



Sri Lanka Institute of Information Technology

Assignment – Implementing Security features in OS and DB

Data and Operating System Security

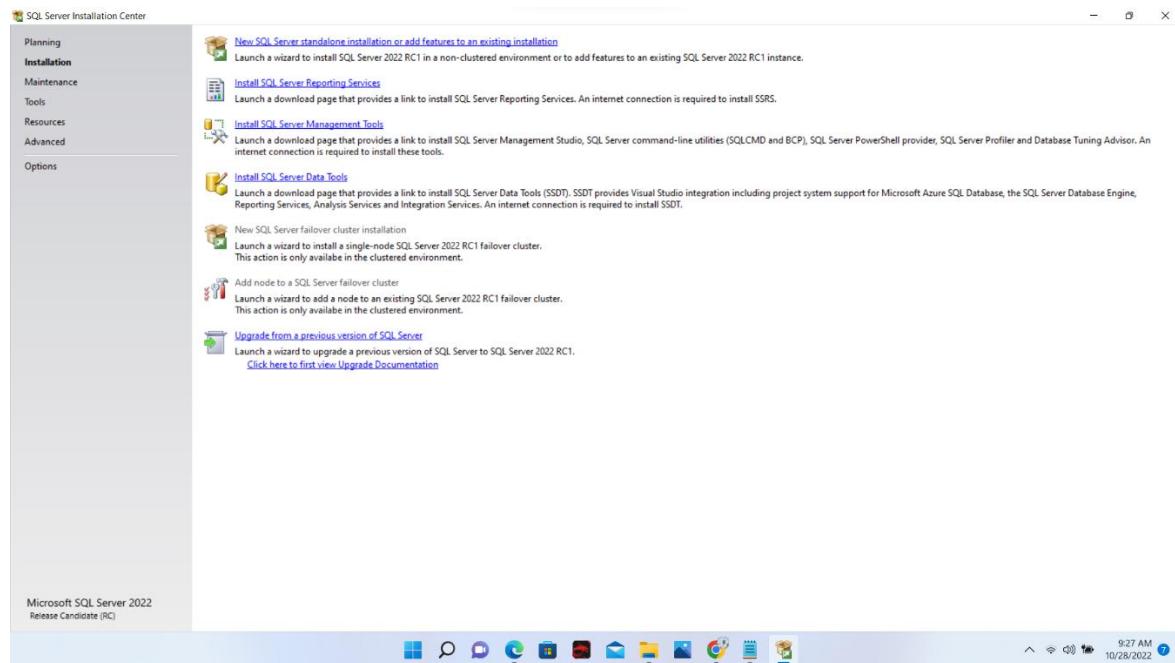
- IE3062

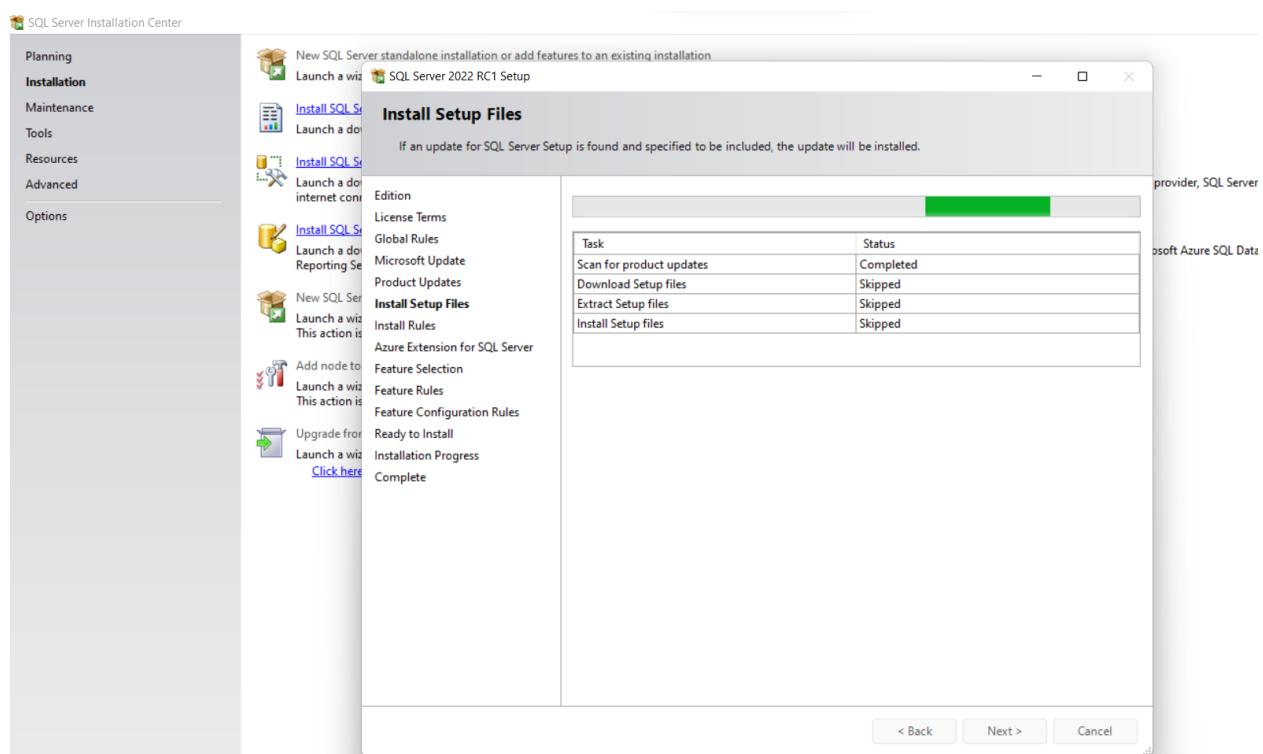
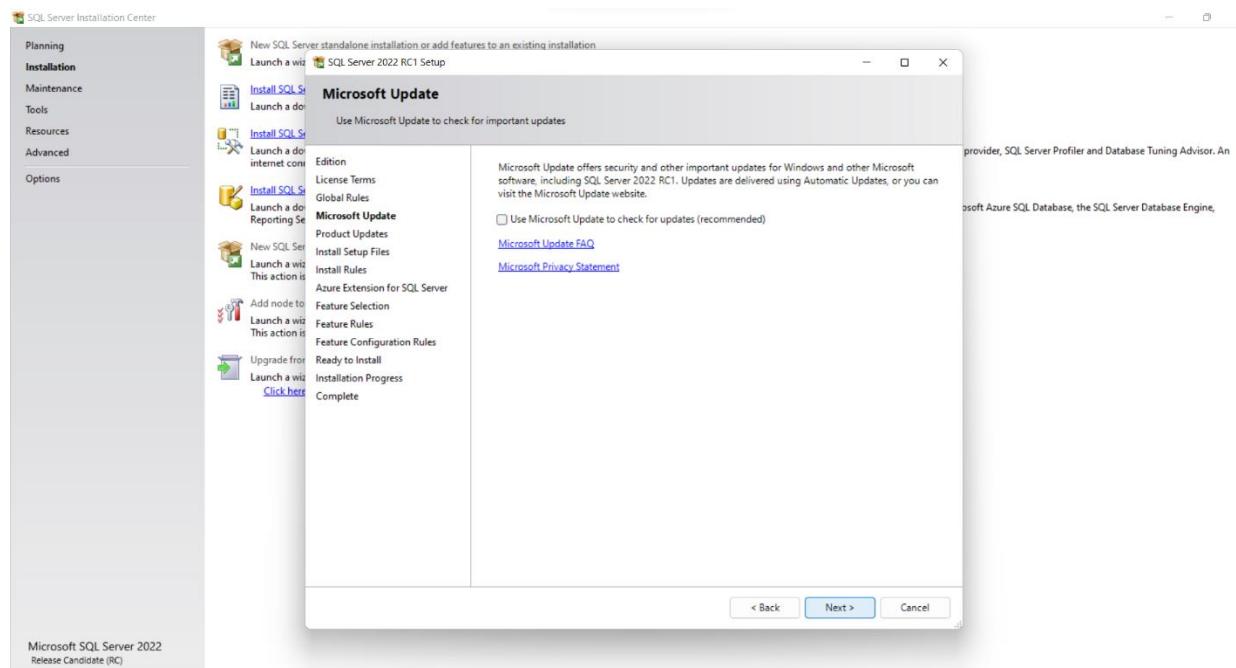
—

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

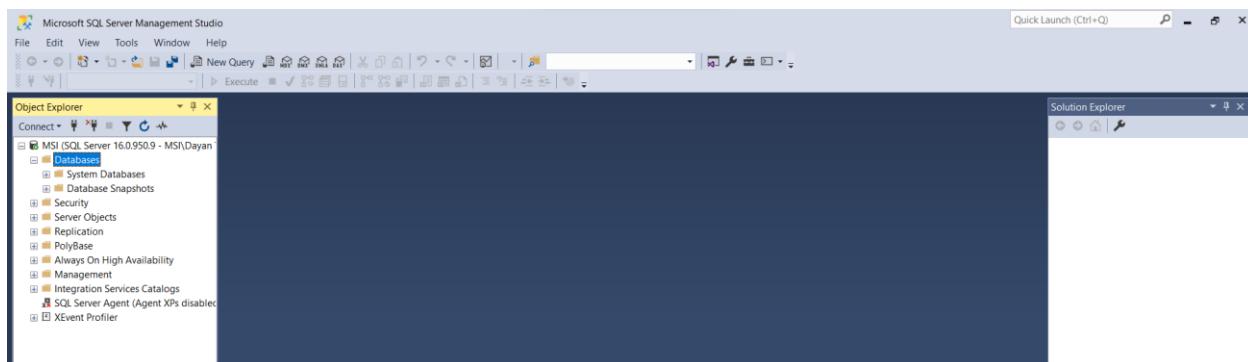
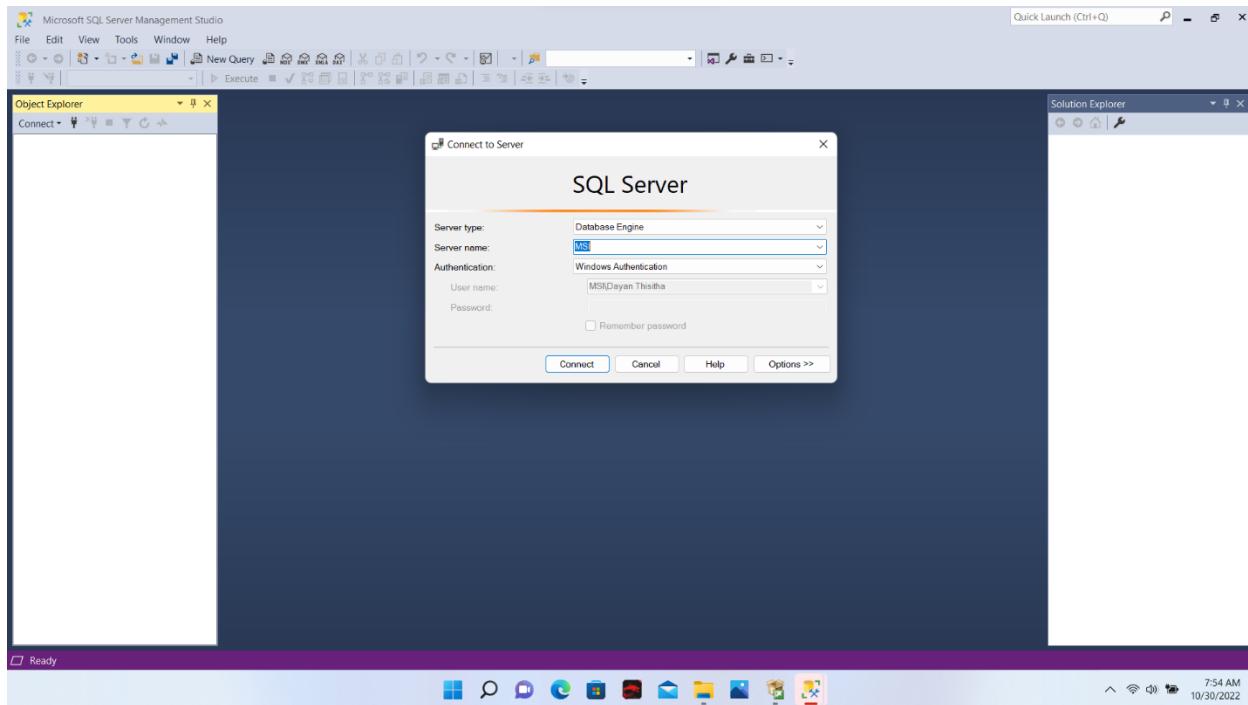


1. Install SQL server

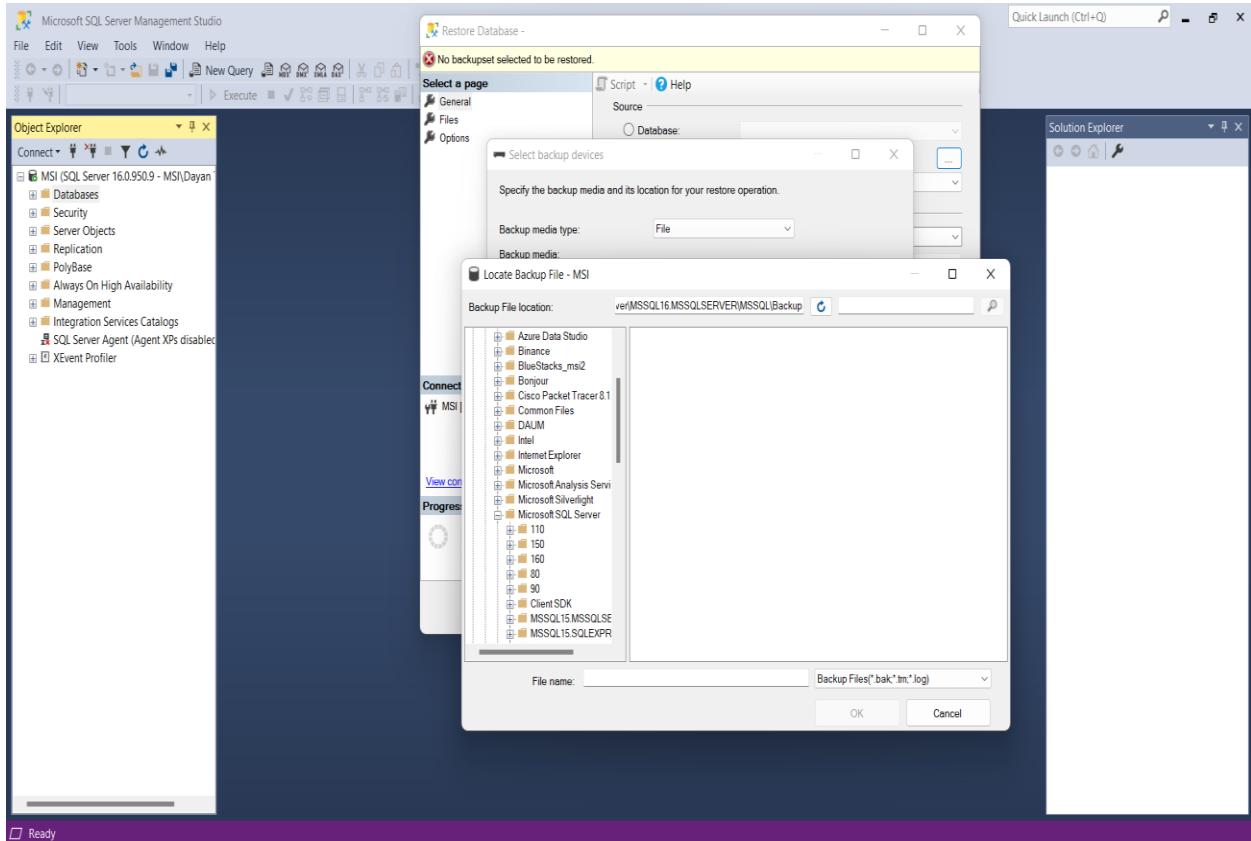




2. Connect to server



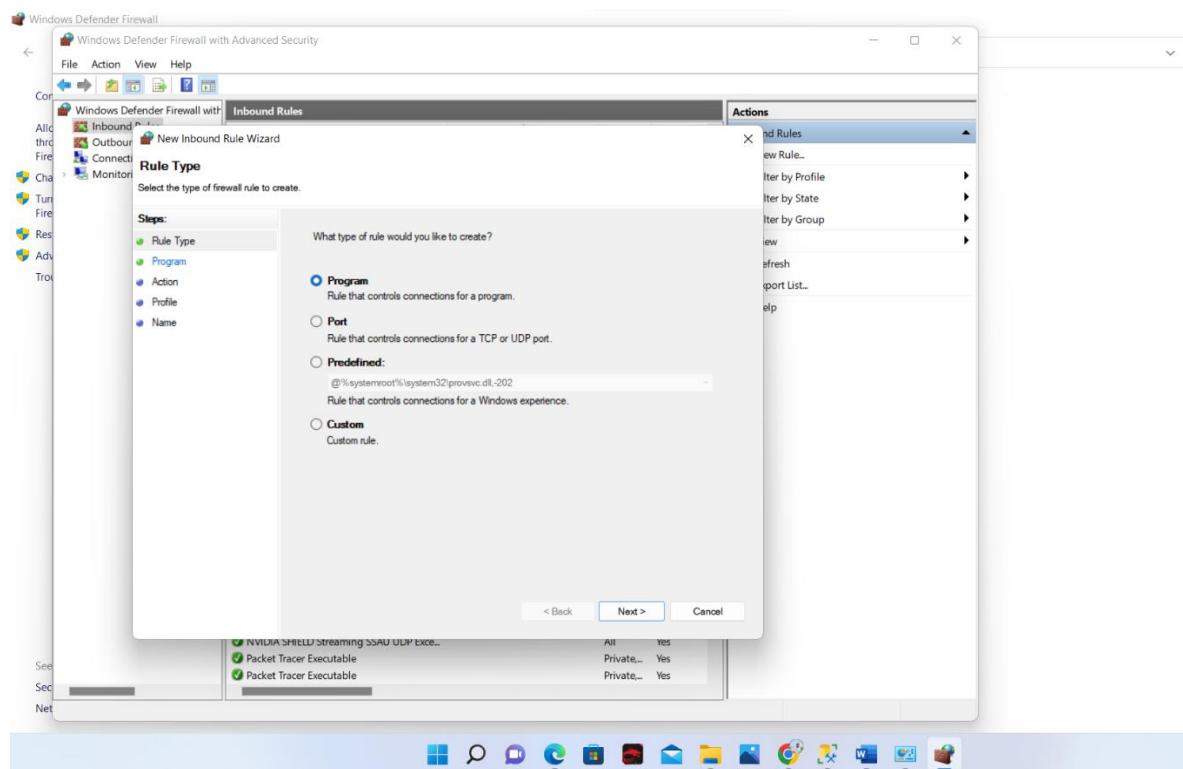
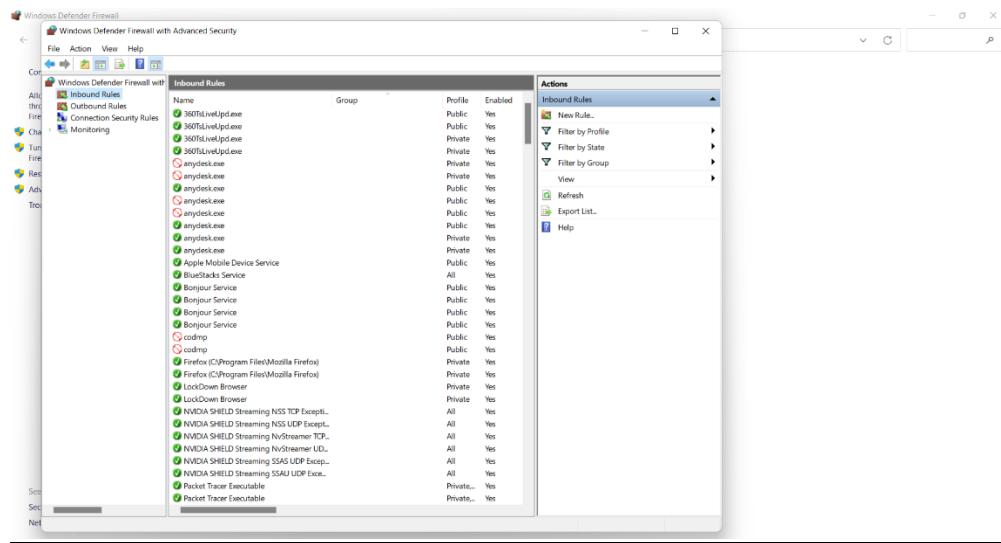
3. Restore / Import database

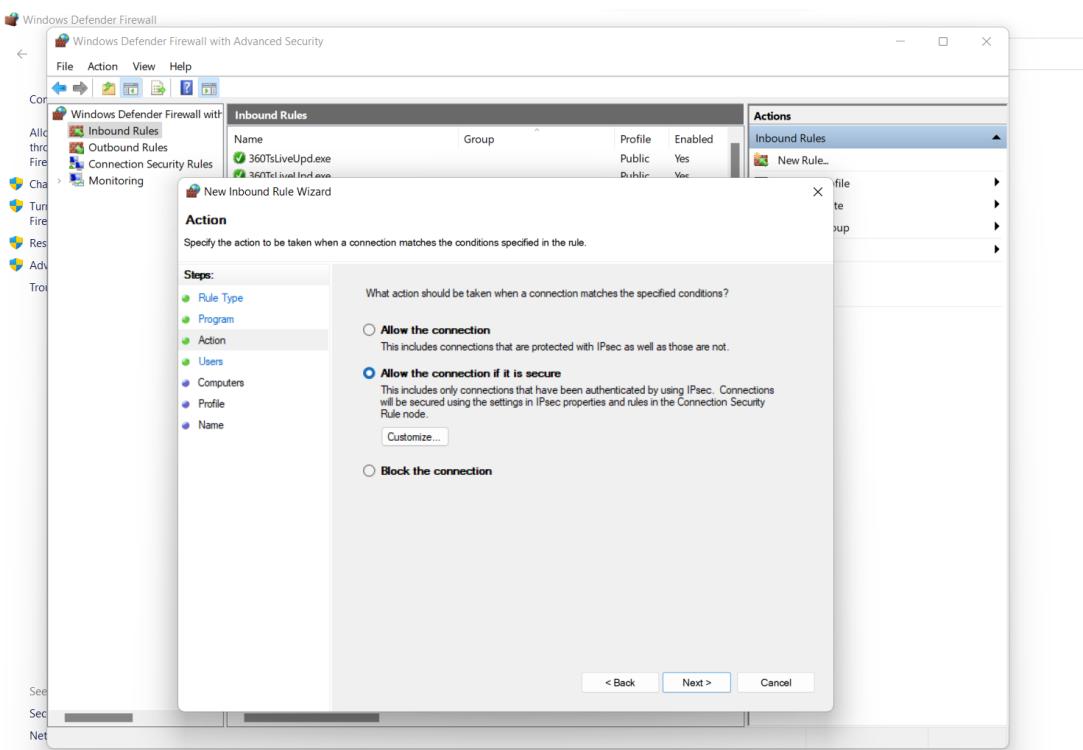
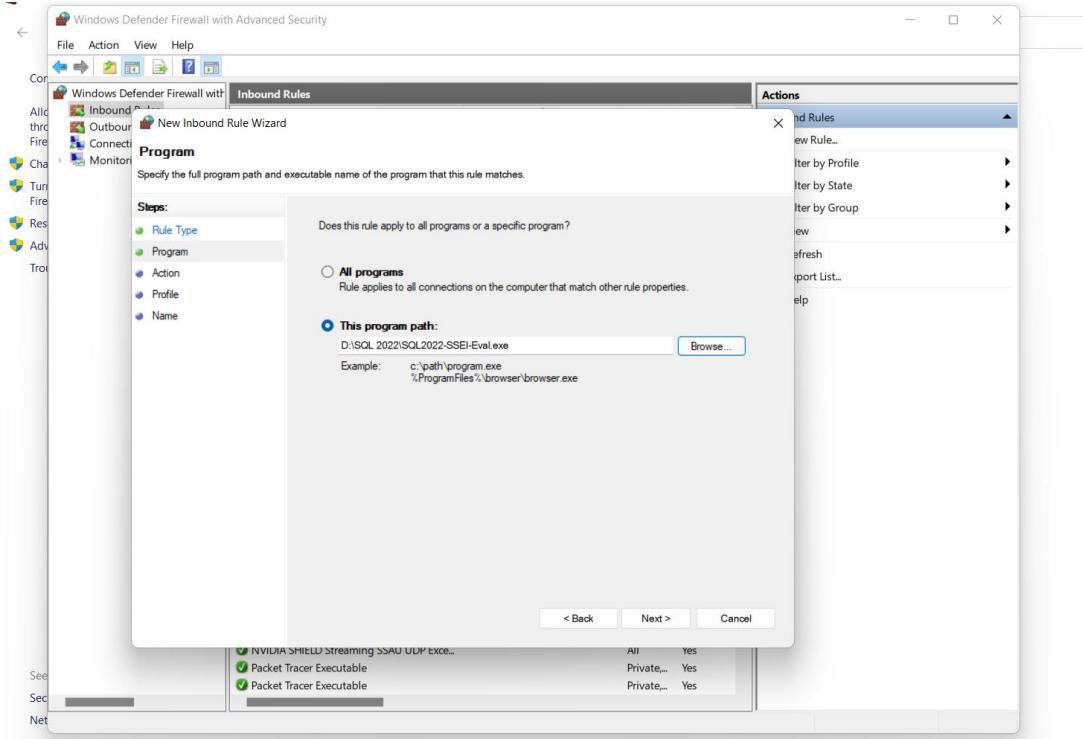


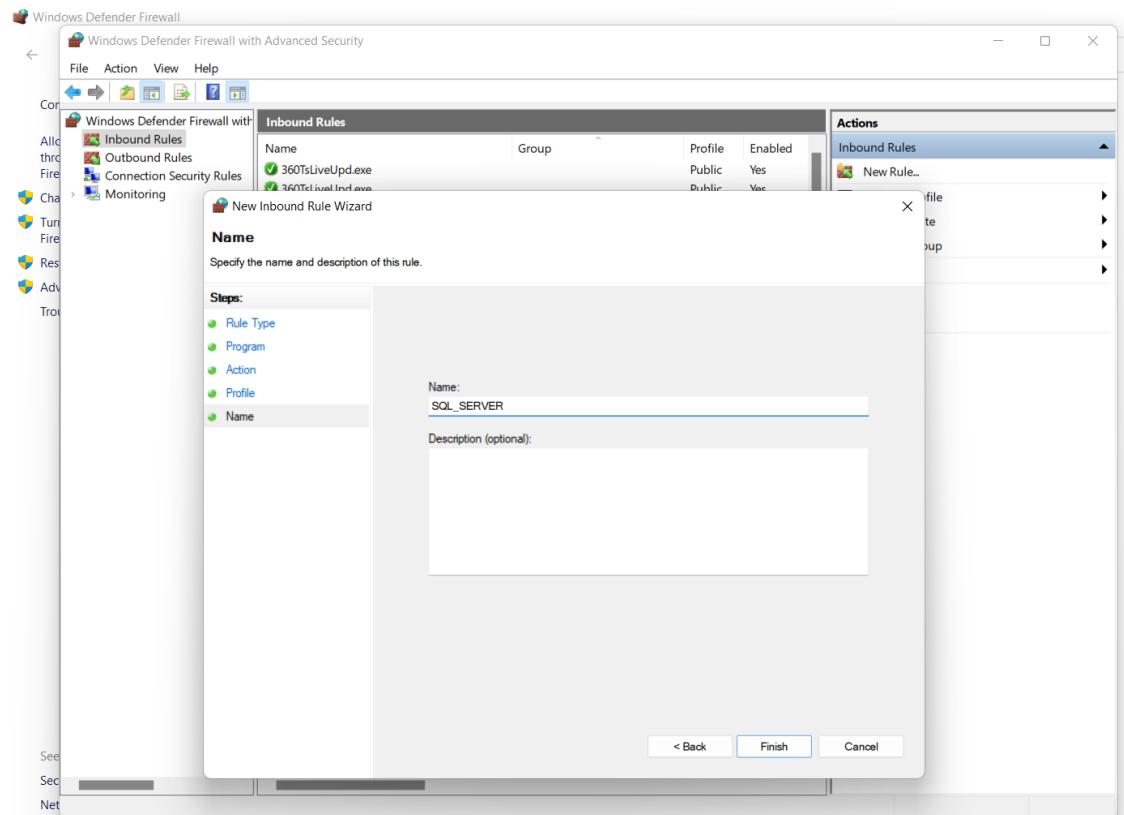
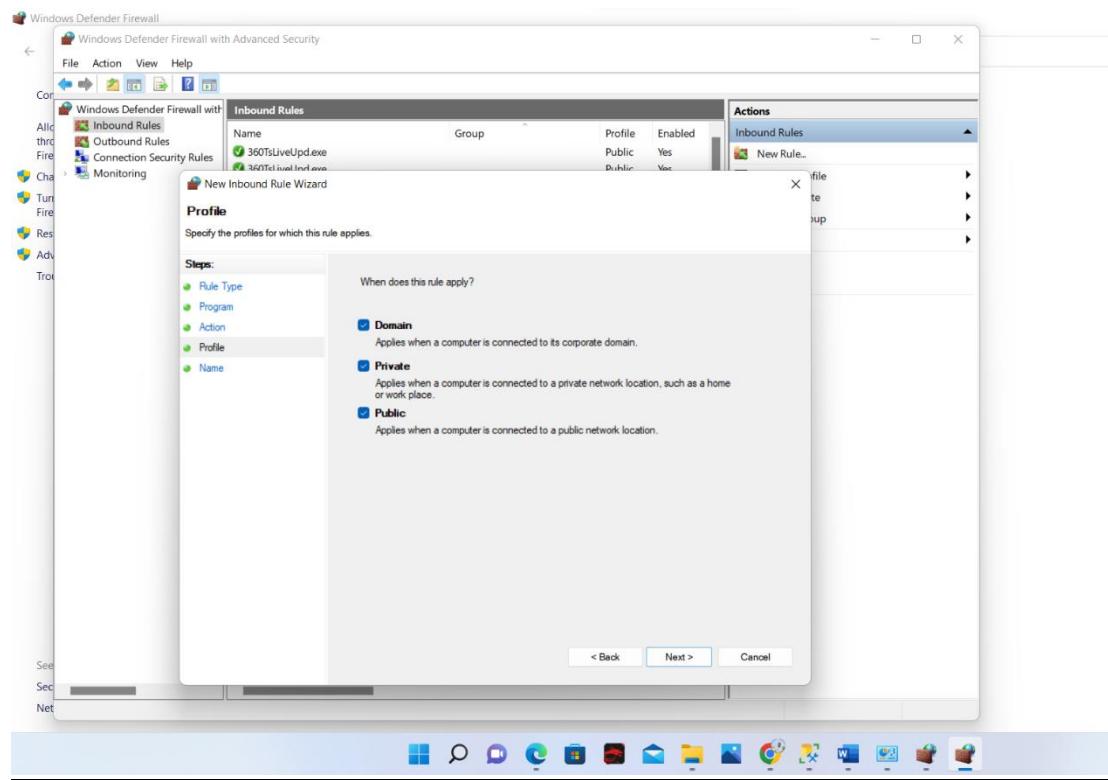
The Security Check list to be implemented

1. Firewall for database servers

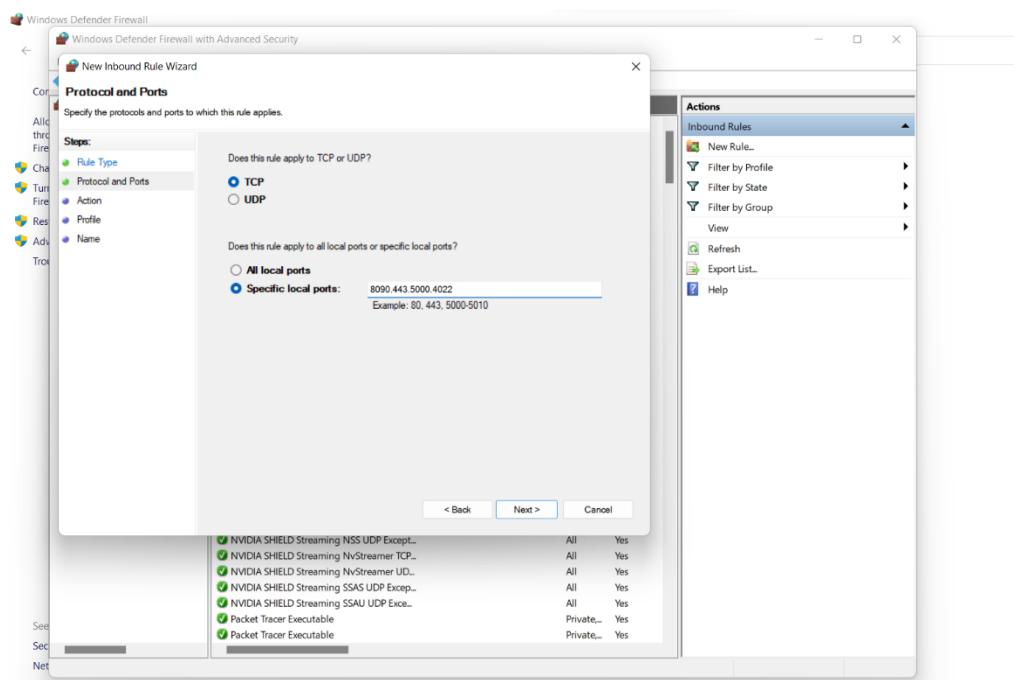
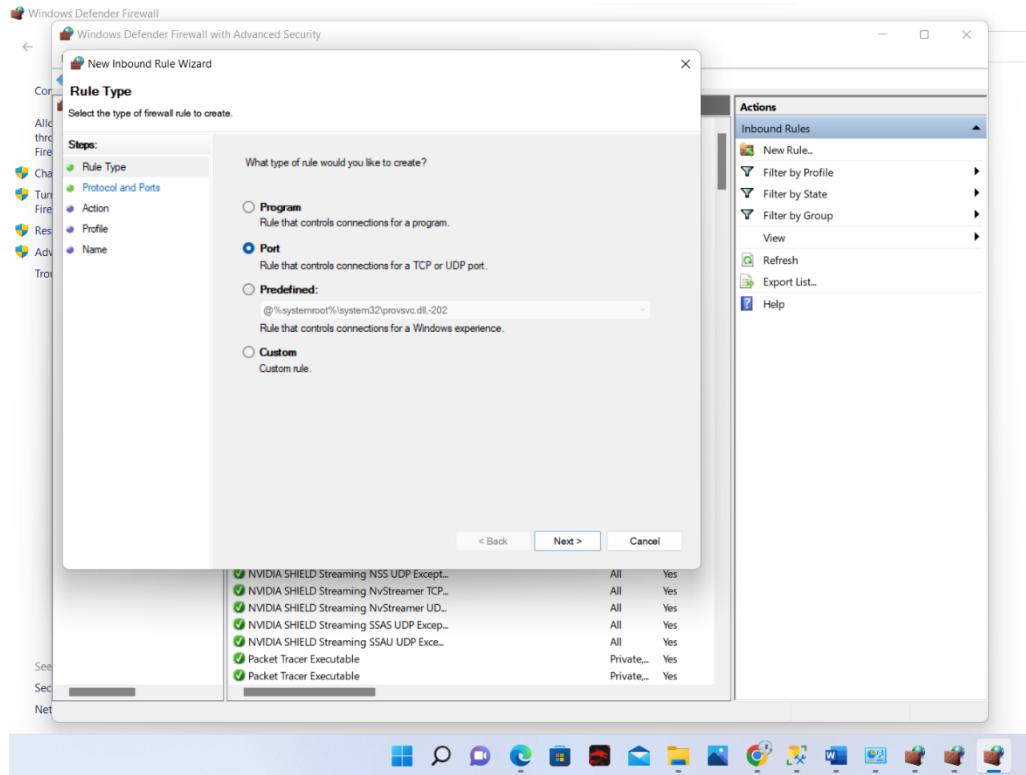
- New inbound rule for program

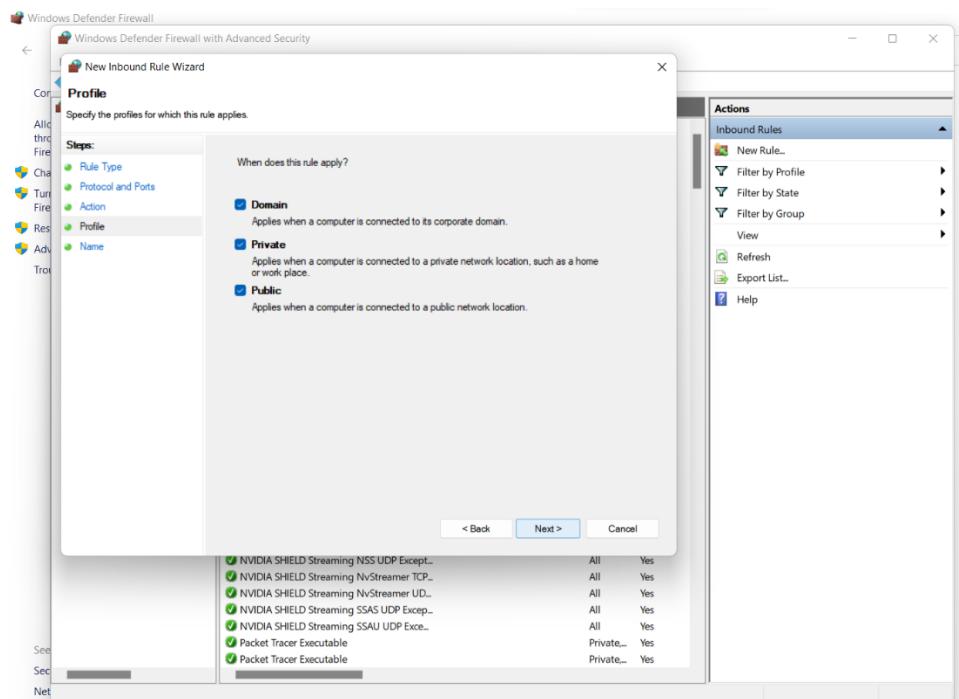
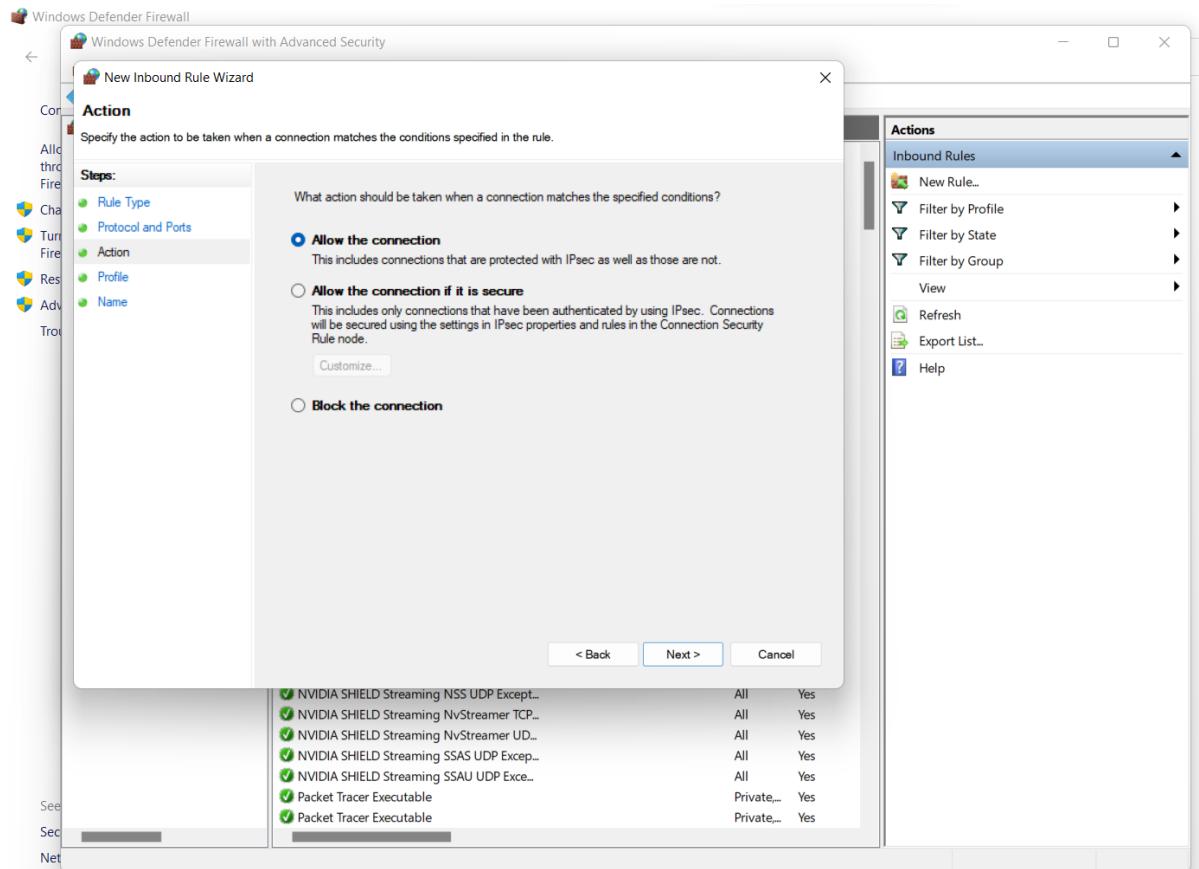


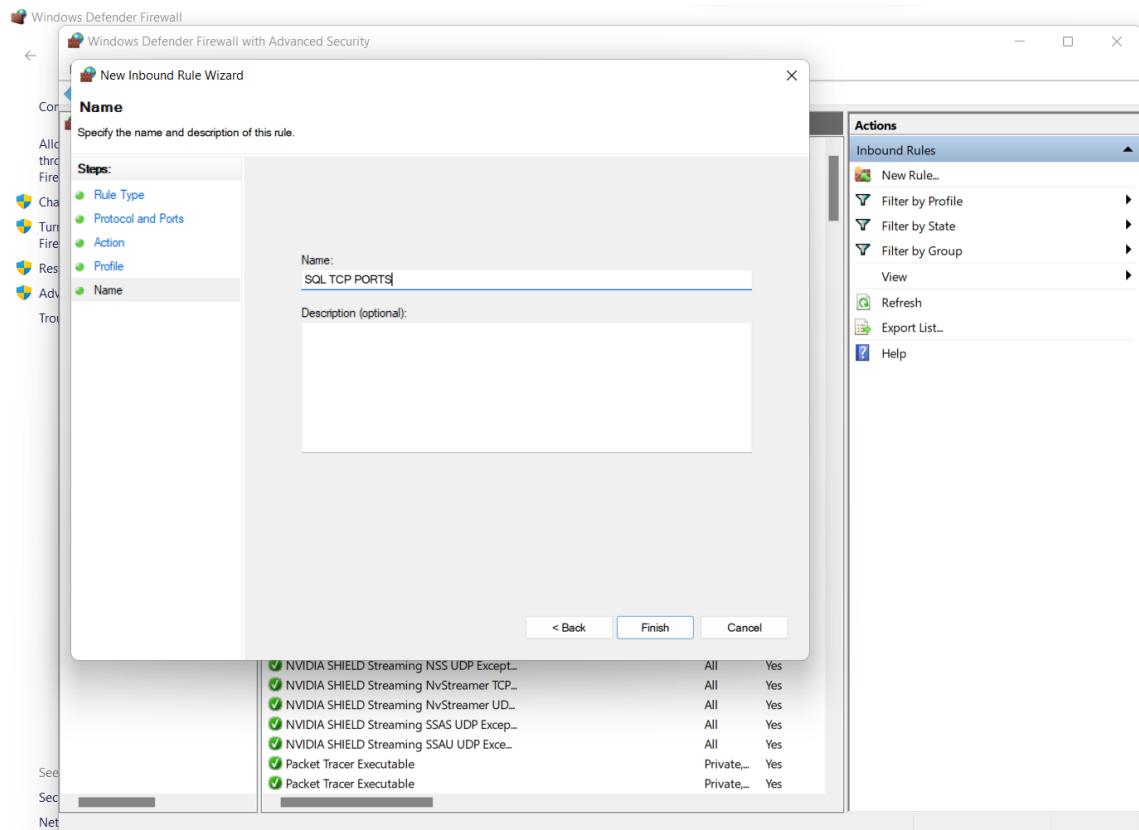




❖ New inbound rule for port security







❖ Run firewall rules in the PowerShell

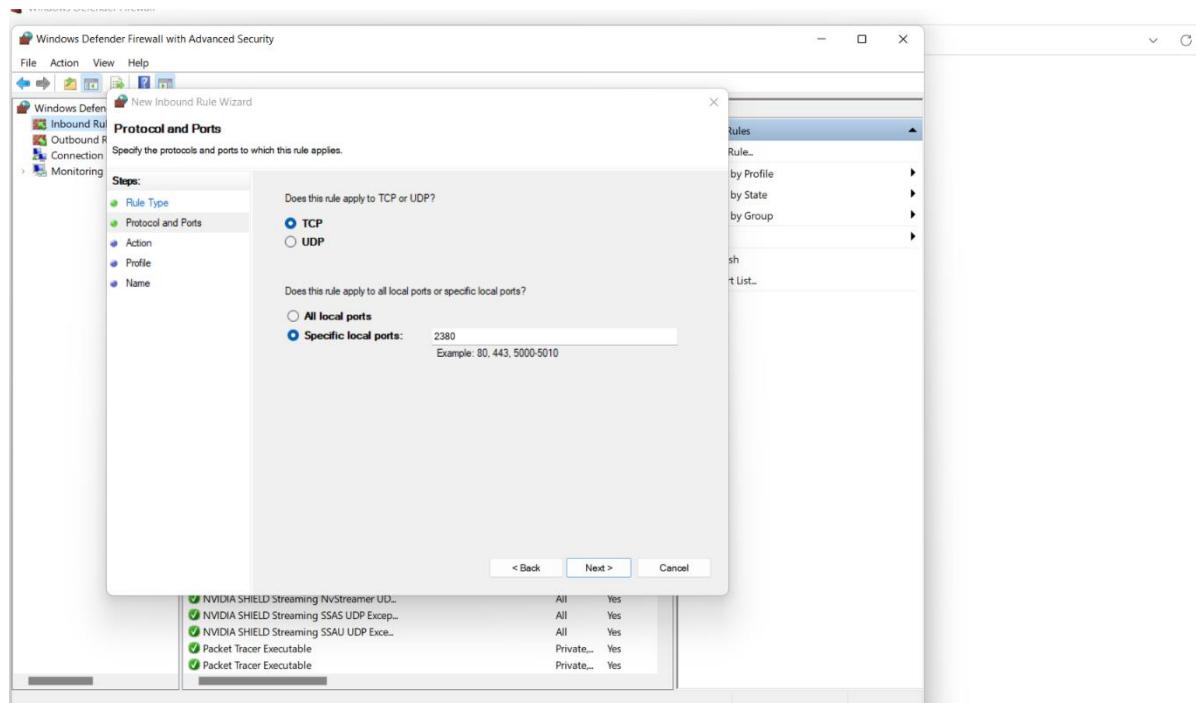
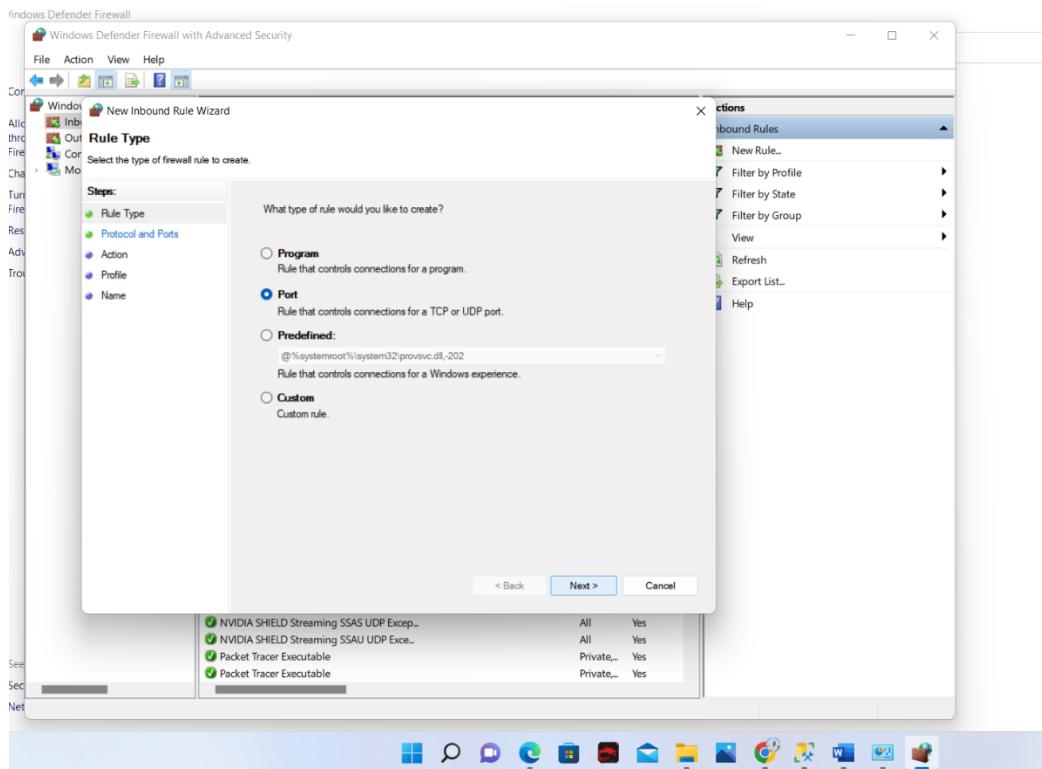
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

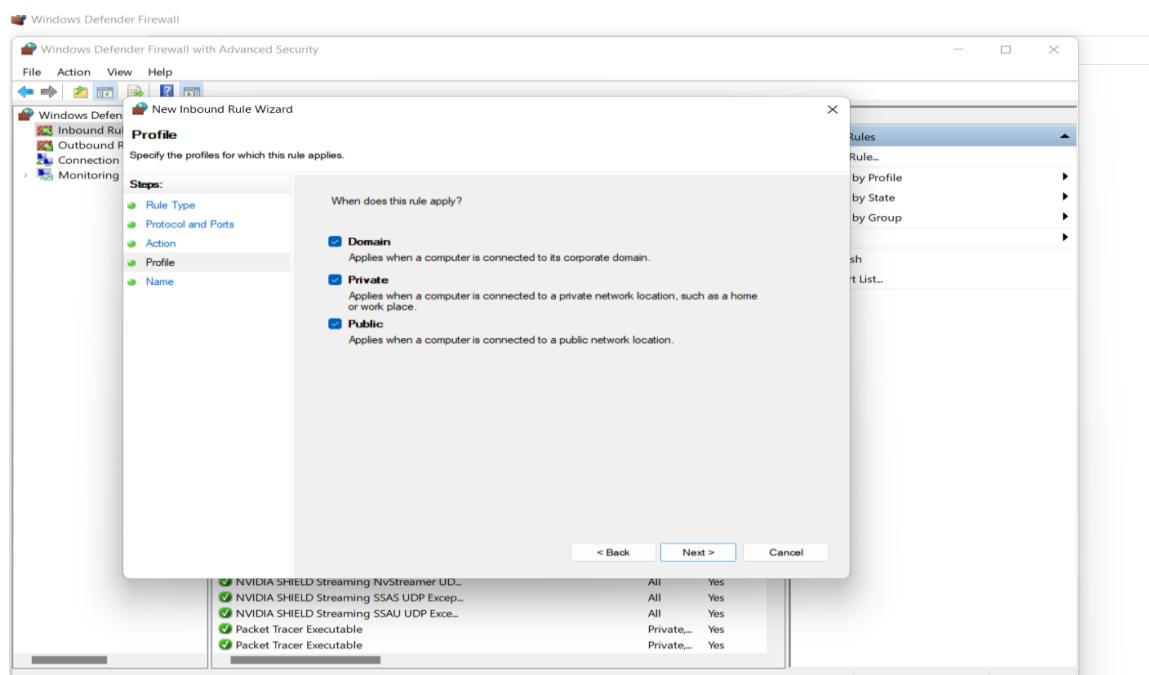
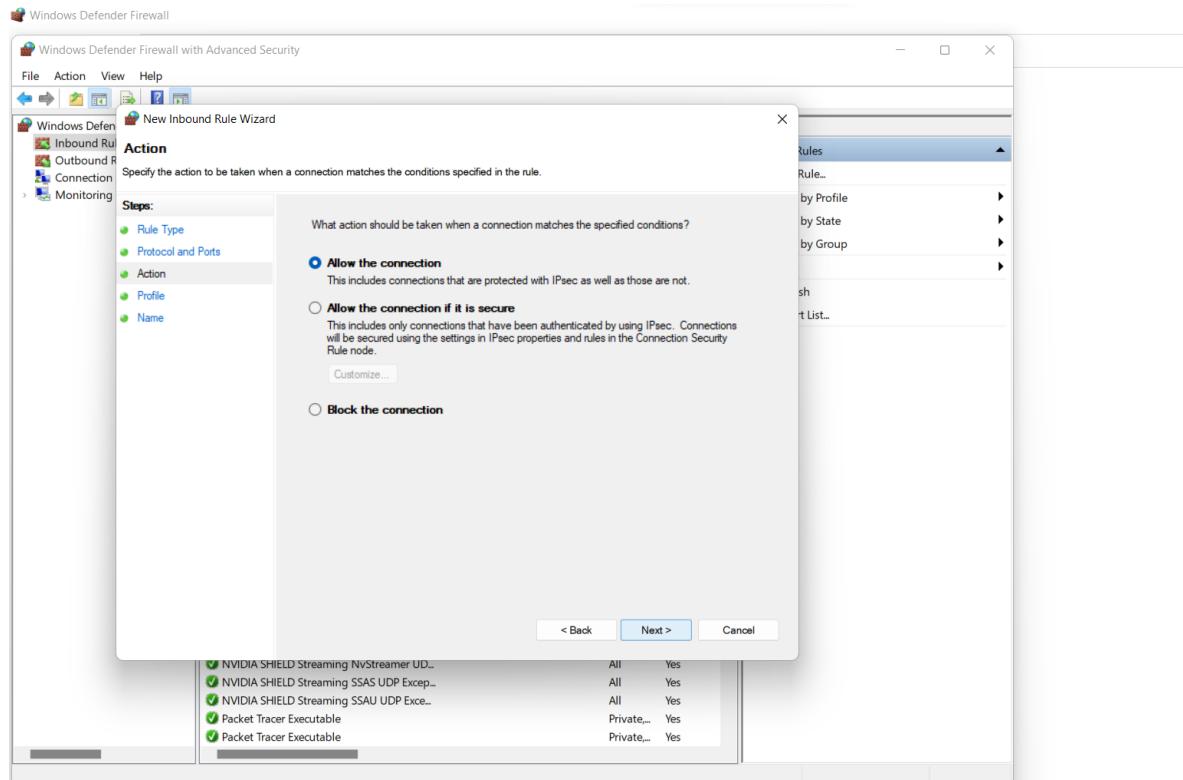
Try the new cross-platform PowerShell https://aka.ms/pscore6

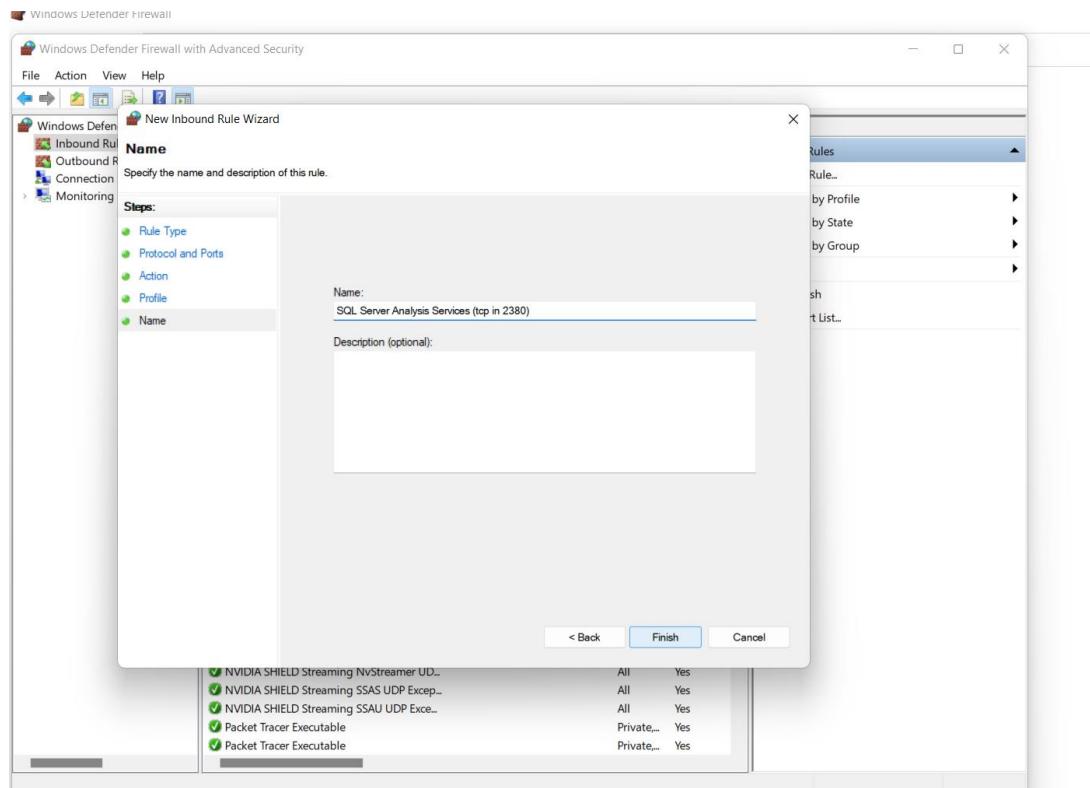
PS C:\WINDOWS\system32> Set-ExecutionPolicy -ExecutionPolicy RemoteSigned
>>> Remoting SQL Server Ports
>>> New-NetFirewallRule -DisplayName "SQL Server" -Direction Inbound -Protocol TCP -LocalPort 1433 -Action allow
>>> New-NetFirewallRule -DisplayName "SQL Admin Connection" -Direction Inbound -Protocol TCP -LocalPort 1434 -Action allow
>>> New-NetFirewallRule -DisplayName "SQL Database Management" -Direction Inbound -Protocol UDP -LocalPort 1434 -Action allow
>>> New-NetFirewallRule -DisplayName "SQL Service Broker" -Direction Inbound -Protocol TCP -LocalPort 4022 -Action allow
>>> New-NetFirewallRule -DisplayName "SQL Debugger/RPC" -Direction Inbound -Protocol TCP -LocalPort 135 -Action allow
>>> Remoting SQL Analysis Ports
>>> New-NetFirewallRule -DisplayName "SQL Analysis Services" -Direction Inbound -Protocol TCP -LocalPort 2383 -Action allow
>>> New-NetFirewallRule -DisplayName "SQL Browser" -Direction Inbound -Protocol TCP -LocalPort 2382 -Action allow
>>> Remoting Misc. Applications
>>> New-NetFirewallRule -DisplayName "HTTP" -Direction Inbound -Protocol TCP -LocalPort 80 -Action allow
>>> New-NetFirewallRule -DisplayName "SSL" -Direction Inbound -Protocol TCP -LocalPort 443 -Action allow
>>> New-NetFirewallRule -DisplayName "SQL Server Browser Service" -Direction Inbound -Protocol UDP -LocalPort 1433 -Action allow
>>> Remoting Windows Firewall
>>> Set-NetFirewallProfile -DefaultInboundAction Block -DefaultOutboundAction Allow -NotifyOnListen True -AllowUnicastResponsesToMulticast True

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose you to the security risks described in the about_Execution_Policies help topic at https://go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
(Y) Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): A
Set-ExecutionPolicy : Windows PowerShell updated your execution policy successfully, but the setting is overridden by a policy defined at a more specific scope. Due to the override, your shell will retain its current effective execution policy of Unrestricted. Type 'Get-ExecutionPolicy -List' to view your execution policy settings. For more information please see 'Get-Help Set-ExecutionPolicy'.
At line:1 char:1
+ Set-ExecutionPolicy -ExecutionPolicy RemoteSigned
+
+ CategoryInfo          : PermissionDenied: (:) [Set-ExecutionPolicy], SecurityException
+ FullyQualifiedErrorId : ExecutionPolicyOverride,Microsoft.PowerShell.Commands.SetExecutionPolicyCommand
```

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







- ❖ Enable the notifications when rule is modified in the firewall

Windows Defender Firewall with Advanced Security on Local Computer

Domain Profile **Private Profile** **Public Profile** **IPsec Settings**

Specify behavior for when a computer is connected to its corporate domain.

State

- Firewall state: **On (recommended)**
- Inbound connections: **Block (default)**
- Outbound connections: **Allow (default)**
- Protected network connections: **Customize...**

Settings

- Specify settings that control Windows Defender Firewall behavior. **Customize...**

Logging

- Specify logging settings for troubleshooting. **Customize...**

OK **Cancel** **Apply**

Customize Settings for the Domain Profile

Specify settings that control Windows Defender Firewall with Advanced Security behavior.

Firewall settings

Display notifications to the user when a program is blocked from receiving inbound connections.

Display a notification: **Yes**

Unicast response

Allow unicast response to multicast or broadcast network traffic.

Allow unicast response: **Yes (default)**

Rule merging

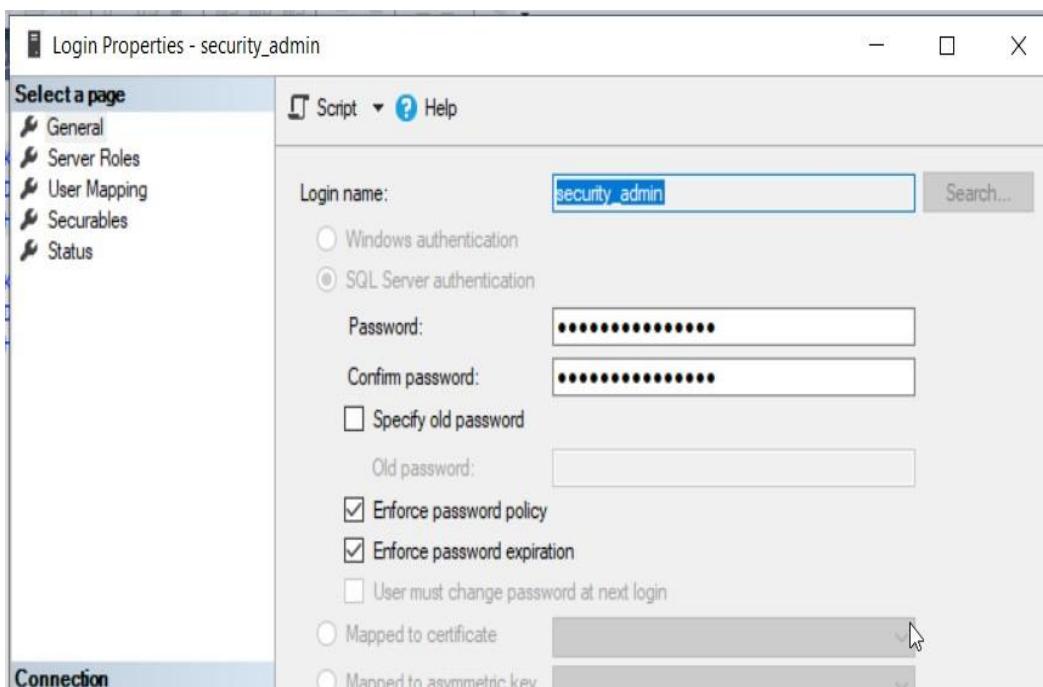
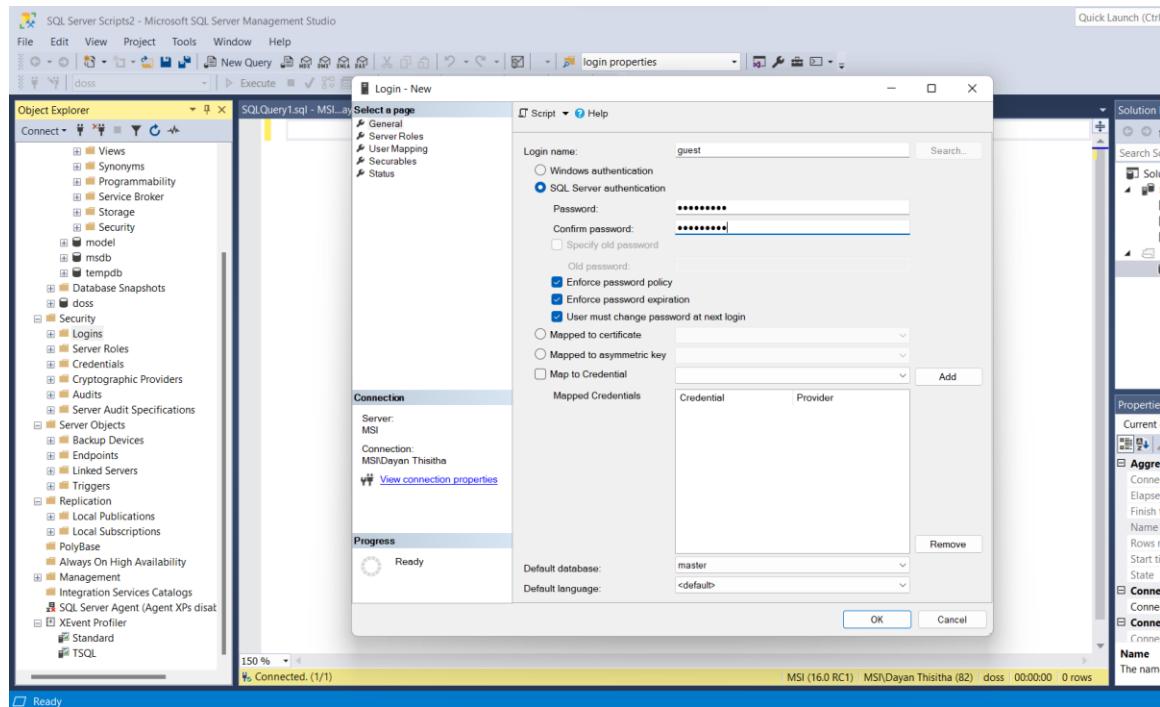
Allows rules created by local administrators to be merged with rules distributed through Group Policy. This setting can only be applied by using Group Policy.

Apply local firewall rules: **Yes (default)**

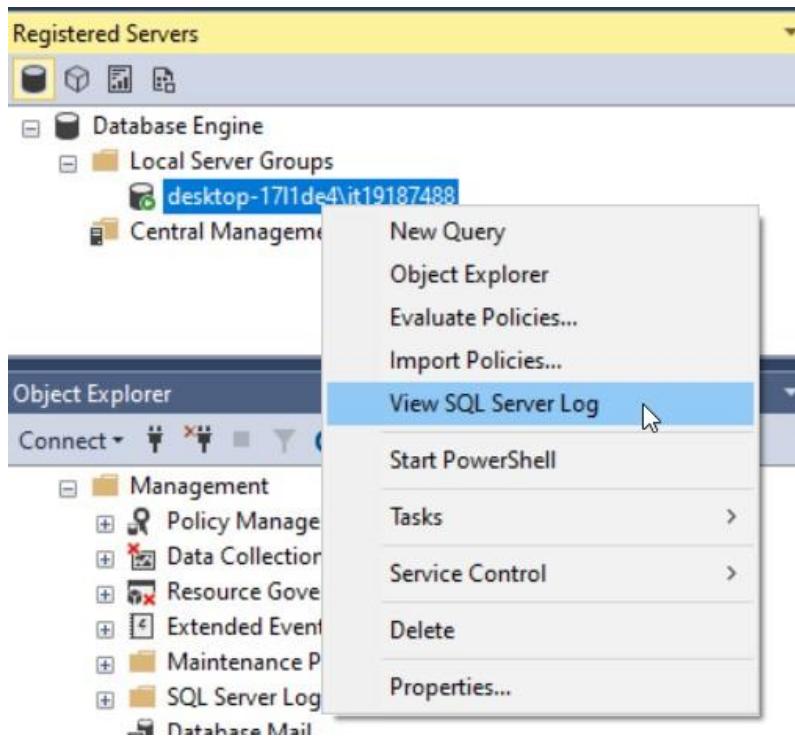
Apply local connection security rules: **Yes (default)**

OK **Cancel**

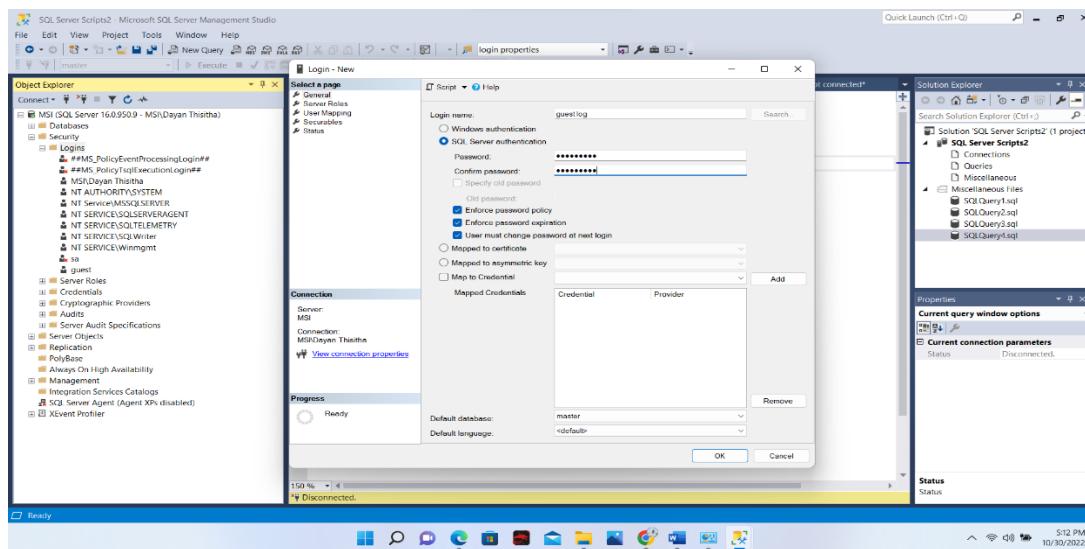
❖ **Database Software (All Unnecessary functions and accounts are removed, default passwords are changed)**

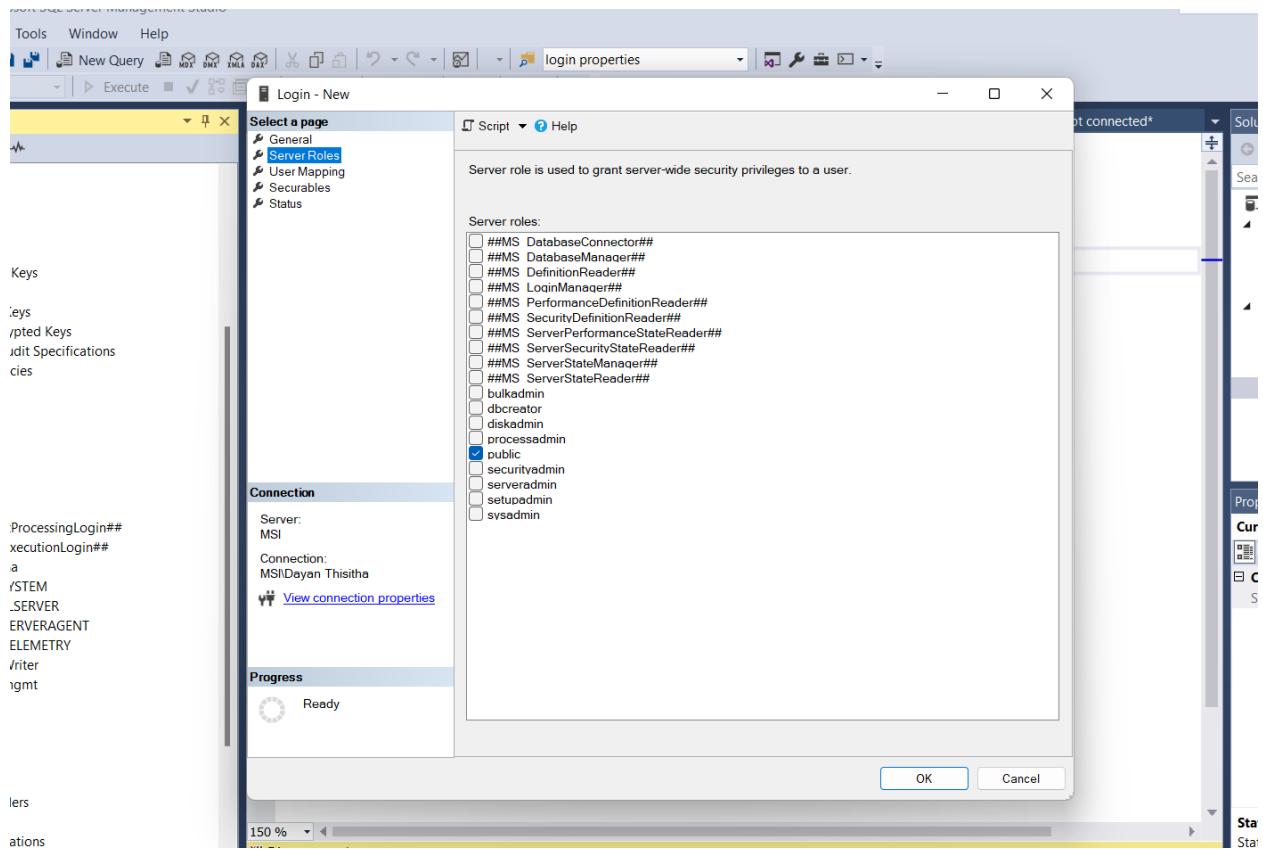


- ❖ Maintain the log records of accessing to the database and maintain the minimum access privileges to the servers and applications.



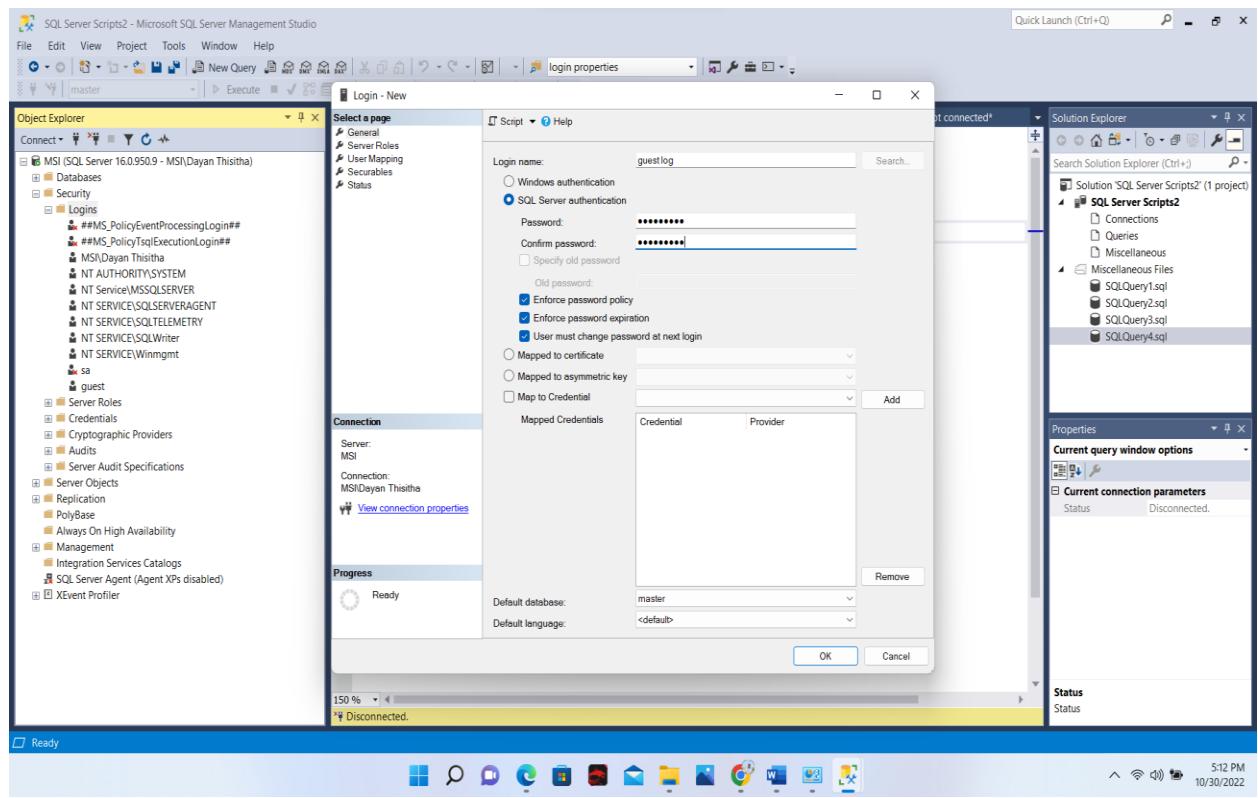
- ❖ Maintain individual login credentials for the people who access the workstation and to perform administrative tasks of the database.

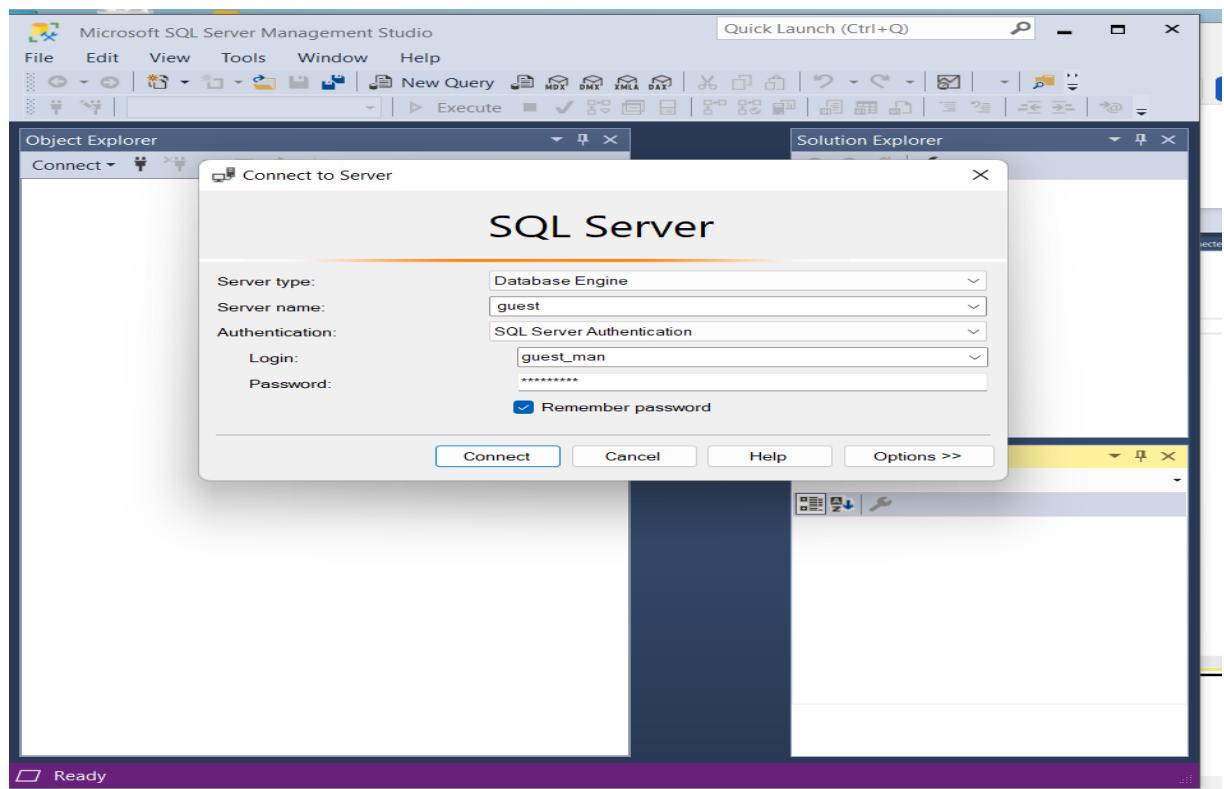
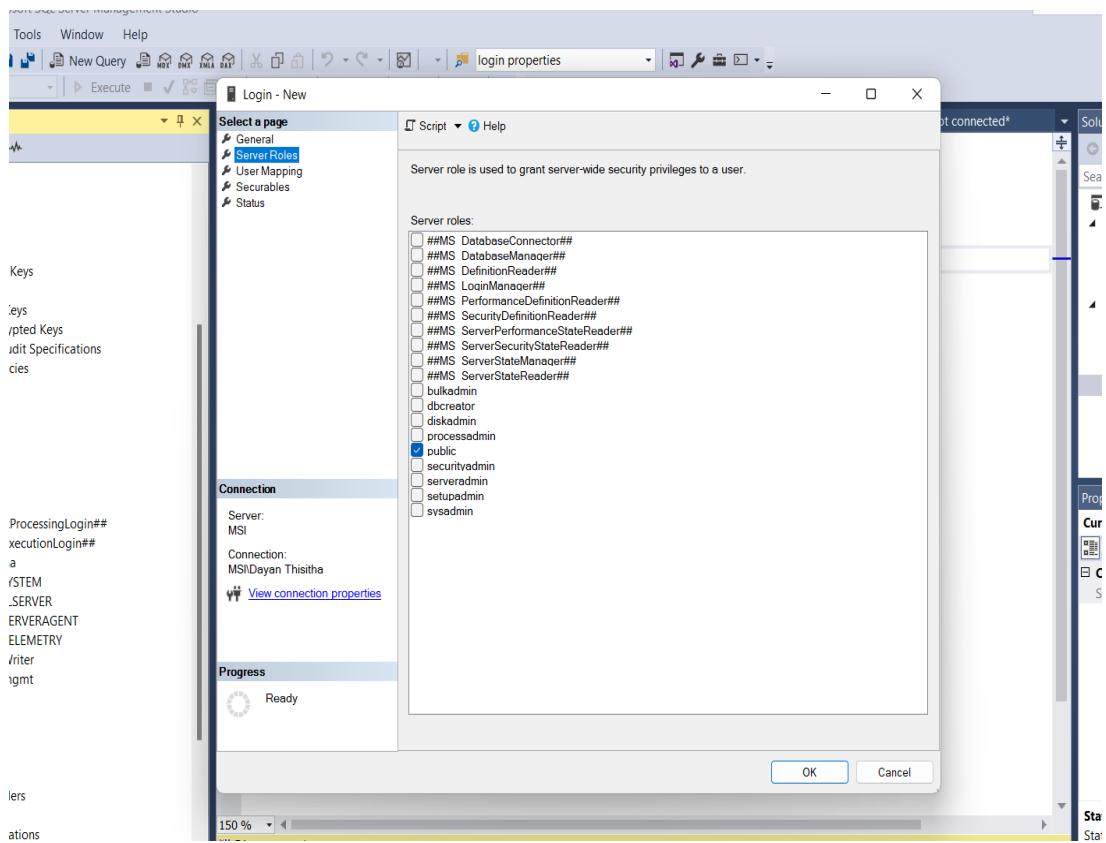


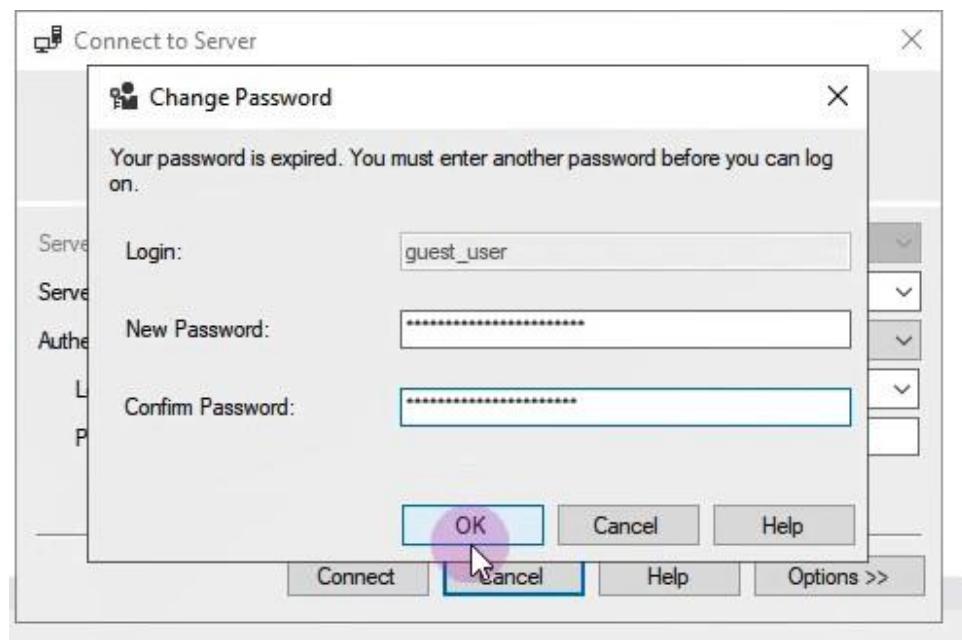




❖ Create login for guest user and testing login

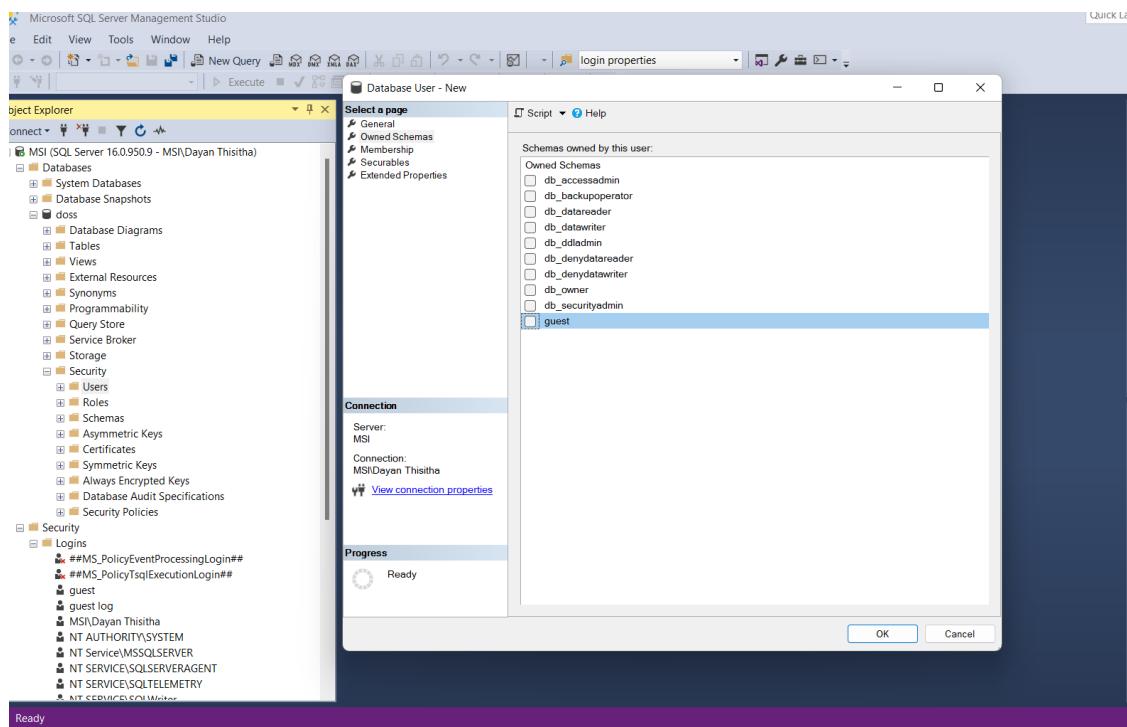
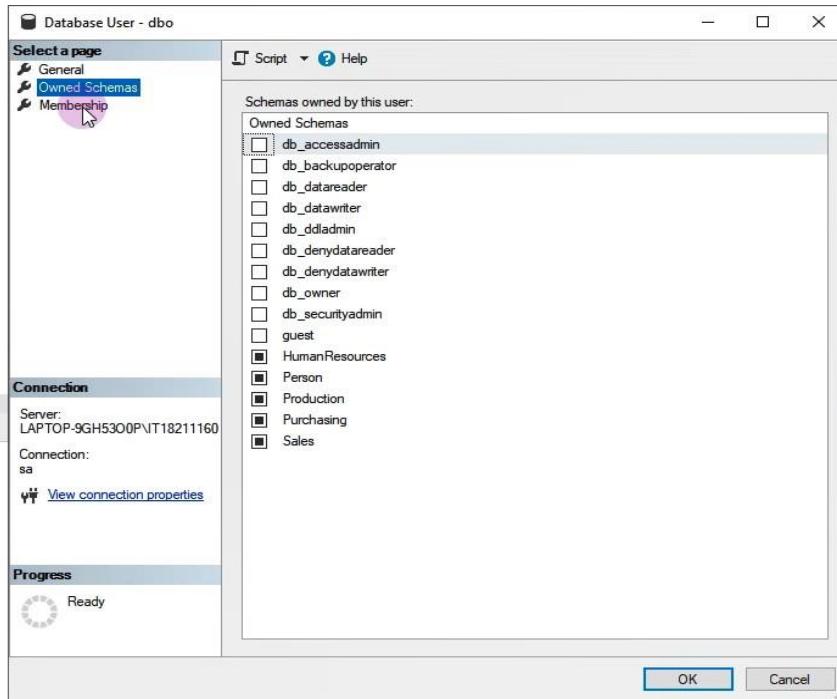




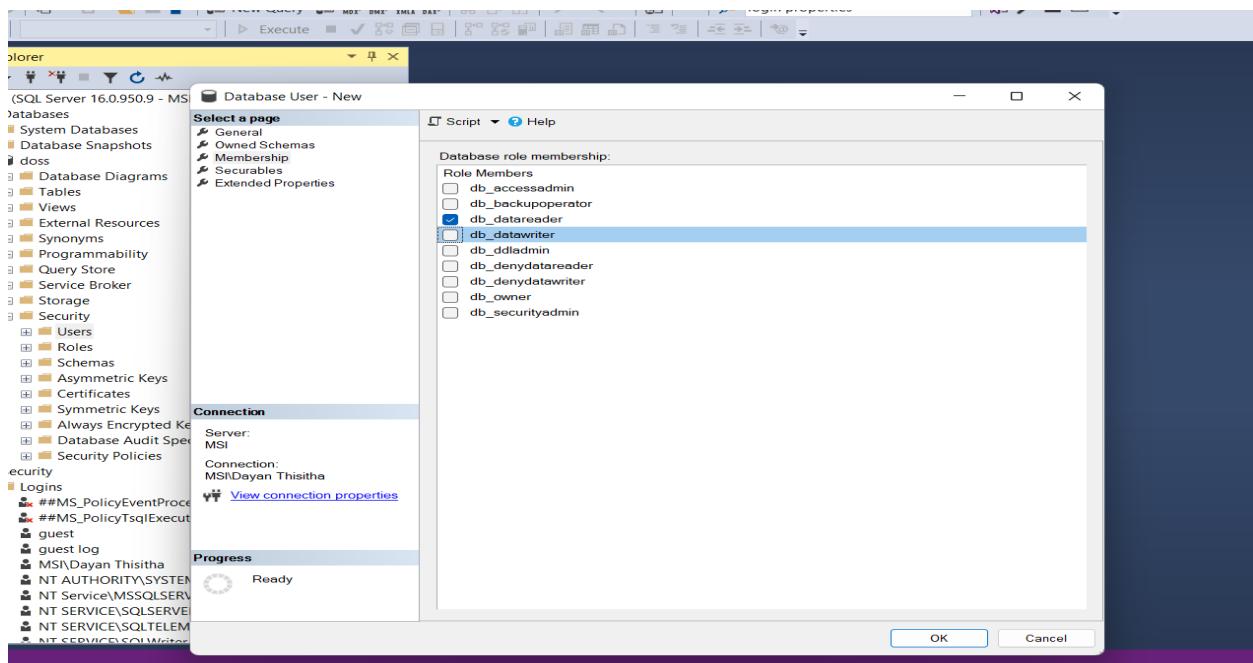
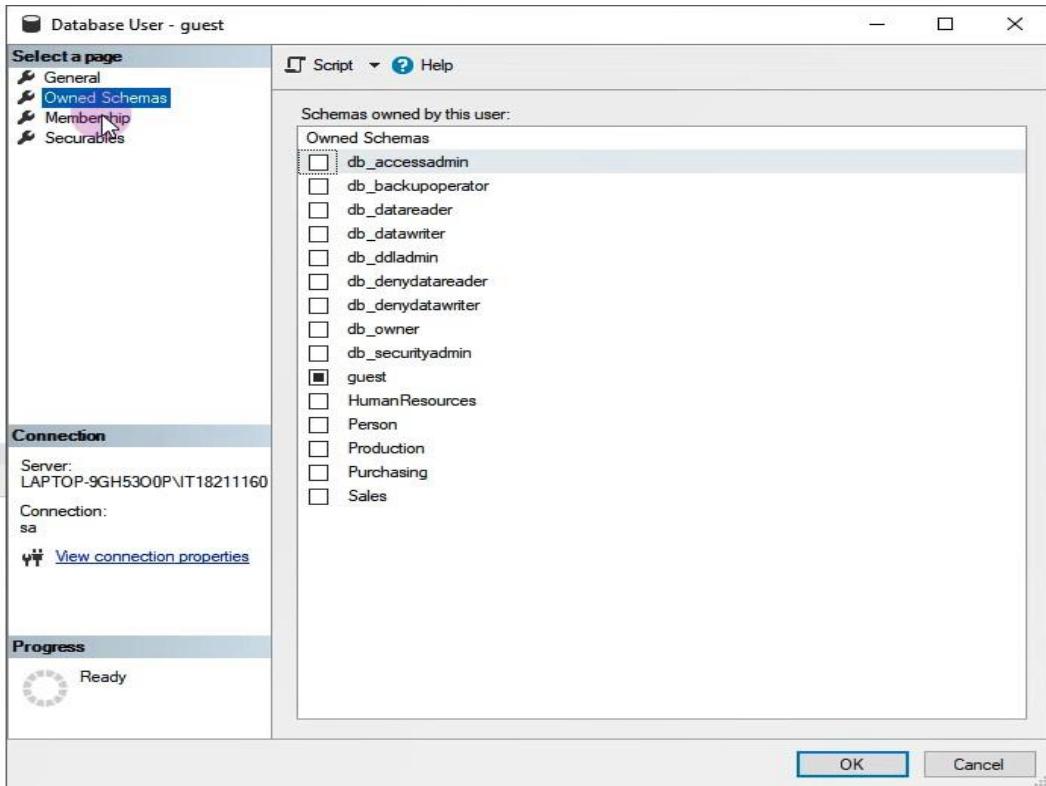


- ❖ Grant minimal permissions that necessary for the people according to their job role in the database.

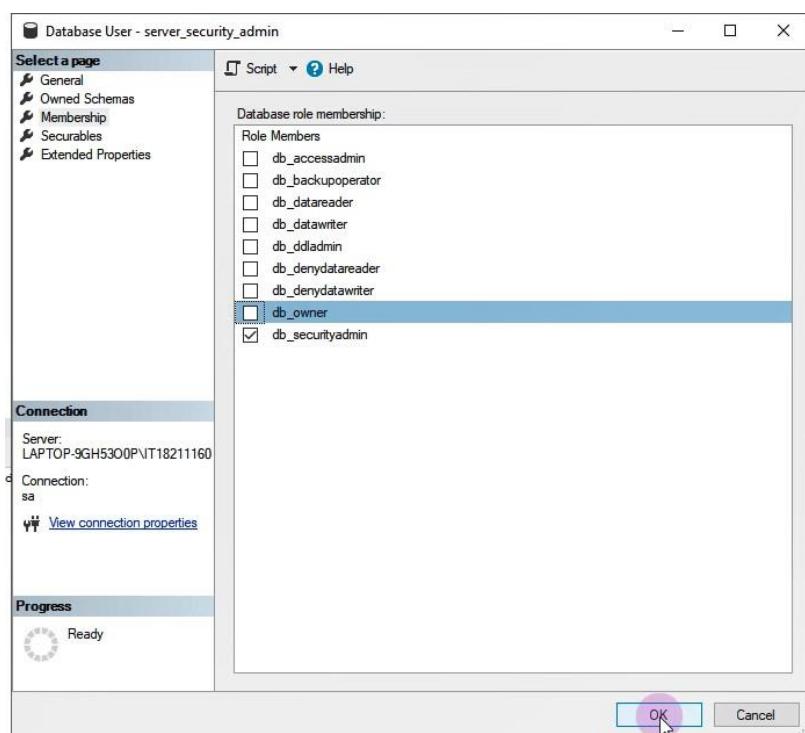
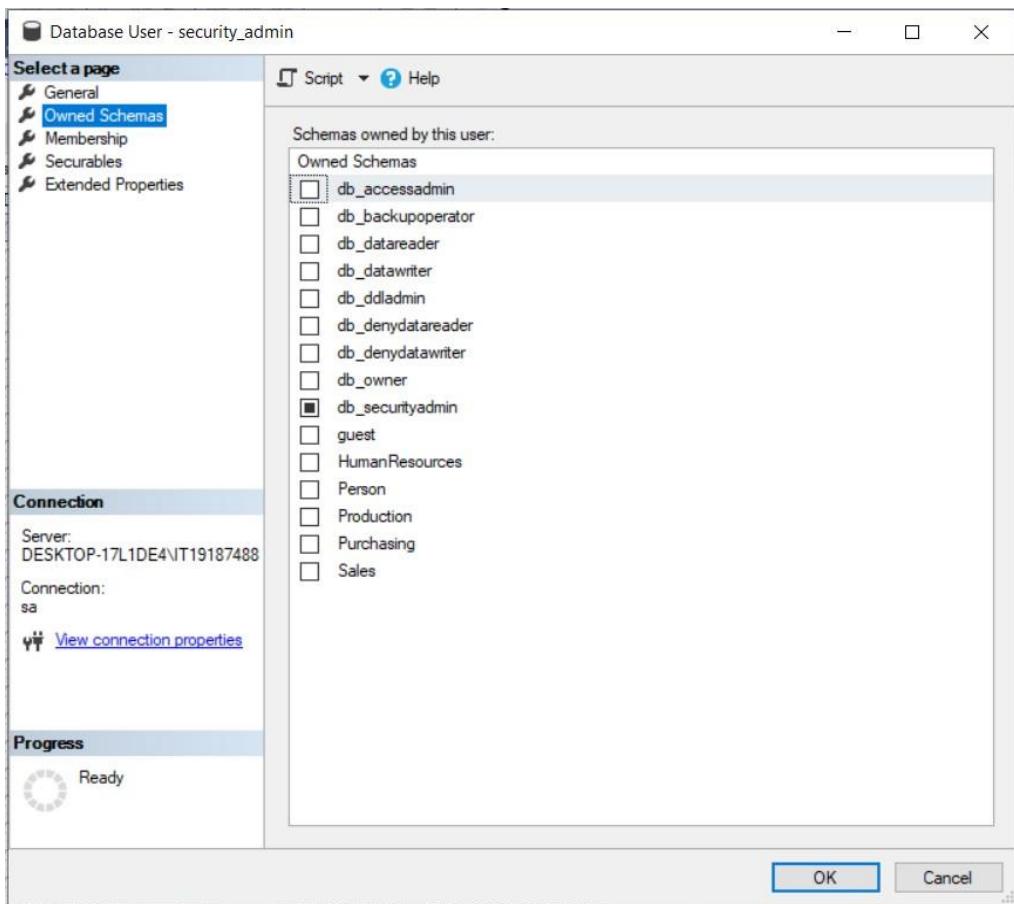
- ❖ Database Owner(dbo)



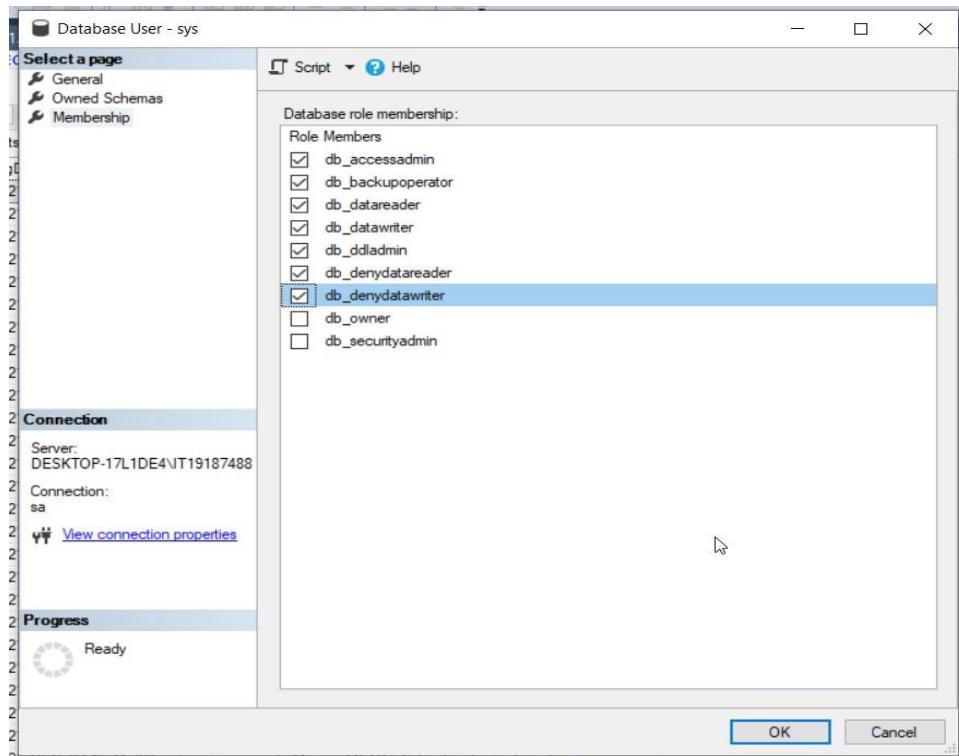
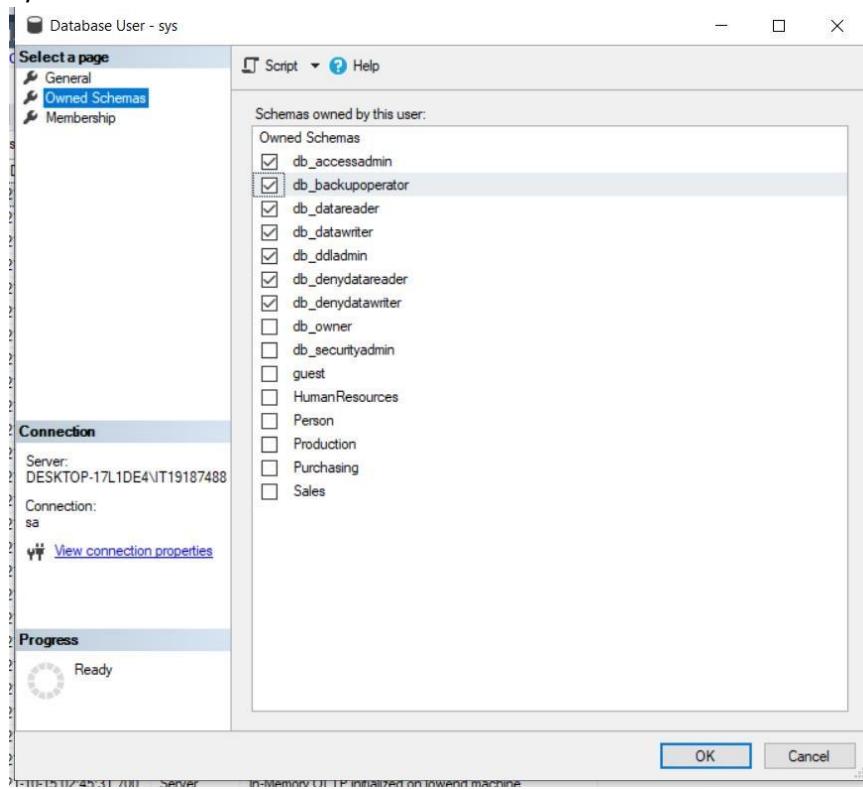
❖ Guest user



❖ Server security admin



❖ Sys



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

The screenshot shows two separate SQL query windows in SQL Server Management Studio.

Top Window (SQLQuery6.sql - MSI...ayan Thisitha (61)):

```
CREATE ROLE hr;
GRANT connect TO hr;
GRANT create table to hr;
GRANT select to hr;
EXEC sp_addrolemember 'hr' , 'user1'
```

Messages pane:

```
Commands completed successfully.
```

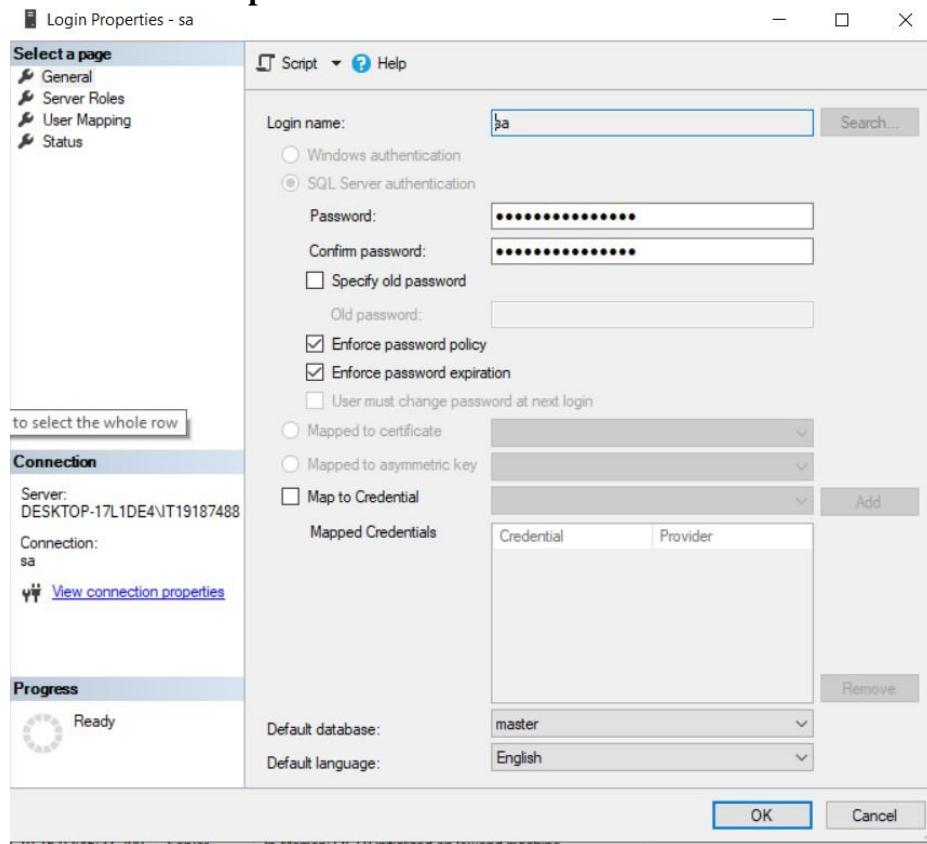
Bottom Window (SQLQuery1.sql - MSI...ayan Thisitha (71)):

```
CREATE TABLE table1
( emp_id INT NOT NULL,
last_name VARCHAR(50) NOT NULL,
first_name VARCHAR(50),
PRIMARY KEY(em_id)
);
```

Messages pane:

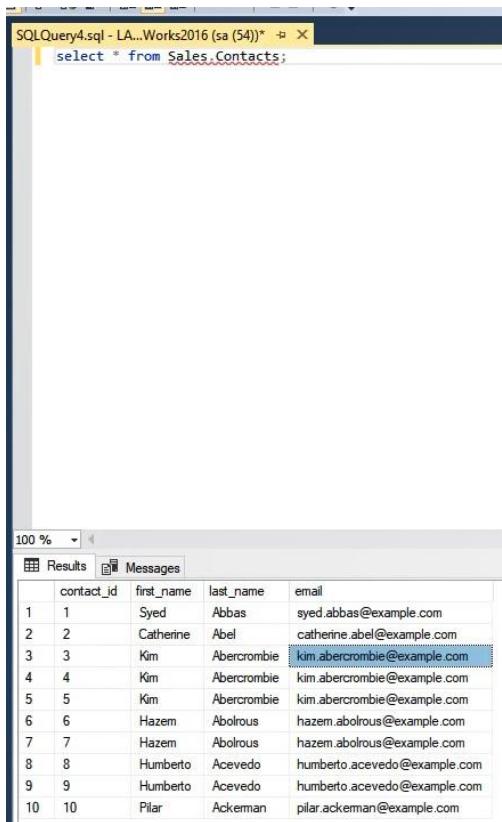
```
Commands completed successfully.
```

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



- Prevent from redundancy of the stored records of the database

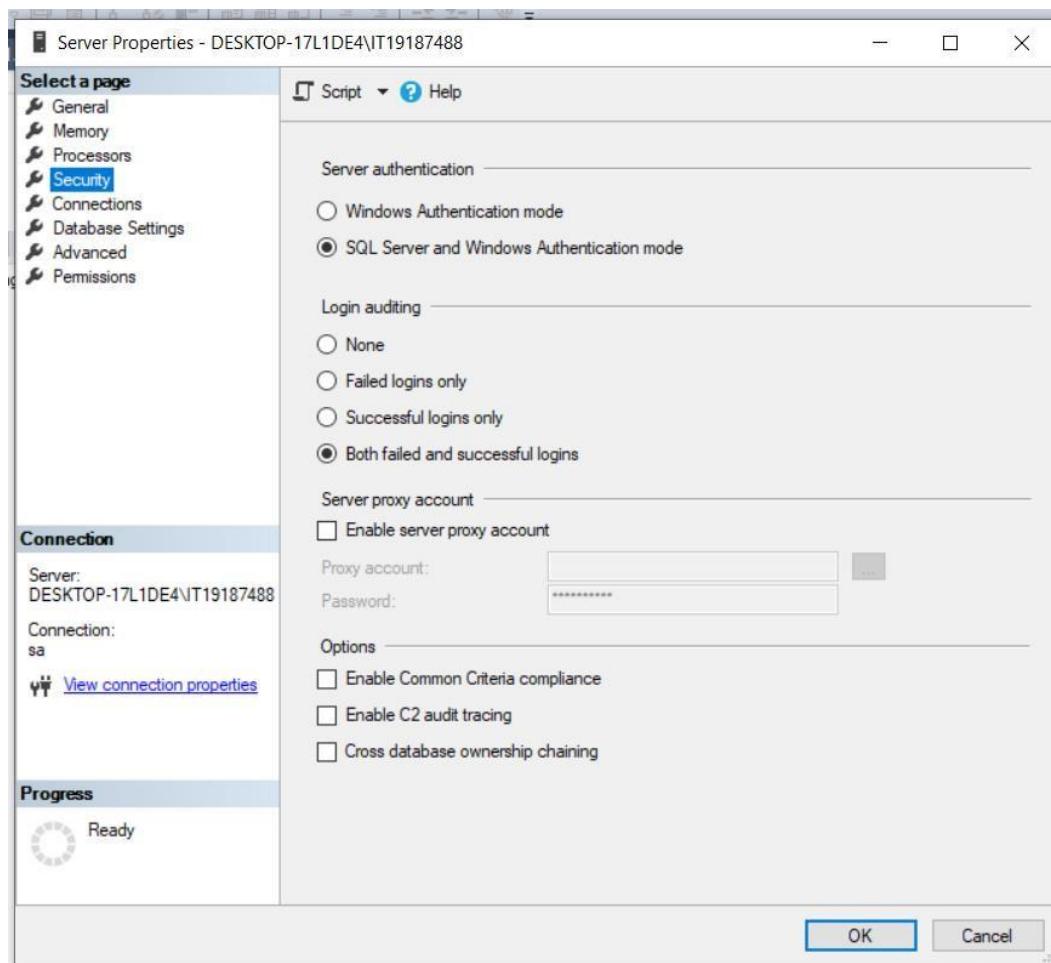
Sales.Contacts redundancy check



The screenshot shows a SQL Server Management Studio window titled "SQLQuery4.sql - LA...Works2016 (sa (54))". The query "select * from Sales.Contacts;" is run, and the results are displayed in a table. The table has columns: contact_id, first_name, last_name, and email. The data shows 10 rows of contacts, with the third row highlighted.

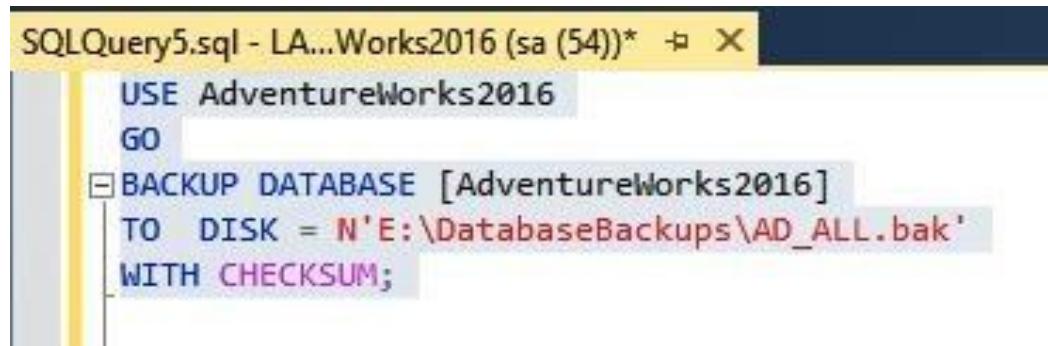
	contact_id	first_name	last_name	email
1	1	Syed	Abbas	syed.abbas@example.com
2	2	Catherine	Abel	catherine.abel@example.com
3	3	Kim	Abercrombie	kim.abercrombie@example.com
4	4	Kim	Abercrombie	kim.abercrombie@example.com
5	5	Kim	Abercrombie	kim.abercrombie@example.com
6	6	Hazem	Abolrous	hazem.abolrous@example.com
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.

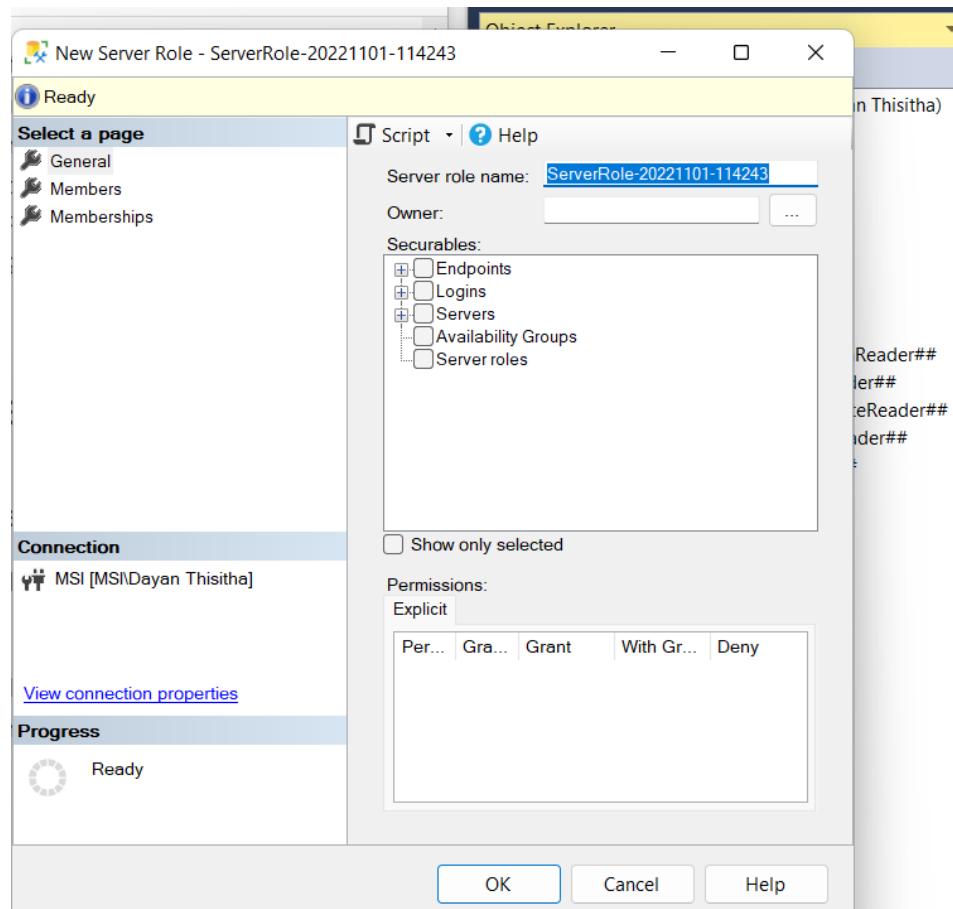


- Discuss how manage the implemented database backup and recovery.

➤ 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

