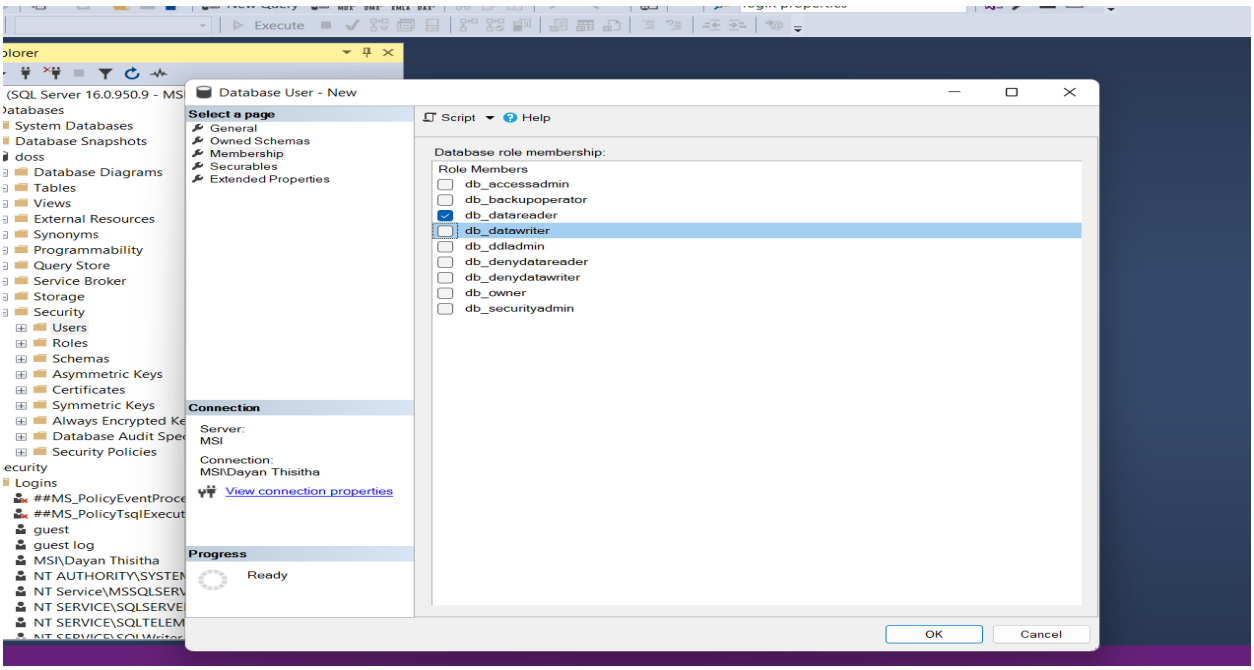
- ❖ Database Owner(dbo)



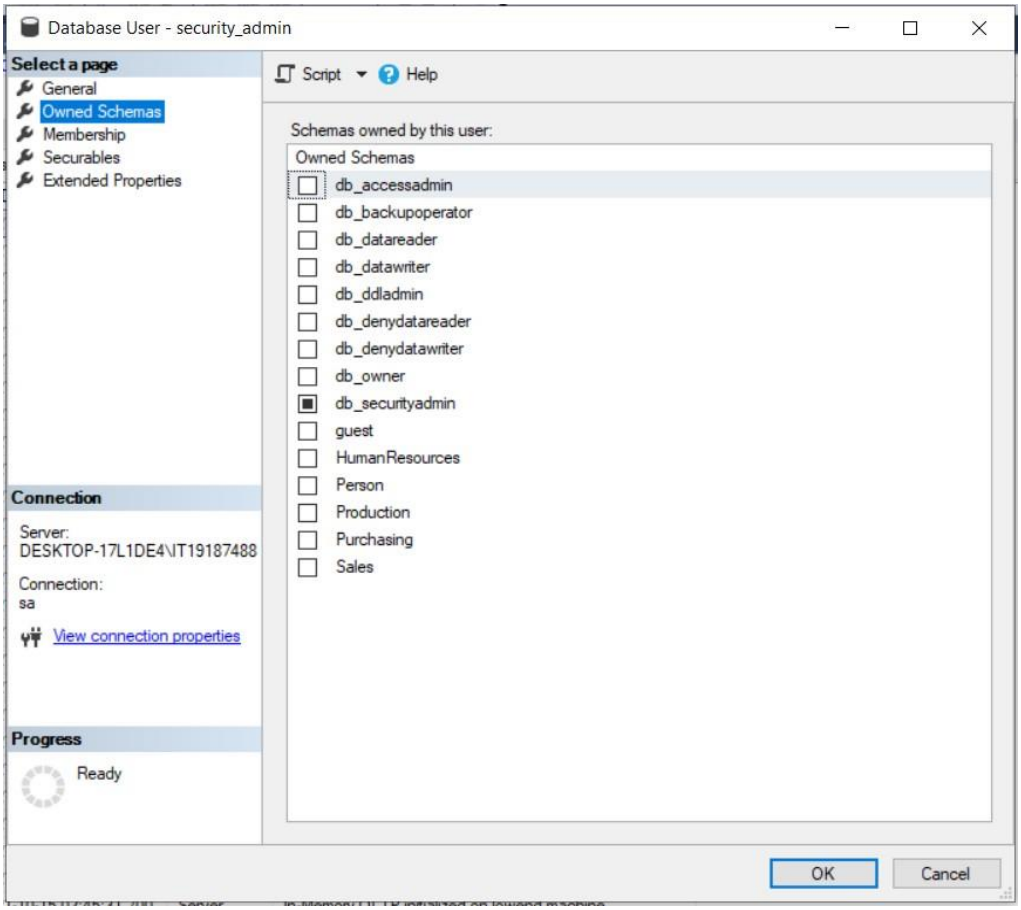


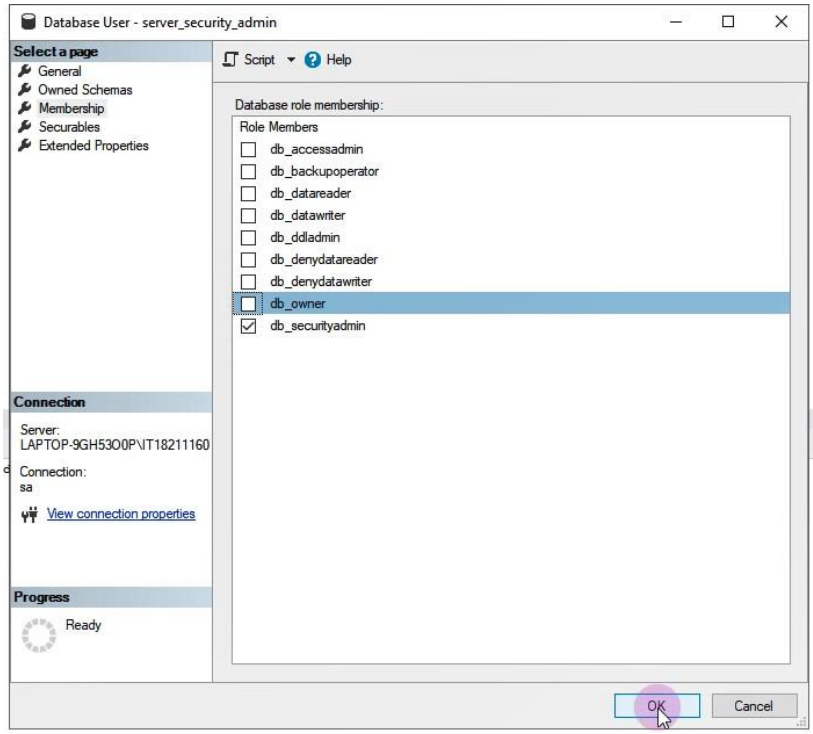
❖ Guest user


Database User - guest
Select a page
General
Owned Schemas
Membership
Securables
Script
Help
Schemas owned by this user:
Owned Schemas
db_accessadmin
db_backupoperator
db_datareader
db_datawriter
db_ddladmin
db_denydatareader
db_denydatawriter
db_owner
db_securityadmin
guest
HumanResources
Person
Production
Purchasing
Sales
Connection
Server:
LAPTOP-9GH53O0P\IT18211160
Connection:
sa
View connection properties
Progress
Ready
OK
Cancel

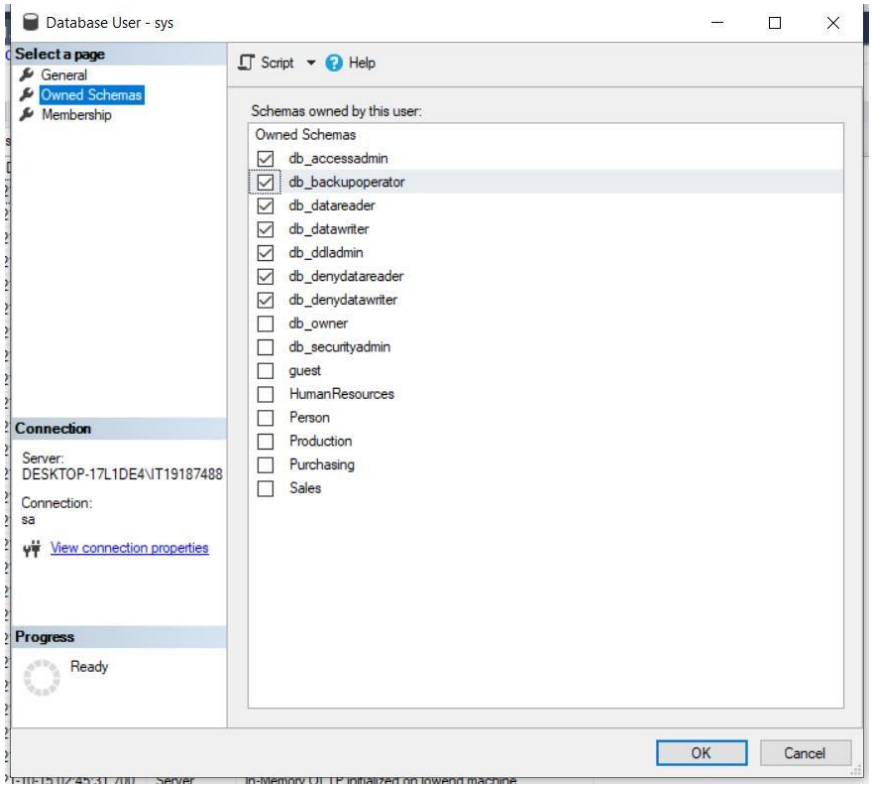

Database User - New
Select a page
General
Owned Schemas
Membership
Securables
Extended Properties
Script
Help
Database role membership:
Role Members
db_accessadmin
db_backupoperator
db_datareader
db_datawriter
db_ddladmin
db_denydatareader
db_denydatawriter
db_owner
db_securityadmin
Connection
Server:
MSI
Connection:
MSI\Dayan Thisitha
View connection properties
Progress
Ready
OK
Cancel

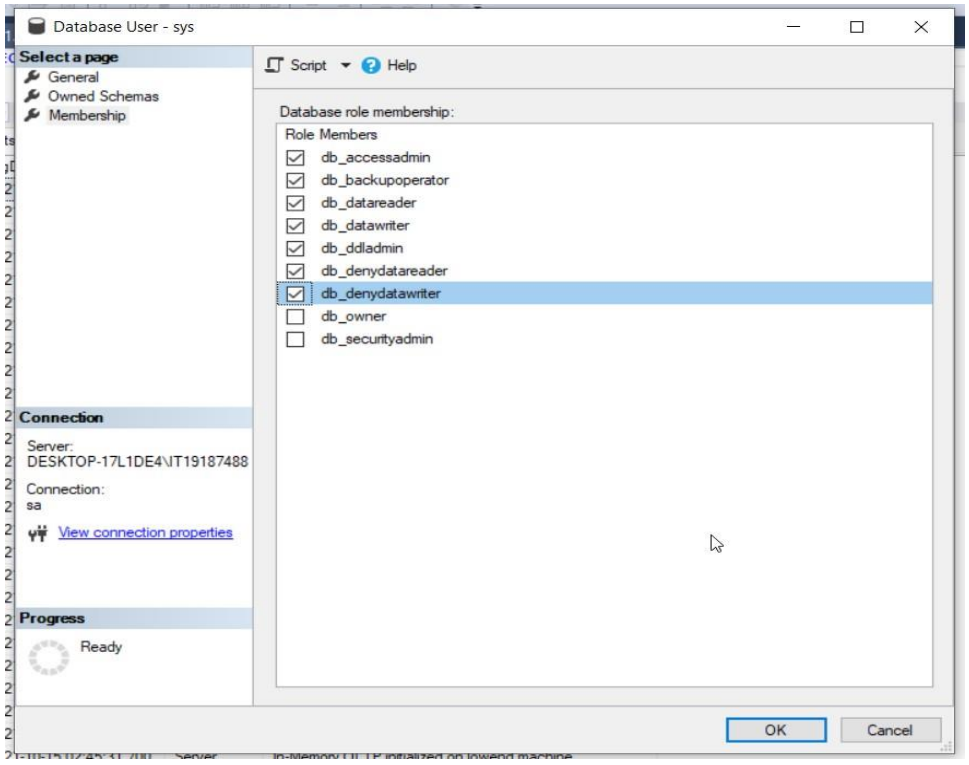
❖ Server security admin



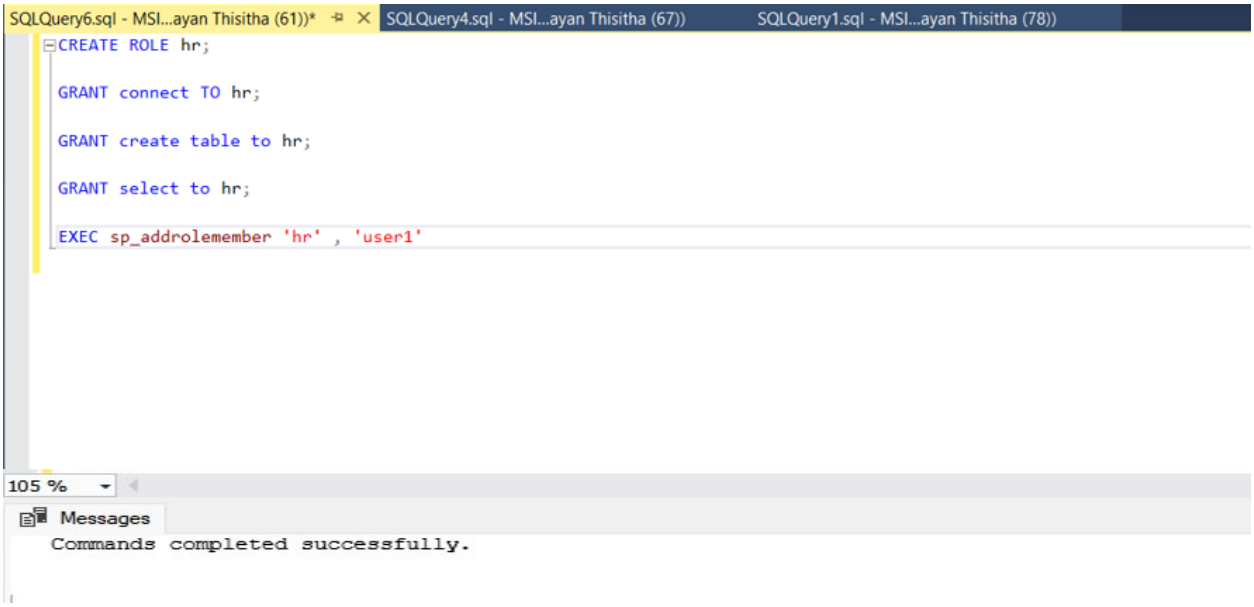


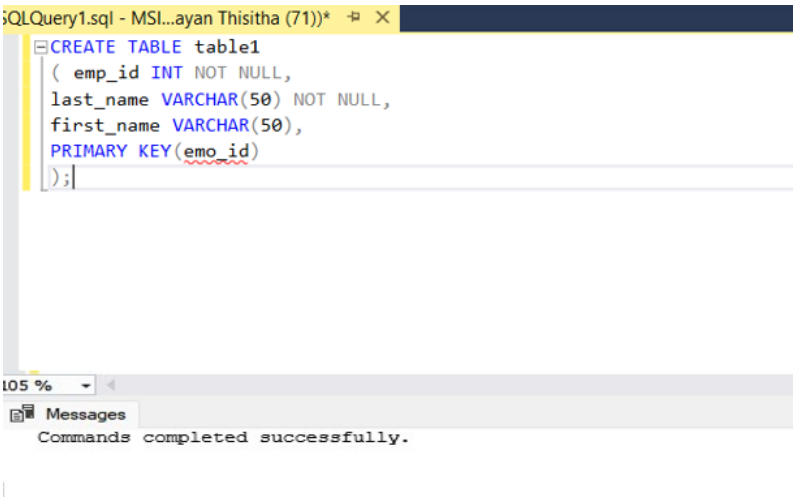
❖ Sys


Database User - sys
Select a page
General
Owned Schemas
Membership
Script
Help
Schemas owned by this user:
Owned Schemas
db_accessadmin
db_backupoperator
db_datareader
db_datawriter
db_ddladmin
db_denydatareader
db_denydatawriter
db_owner
db_securityadmin
guest
HumanResources
Person
Production
Purchasing
Sales
Connection
Server:
DESKTOP-17L1DE4\IT19187488
Connection:
sa
View connection properties
Progress
Ready
OK
Cancel

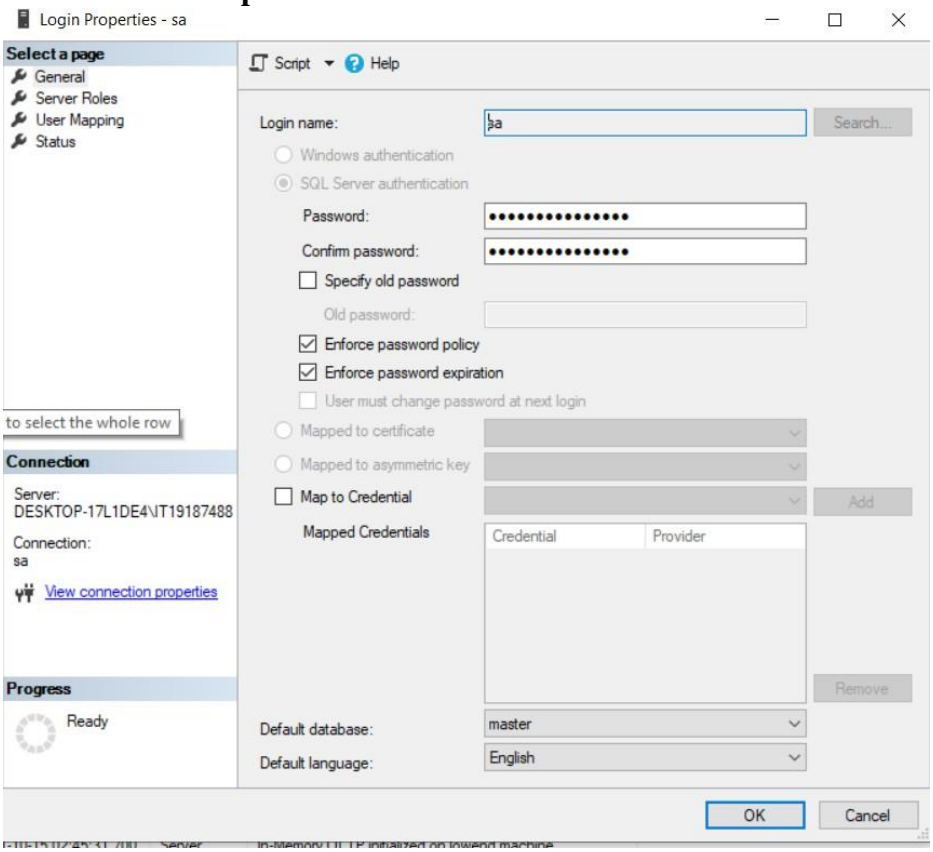

Database User - sys
Select a page
General
Owned Schemas
Membership
Script
Help
Database role membership:
Role Members
db_accessadmin
db_backupoperator
db_datareader
db_datawriter
db_ddladmin
db_denydatareader
db_denydatawriter
db_owner
db_securityadmin
Connection
Server:
DESKTOP-17L1DE4\IT19187488
Connection:
sa
View connection properties
Progress
Ready
OK
Cancel

- **Permissions should be managed through roles or groups and not by direct grants to User IDs where possible.**



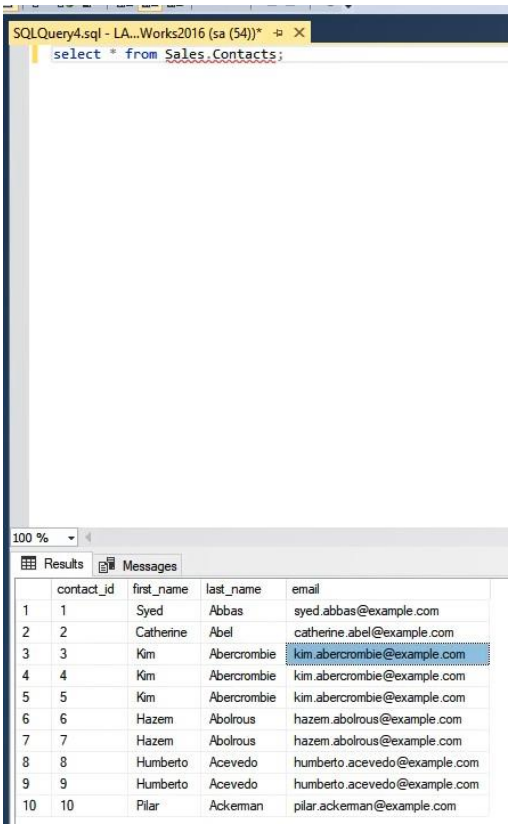


- **Manage to use strong password and follow secure methods to preserve the stored passwords.**



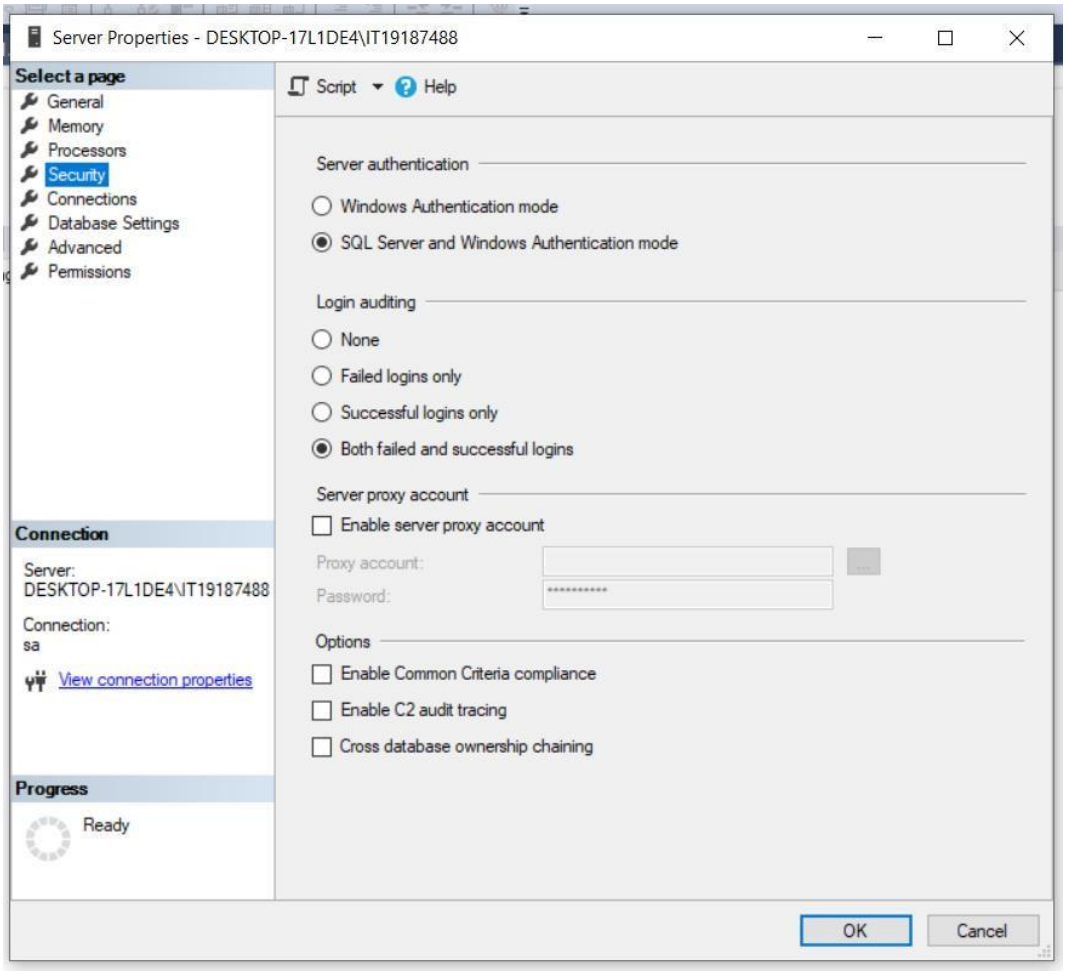
- **Prevent from redundancy of the stored records of the database**

Sales.Contacts redundancy check



	contact_id	first_name	last_name	email
1	1	Syed	Abbas	syed.abbas@example.com
2	2	Catherine	Abel	catherine.abel@example.com
3	3	Kim	Abercrombie	kim.abercrombie@example.com
4	4	Kim	Abercrombie	kim.abercrombie@example.com
5	5	Kim	Abercrombie	kim.abercrombie@example.com
6	6	Hazem	Abolrous	hazem.abolrous@example.com
7	7	Hazem	Abolrous	hazem.abolrous@example.com
8	8	Humberto	Acevedo	humberto.acevedo@example.com
9	9	Humberto	Acevedo	humberto.acevedo@example.com
10	10	Pilar	Ackerman	pilar.ackerman@example.com

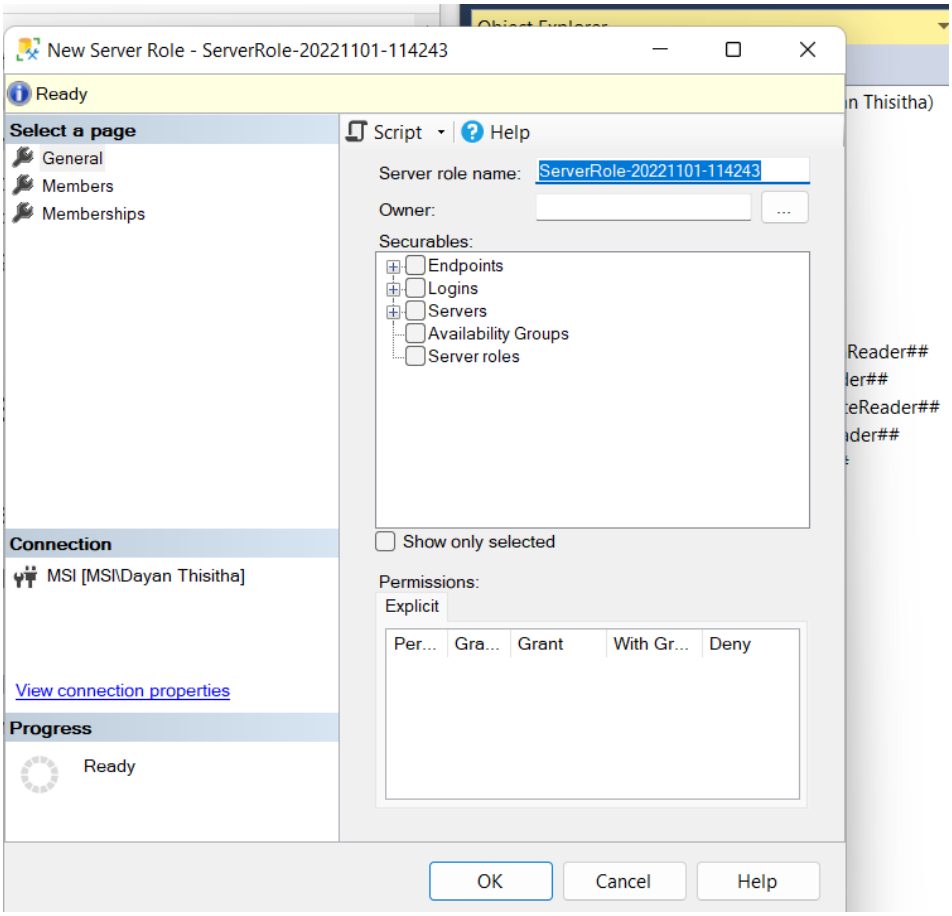
- **Turn on Auditing where technically possible for the database objects with protected data.**



- **Discuss how manage the implemented database backup and recovery.**

  - server backup with t-sql

```
USE AdventureWorks2016
GO
BACKUP DATABASE [AdventureWorks2016]
TO  DISK = N'E:\DatabaseBackups\AD_ALL.bak'
WITH CHECKSUM;
```



server backup with scheduler