SECURE SYSTEMS ENGINEERING

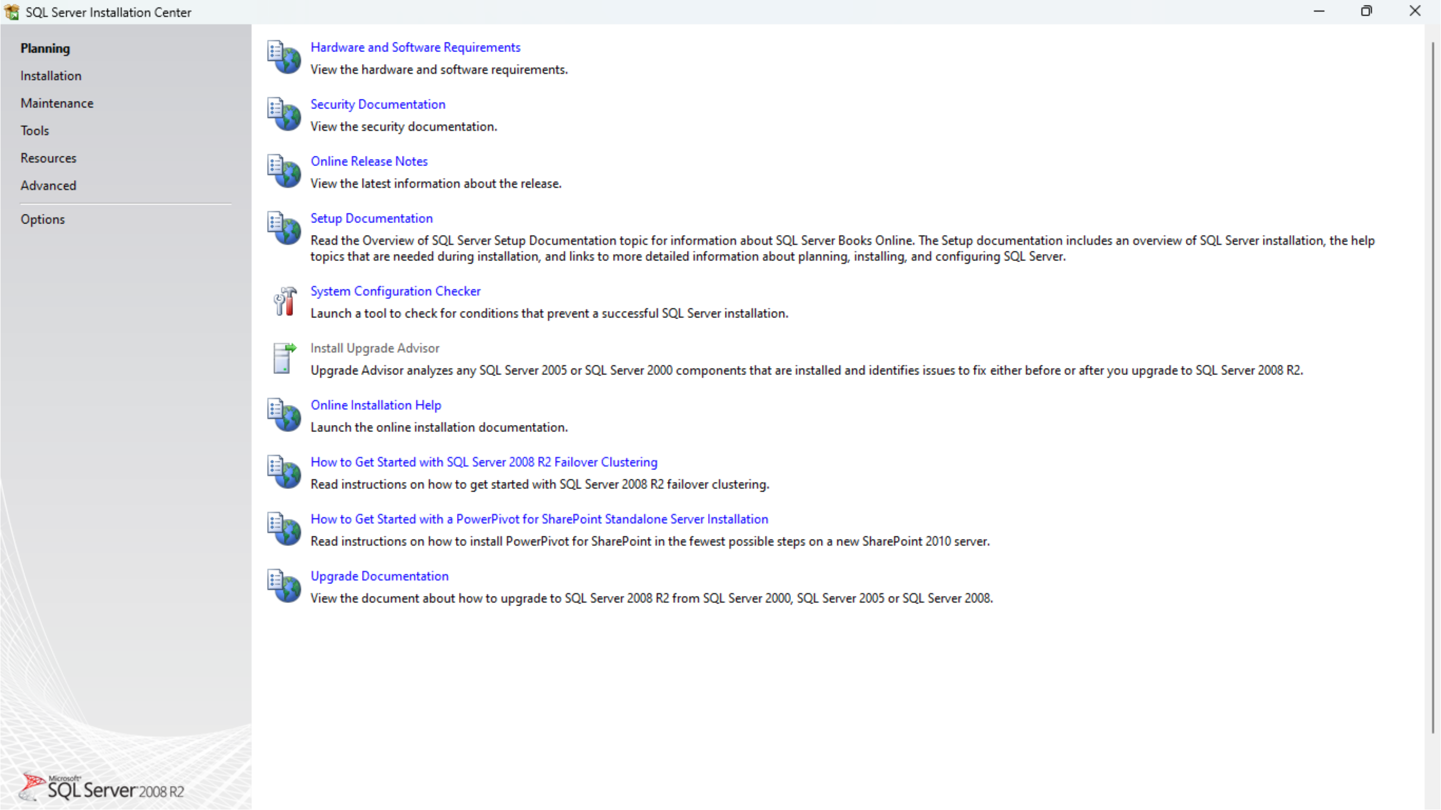
Assignment – 2

(DVTA)

V NANDITHA
CB.SC.P2CYS23018

(2nd Year / 3rd Sem- MTech, CYBERSECURITY)

DVTA SET-UP



Hardware and Software Requirements
View the hardware and software requirements.

Security Documentation
View the security documentation.

Online Release Notes
View the latest information about the release.

Setup Documentation
Read the Overview of SQL Server Setup Documentation topic for information about SQL Server Books Online. The Setup documentation includes an overview of SQL Server installation, the help topics that are needed during installation, and links to more detailed information about planning, installing, and configuring SQL Server.

System Configuration Checker
Launch a tool to check for conditions that prevent a successful SQL Server installation.

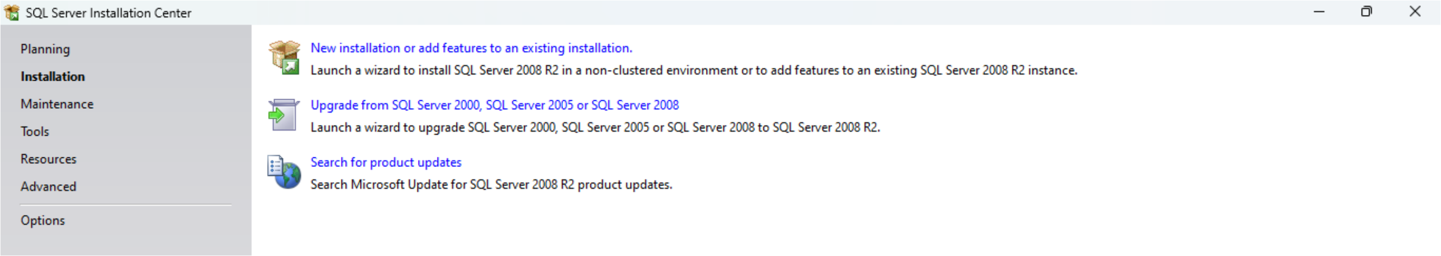
Install Upgrade Advisor
Upgrade Advisor analyzes any SQL Server 2005 or SQL Server 2000 components that are installed and identifies issues to fix either before or after you upgrade to SQL Server 2008 R2.

Online Installation Help
Launch the online installation documentation.

How to Get Started with SQL Server 2008 R2 Failover Clustering
Read instructions on how to get started with SQL Server 2008 R2 failover clustering.

How to Get Started with a PowerPivot for SharePoint Standalone Server Installation
Read instructions on how to install PowerPivot for SharePoint in the fewest possible steps on a new SharePoint 2010 server.

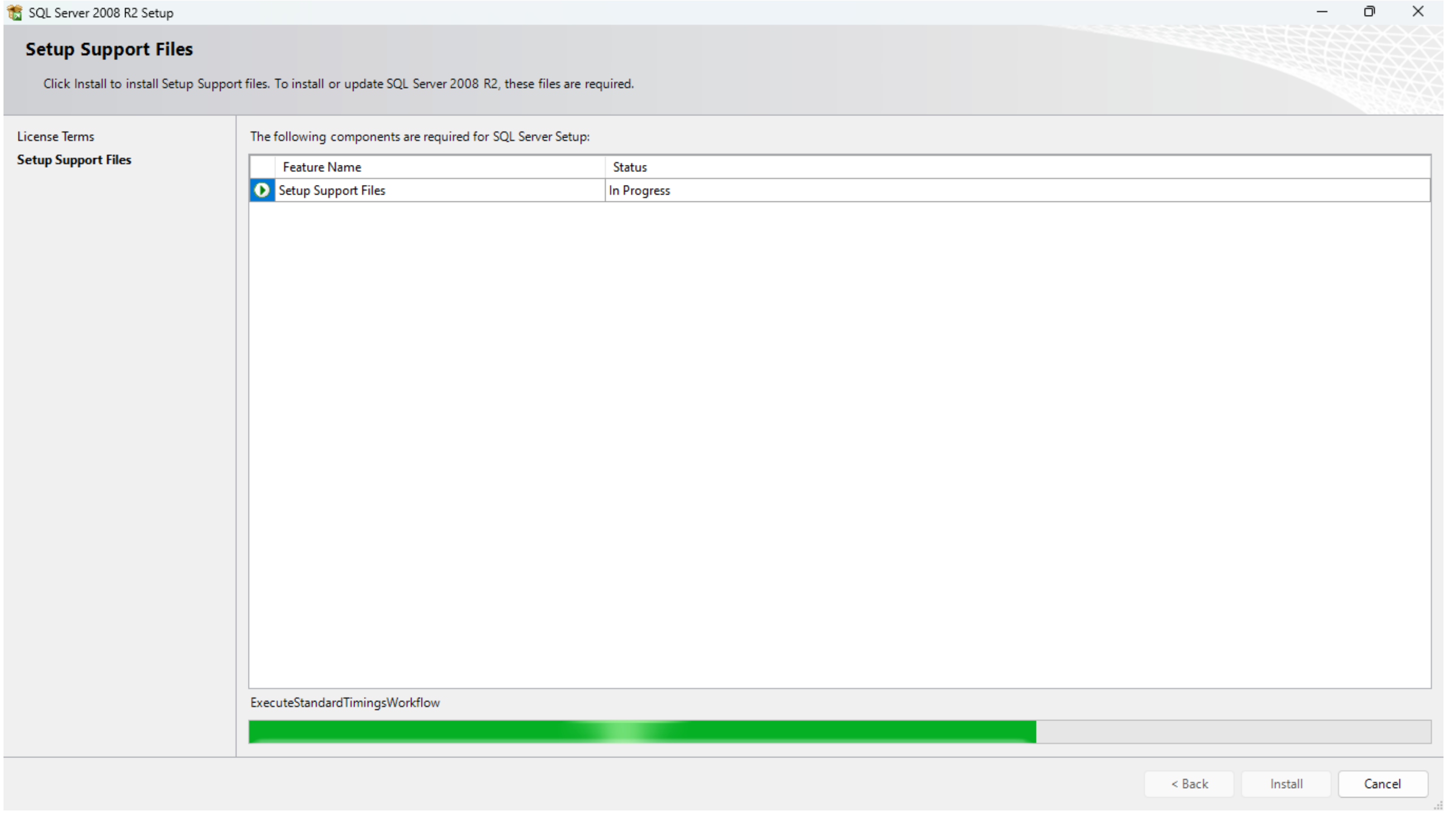
Upgrade Documentation
View the document about how to upgrade to SQL Server 2008 R2 from SQL Server 2000, SQL Server 2005 or SQL Server 2008.



New installation or add features to an existing installation.
Launch a wizard to install SQL Server 2008 R2 in a non-clustered environment or to add features to an existing SQL Server 2008 R2 instance.

Upgrade from SQL Server 2000, SQL Server 2005 or SQL Server 2008
Launch a wizard to upgrade SQL Server 2000, SQL Server 2005 or SQL Server 2008 to SQL Server 2008 R2.

Search for product updates
Search Microsoft Update for SQL Server 2008 R2 product updates.


SQL Server 2008 R2 Setup

Setup Support Files

Click Install to install Setup Support files. To install or update SQL Server 2008 R2, these files are required.

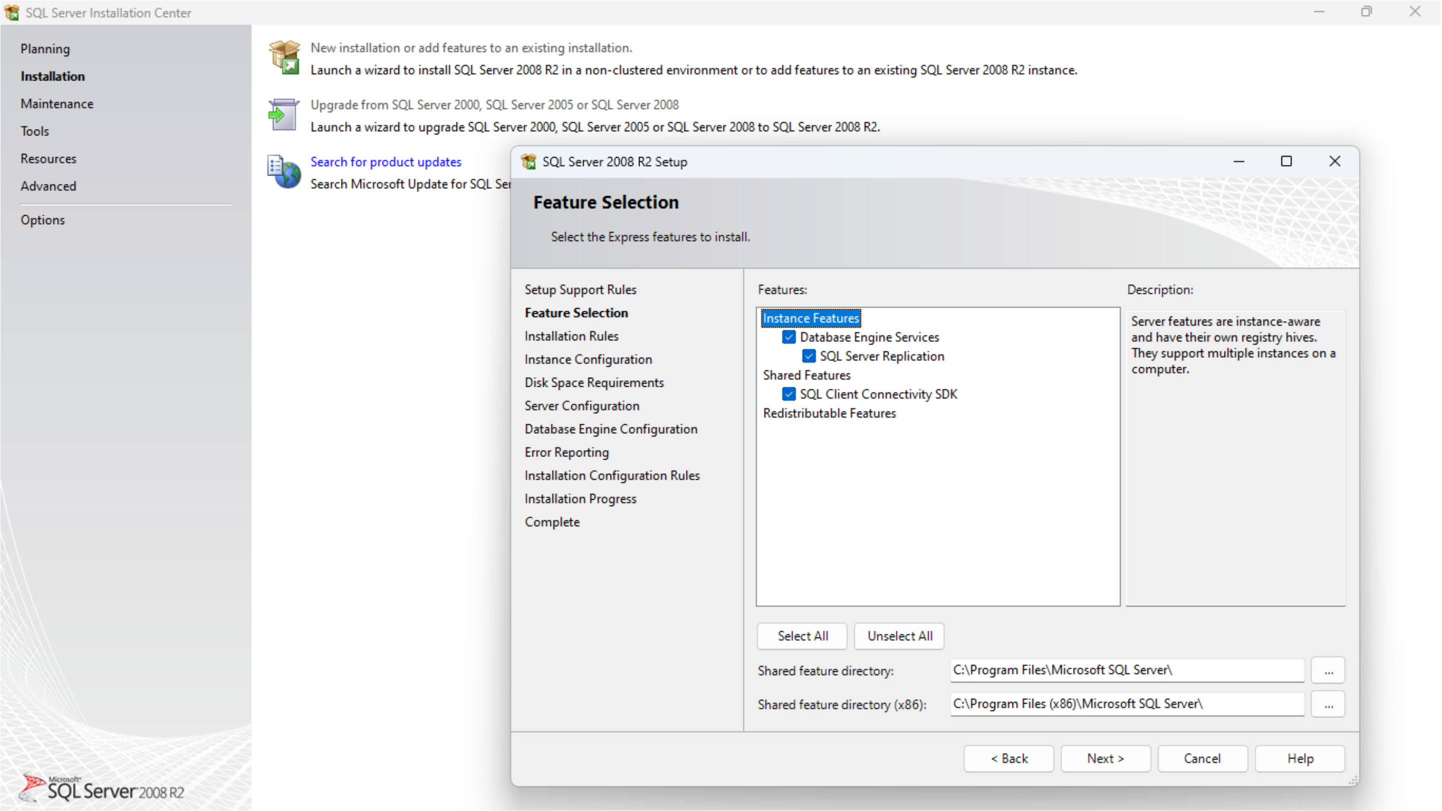
License Terms

Setup Support Files

The following components are required for SQL Server Setup:

Feature Name	Status
Setup Support Files	In Progress

ExecuteStandardTimingsWorkflow


SQL Server Installation Center

Planning

Installation

Maintenance

Tools

Resources

Advanced

Options

New installation or add features to an existing installation.
Launch a wizard to install SQL Server 2008 R2 in a non-clustered environment or to add features to an existing SQL Server 2008 R2 instance.

Upgrade from SQL Server 2000, SQL Server 2005 or SQL Server 2008
Launch a wizard to upgrade SQL Server 2000, SQL Server 2005 or SQL Server 2008 to SQL Server 2008 R2.

Search for product updates
Search Microsoft Update for SQL Se

SQL Server 2008 R2 Setup

Feature Selection

Select the Express features to install.

Setup Support Rules

Feature Selection

Installation Rules

Instance Configuration

Disk Space Requirements

Server Configuration

Database Engine Configuration

Error Reporting

Installation Configuration Rules

Installation Progress

Complete

Features:

Instance Features
- ☑ Database Engine Services
  - ☑ SQL Server Replication

Shared Features
- ☑ SQL Client Connectivity SDK

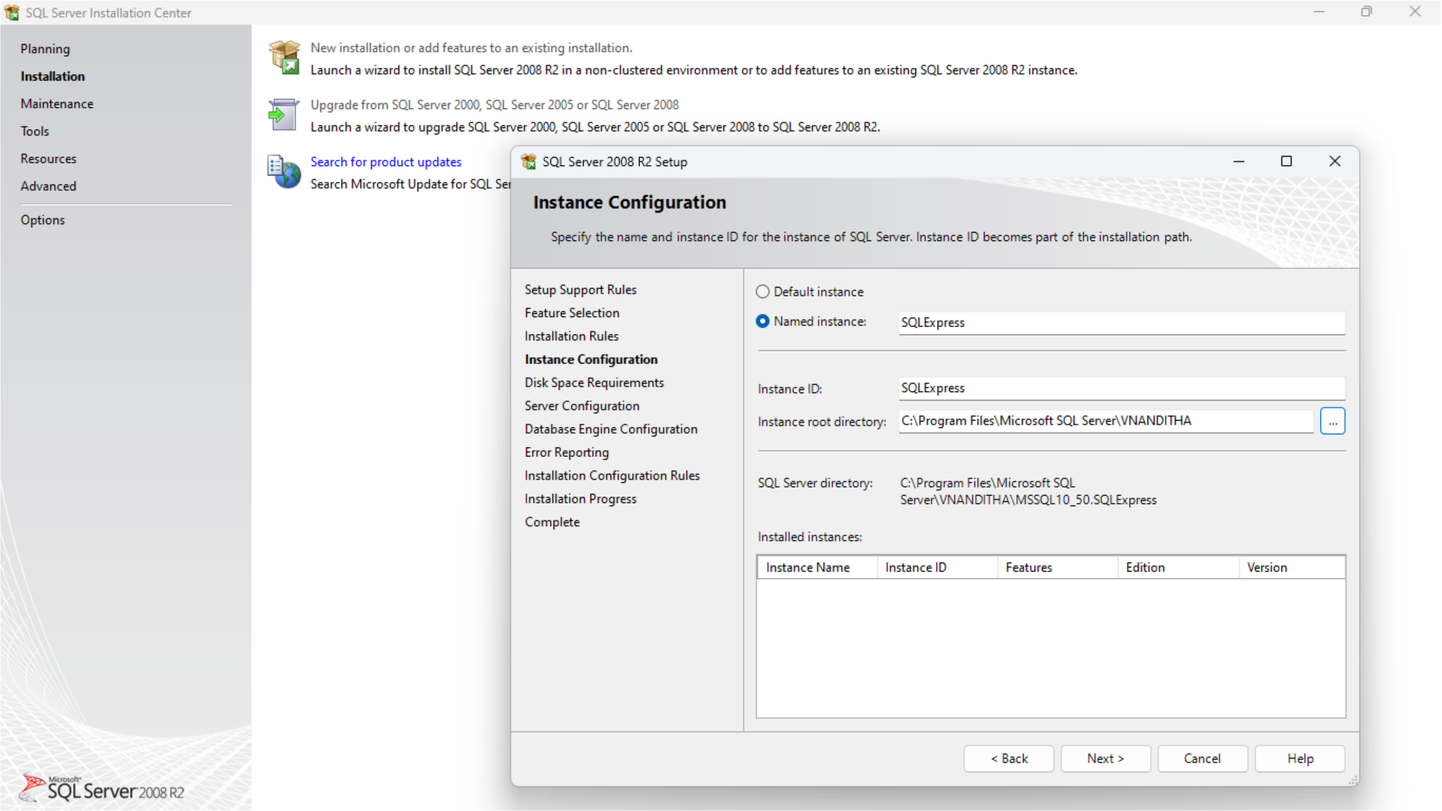
Redistributable Features

Description:

Server features are instance-aware and have their own registry hives. They support multiple instances on a computer.

Shared feature directory: C:\Program Files\Microsoft SQL Server\

Shared feature directory (x86): C:\Program Files (x86)\Microsoft SQL Server\



New installation or add features to an existing installation.

Launch a wizard to install SQL Server 2008 R2 in a non-clustered environment or to add features to an existing SQL Server 2008 R2 instance.

Upgrade from SQL Server 2000, SQL Server 2005 or SQL Server 2008

Launch a wizard to upgrade SQL Server 2000, SQL Server 2005 or SQL Server 2008 to SQL Server 2008 R2.

Search for product updates

Search Microsoft Update for SQL Ser

Instance Configuration

Specify the name and instance ID for the instance of SQL Server. Instance ID becomes part of the installation path.

- Setup Support Rules
- Feature Selection
- Installation Rules
- **Instance Configuration**
- Disk Space Requirements
- Server Configuration
- Database Engine Configuration
- Error Reporting
- Installation Configuration Rules
- Installation Progress
- Complete

○ Default instance

● Named instance: SQLExpress

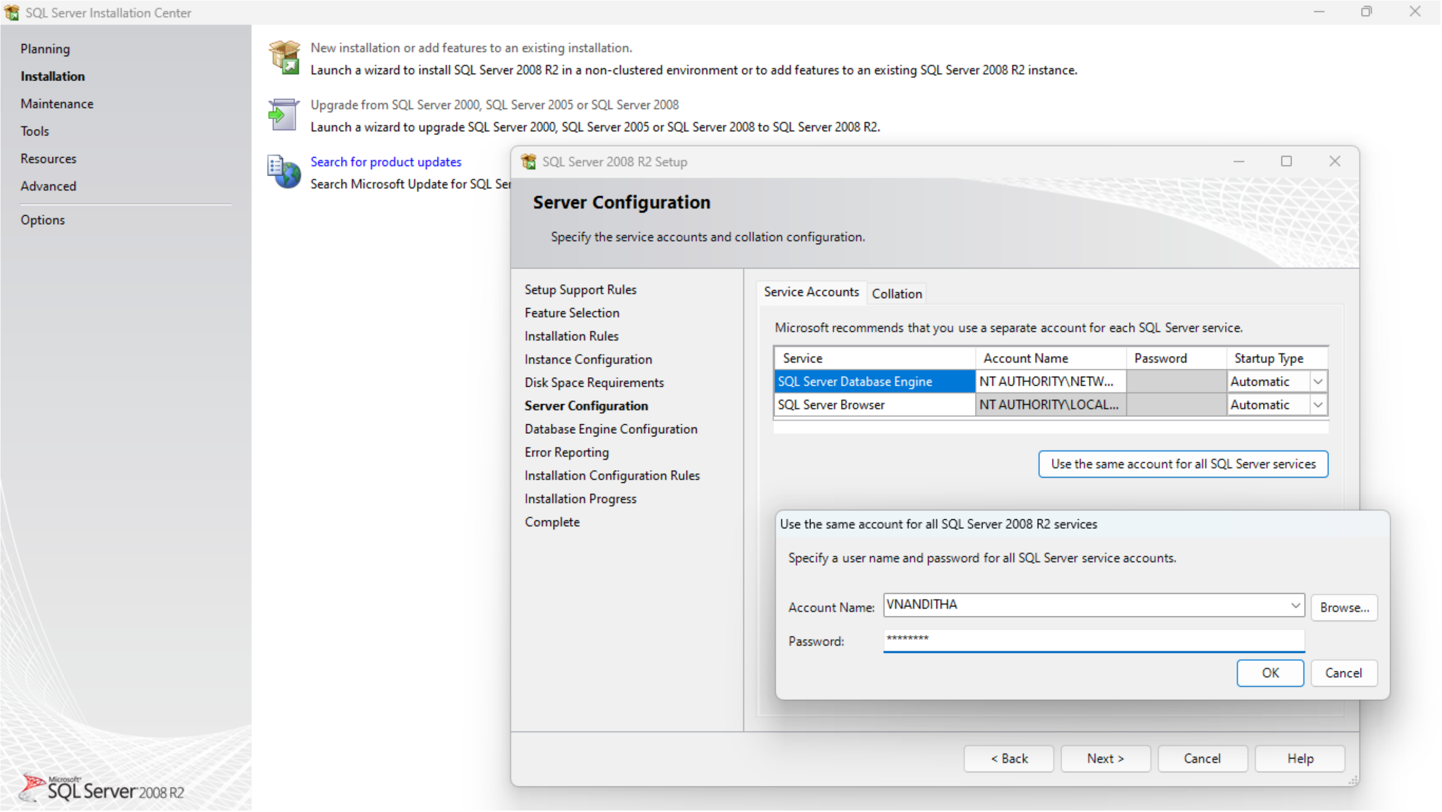
Instance ID: SQLExpress

Instance root directory: C:\Program Files\Microsoft SQL Server\VNANDITHA

SQL Server directory: C:\Program Files\Microsoft SQL Server\VNANDITHA\MSSQL10_50.SQLExpress

Installed instances:

Instance Name	Instance ID	Features	Edition	Version



New installation or add features to an existing installation.

Launch a wizard to install SQL Server 2008 R2 in a non-clustered environment or to add features to an existing SQL Server 2008 R2 instance.

Upgrade from SQL Server 2000, SQL Server 2005 or SQL Server 2008

Launch a wizard to upgrade SQL Server 2000, SQL Server 2005 or SQL Server 2008 to SQL Server 2008 R2.

Search for product updates

Search Microsoft Update for SQL Ser

Server Configuration

Specify the service accounts and collation configuration.

- Setup Support Rules
- Feature Selection
- Installation Rules
- Instance Configuration
- Disk Space Requirements
- **Server Configuration**
- Database Engine Configuration
- Error Reporting
- Installation Configuration Rules
- Installation Progress
- Complete

Service Accounts | Collation

Microsoft recommends that you use a separate account for each SQL Server service.

Service	Account Name	Password	Startup Type
SQL Server Database Engine	NT AUTHORITY\NETW...		Automatic
SQL Server Browser	NT AUTHORITY\LOCAL...		Automatic

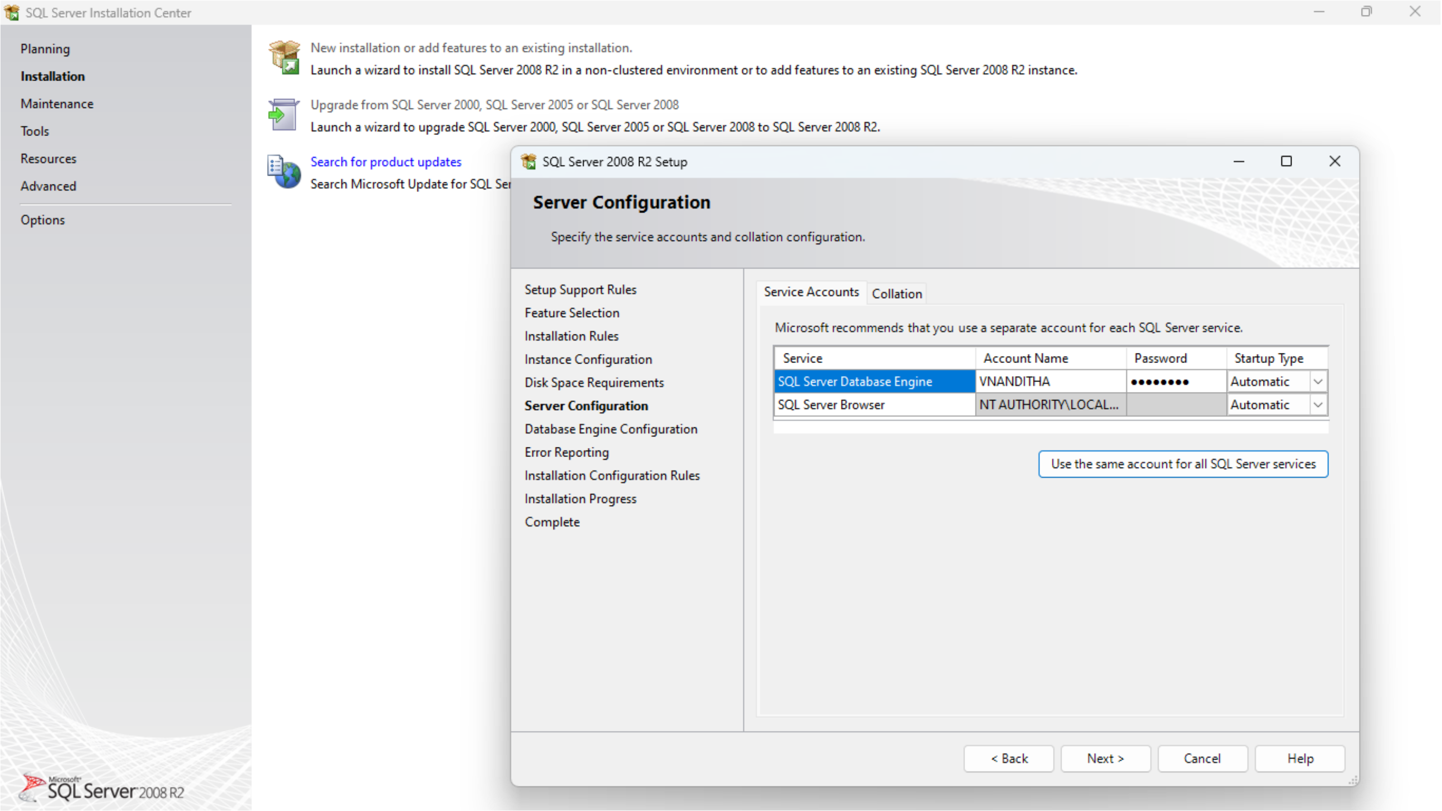
Use the same account for all SQL Server services

Use the same account for all SQL Server 2008 R2 services

Specify a user name and password for all SQL Server service accounts.

Account Name: VNANDITHA

Password: ********



New installation or add features to an existing installation.
Launch a wizard to install SQL Server 2008 R2 in a non-clustered environment or to add features to an existing SQL Server 2008 R2 instance.

Upgrade from SQL Server 2000, SQL Server 2005 or SQL Server 2008
Launch a wizard to upgrade SQL Server 2000, SQL Server 2005 or SQL Server 2008 to SQL Server 2008 R2.

Search for product updates
Search Microsoft Update for SQL Ser

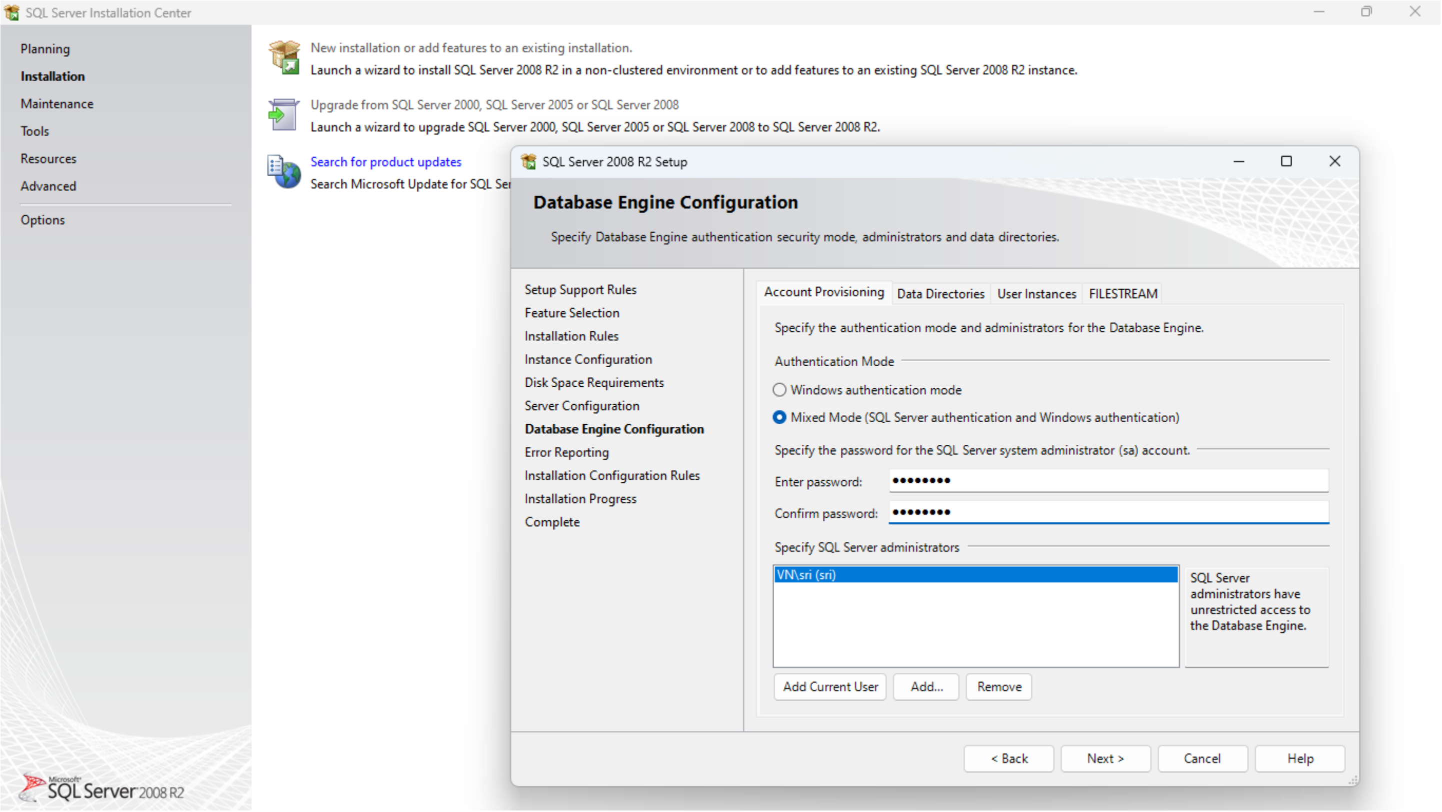
SQL Server 2008 R2 Setup

Server Configuration

Specify the service accounts and collation configuration.

Microsoft recommends that you use a separate account for each SQL Server service.

Service	Account Name	Password	Startup Type
SQL Server Database Engine	VNANDITHA	••••••••	Automatic
SQL Server Browser	NT AUTHORITY\LOCAL...		Automatic



New installation or add features to an existing installation.
Launch a wizard to install SQL Server 2008 R2 in a non-clustered environment or to add features to an existing SQL Server 2008 R2 instance.

Upgrade from SQL Server 2000, SQL Server 2005 or SQL Server 2008
Launch a wizard to upgrade SQL Server 2000, SQL Server 2005 or SQL Server 2008 to SQL Server 2008 R2.

Search for product updates
Search Microsoft Update for SQL Ser

SQL Server 2008 R2 Setup

Database Engine Configuration

Specify Database Engine authentication security mode, administrators and data directories.

Specify the authentication mode and administrators for the Database Engine.

Authentication Mode

○ Windows authentication mode
● Mixed Mode (SQL Server authentication and Windows authentication)

Specify the password for the SQL Server system administrator (sa) account.

Enter password: ••••••••
Confirm password: ••••••••

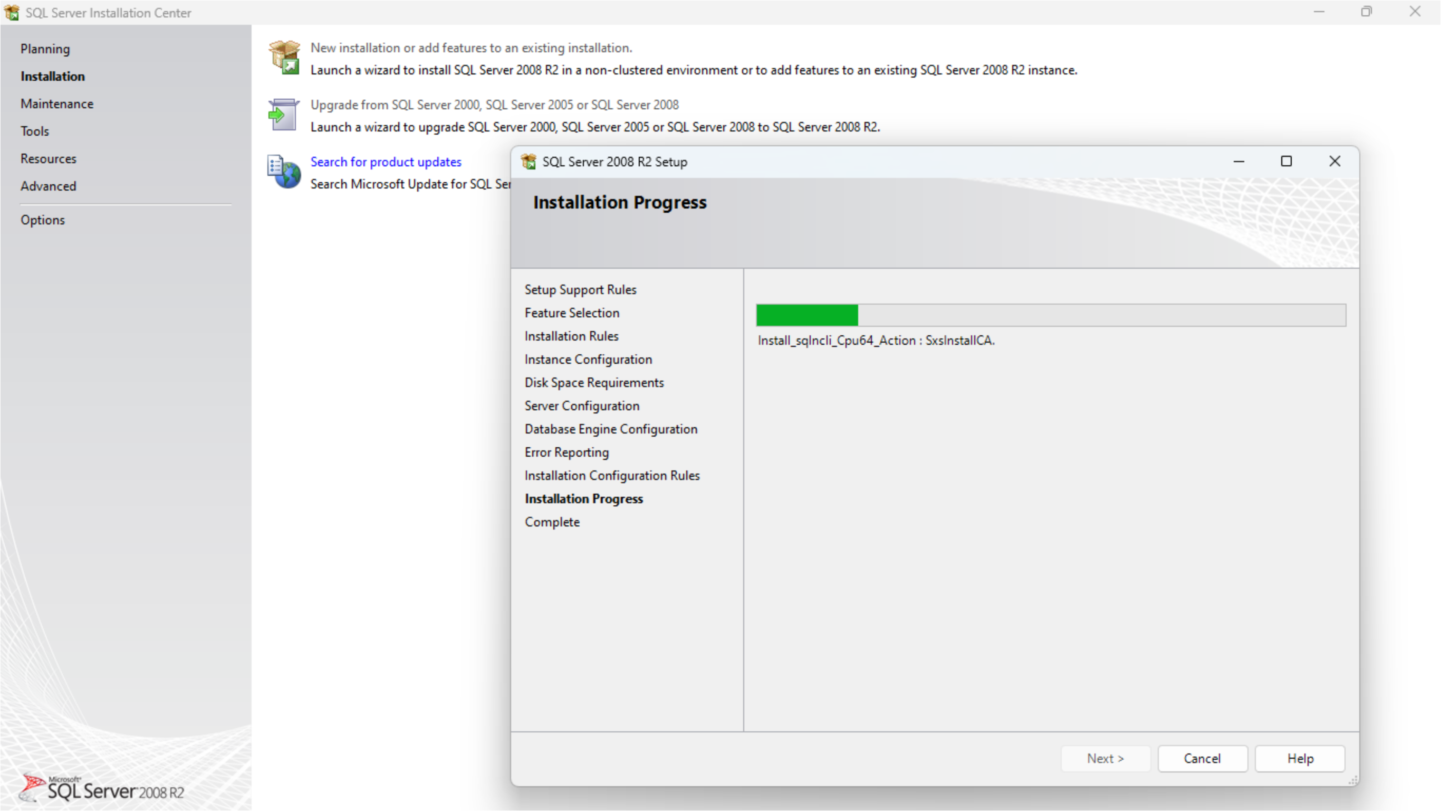
Specify SQL Server administrators

VN\sri (sri)

SQL Server administrators have unrestricted access to the Database Engine.

Password : P@ssw0rd

We also added the Current User (VN)



New installation or add features to an existing installation.

Launch a wizard to install SQL Server 2008 R2 in a non-clustered environment or to add features to an existing SQL Server 2008 R2 instance.

Upgrade from SQL Server 2000, SQL Server 2005 or SQL Server 2008

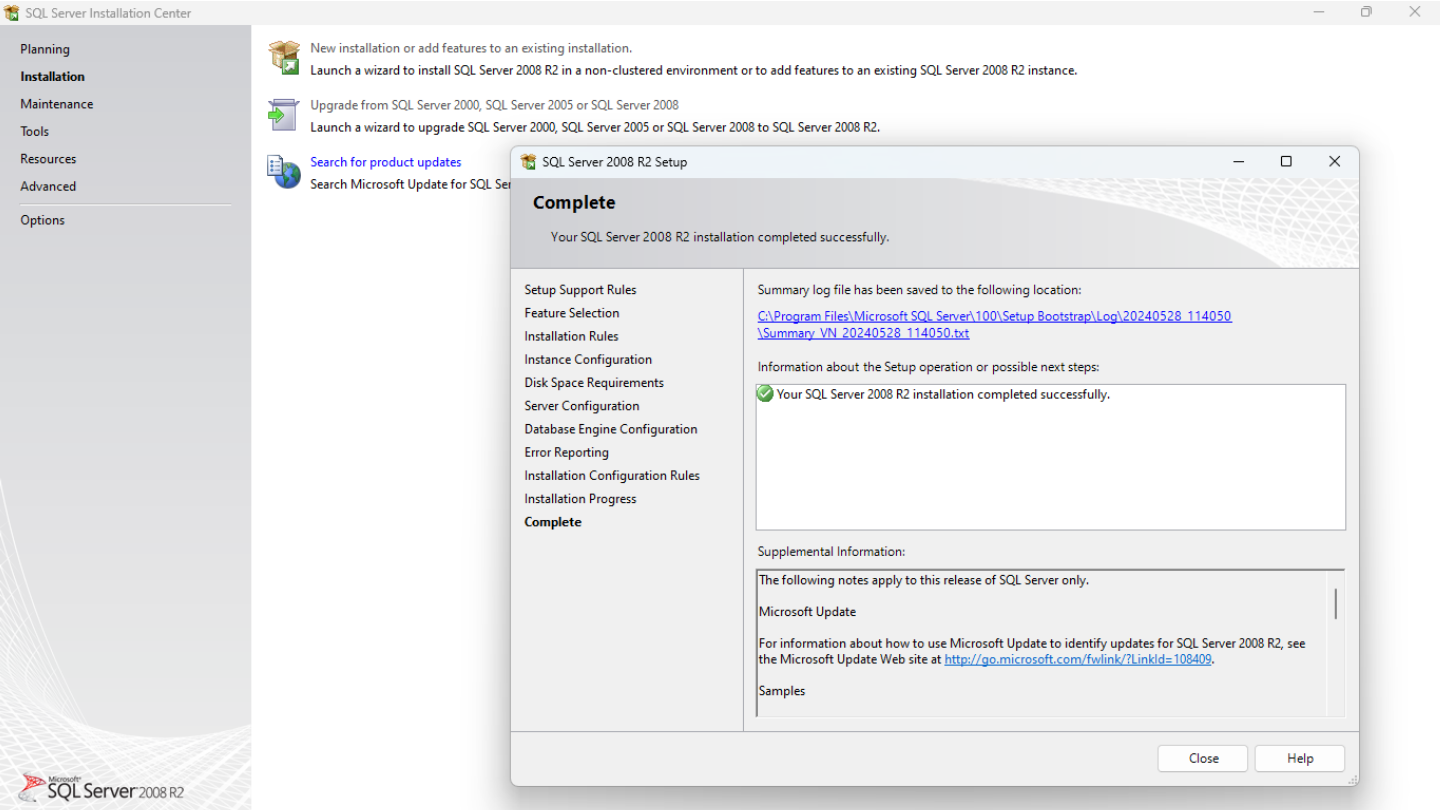
Launch a wizard to upgrade SQL Server 2000, SQL Server 2005 or SQL Server 2008 to SQL Server 2008 R2.

Search for product updates

Search Microsoft Update for SQL Ser

Installation Progress

Install_sqlncli_Cpu64_Action : SxsInstallCA.



New installation or add features to an existing installation.

Launch a wizard to install SQL Server 2008 R2 in a non-clustered environment or to add features to an existing SQL Server 2008 R2 instance.

Upgrade from SQL Server 2000, SQL Server 2005 or SQL Server 2008

Launch a wizard to upgrade SQL Server 2000, SQL Server 2005 or SQL Server 2008 to SQL Server 2008 R2.

Search for product updates

Search Microsoft Update for SQL Ser

Complete

Your SQL Server 2008 R2 installation completed successfully.

Summary log file has been saved to the following location:

C:\Program Files\Microsoft SQL Server\100\Setup Bootstrap\Log\20240528_114050
\Summary_VN_20240528_114050.txt

Information about the Setup operation or possible next steps:

✓ Your SQL Server 2008 R2 installation completed successfully.

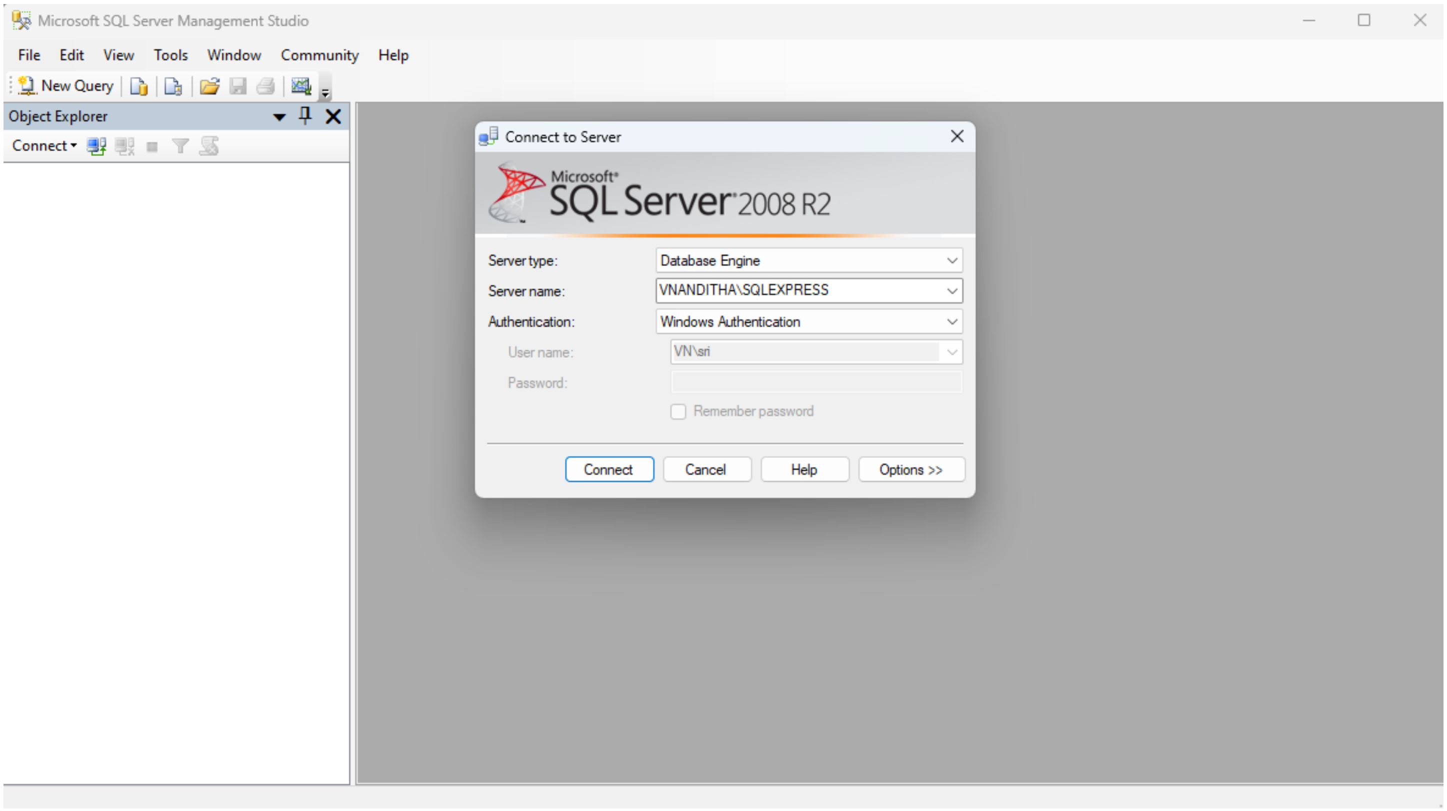
Supplemental Information:

The following notes apply to this release of SQL Server only.

Microsoft Update

For information about how to use Microsoft Update to identify updates for SQL Server 2008 R2, see the Microsoft Update Web site at http://go.microsoft.com/fwlink/?LinkId=108409.

Samples



Server type: Database Engine

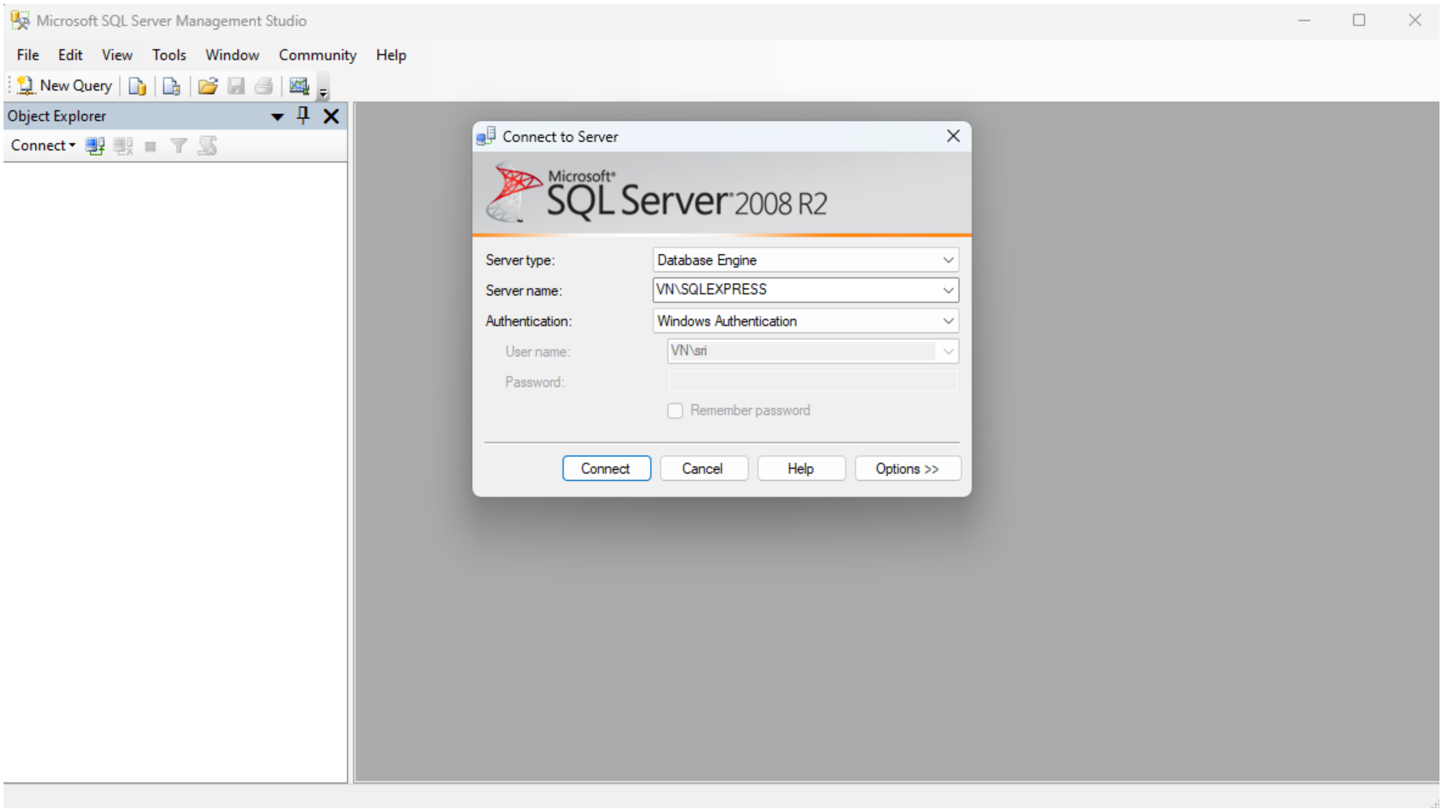
Server name: VNANDITHA\SQLEXPRESS

Authentication: Windows Authentication

User name: VN\sri

Password:

□ Remember password



Server type: Database Engine

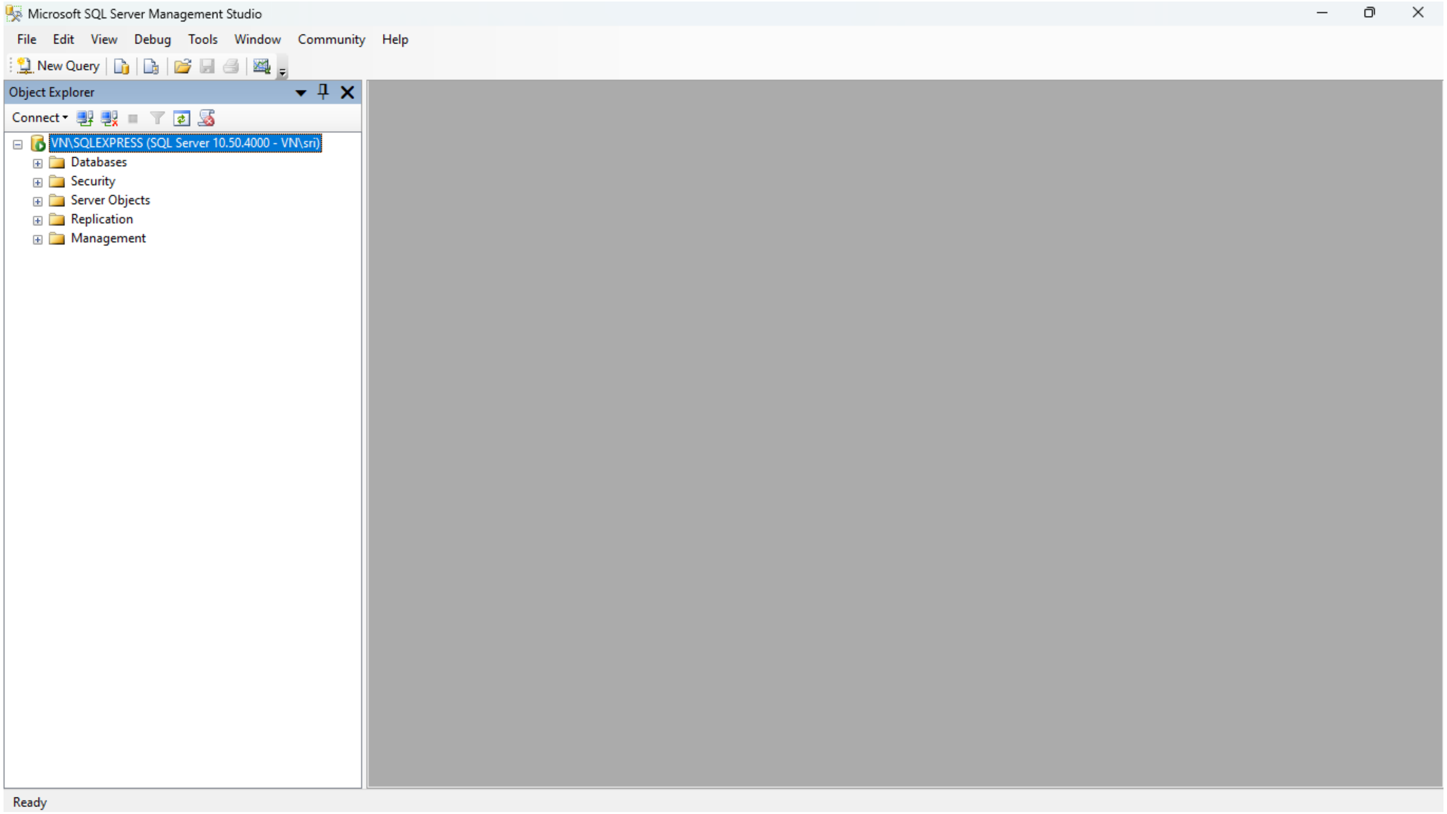
Server name: VN\SQLEXPRESS

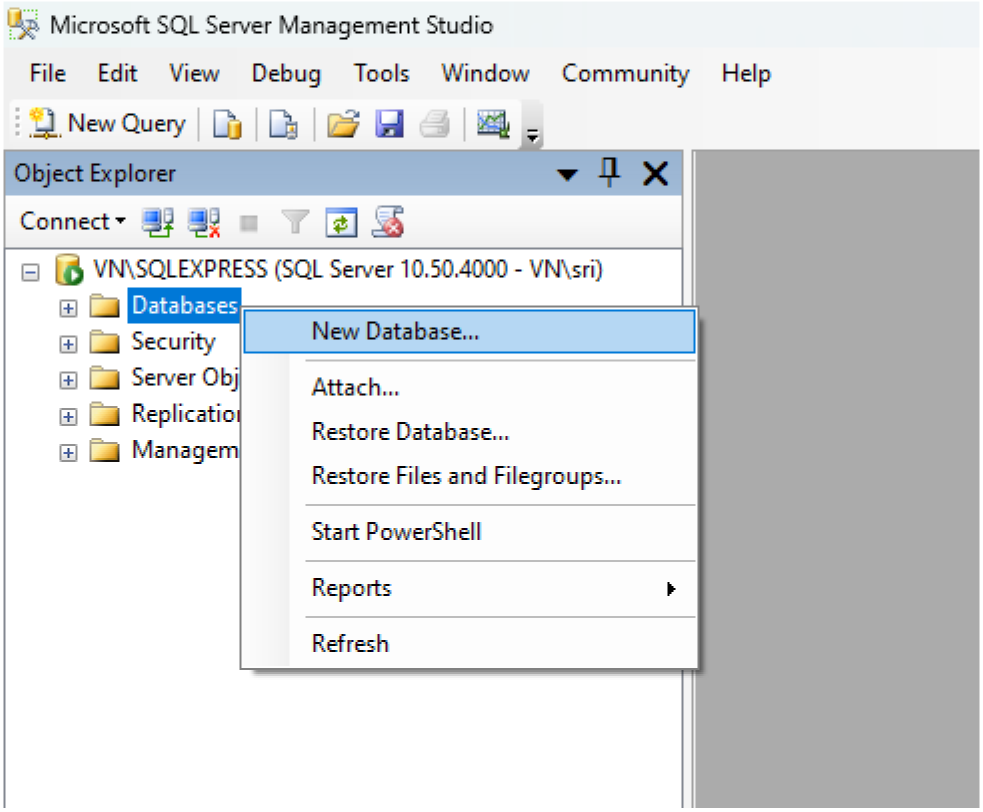
Authentication: Windows Authentication

User name: VN\sri

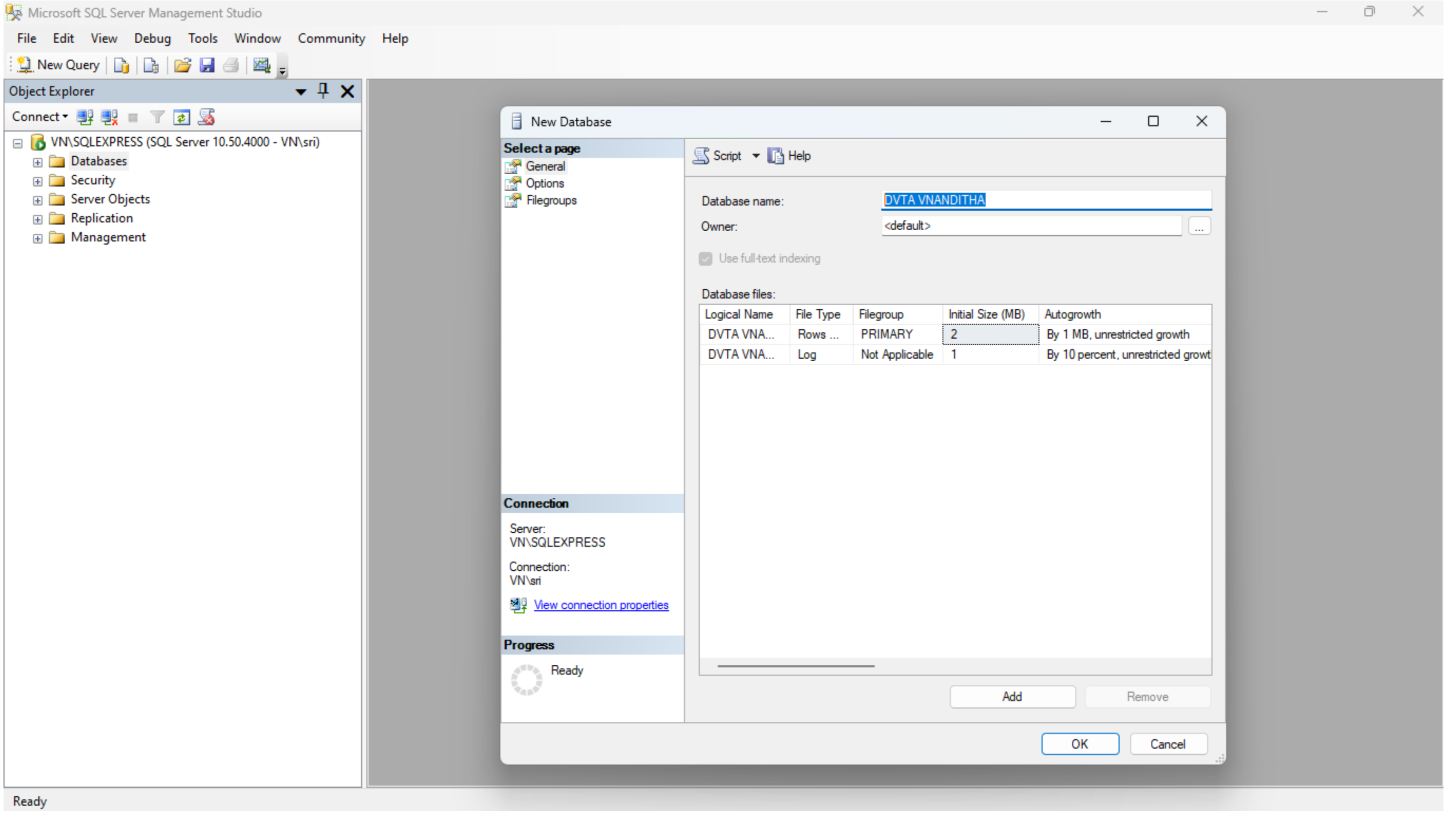
Password:

□ Remember password


Microsoft SQL Server Management Studio
File Edit View Debug Tools Window Community Help
New Query
Object Explorer
Connect
VN\SQLEXPRESS (SQL Server 10.50.4000 - VN\sri)
Databases
Security
Server Objects
Replication
Management
Ready


Microsoft SQL Server Management Studio
File Edit View Debug Tools Window Community Help
New Query
Object Explorer
Connect
VN\SQLEXPRESS (SQL Server 10.50.4000 - VN\sri)
Databases
Security
Server Obj
Replicatio
Managem
New Database...
Attach...
Restore Database...
Restore Files and Filegroups...
Start PowerShell
Reports
Refresh

Creating a New DB



Database name: DVTA VNANDITHA

Owner: <default>

☑ Use full-text indexing

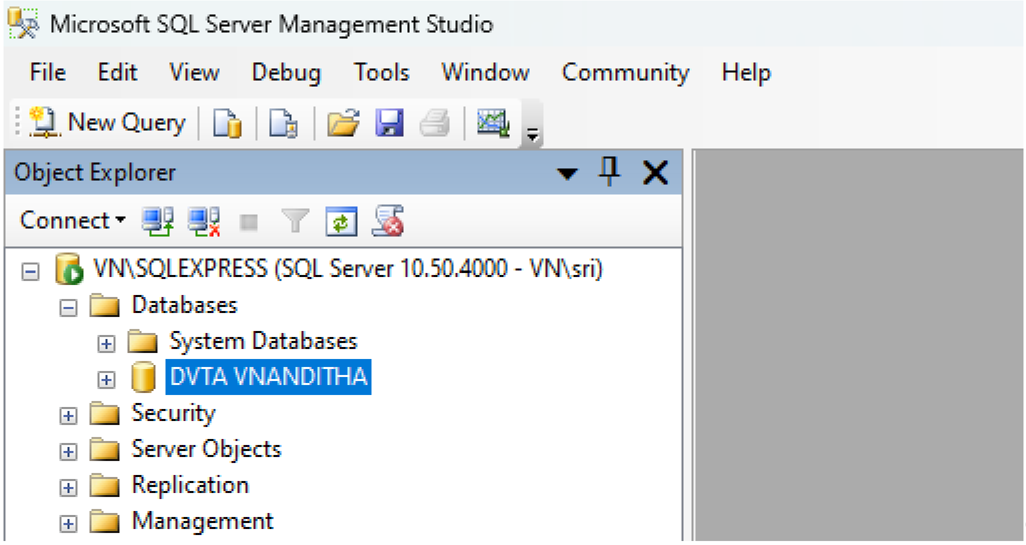
Database files:

Logical Name	File Type	Filegroup	Initial Size (MB)	Autogrowth
DVTA VNA...	Rows ...	PRIMARY	2	By 1 MB, unrestricted growth
DVTA VNA...	Log	Not Applicable	1	By 10 percent, unrestricted growt

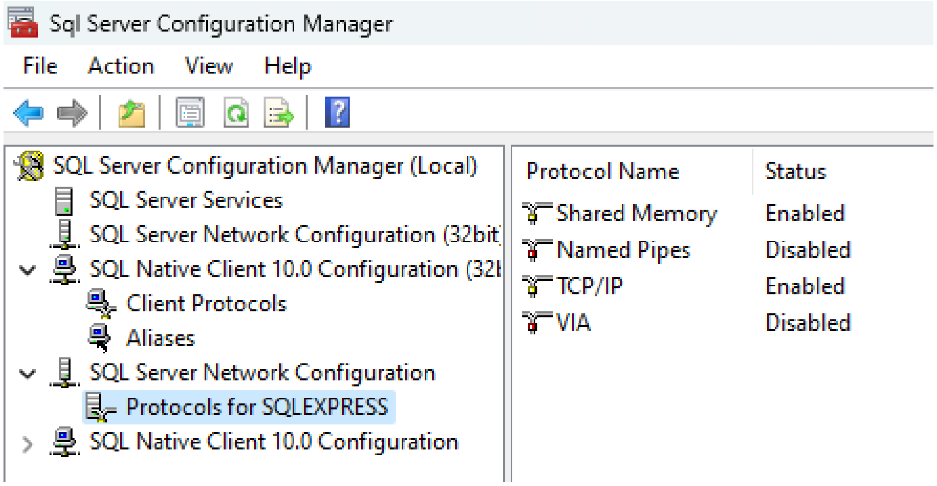
Server:
VN\SQLEXPRESS

Connection:
VN\sri

Ready

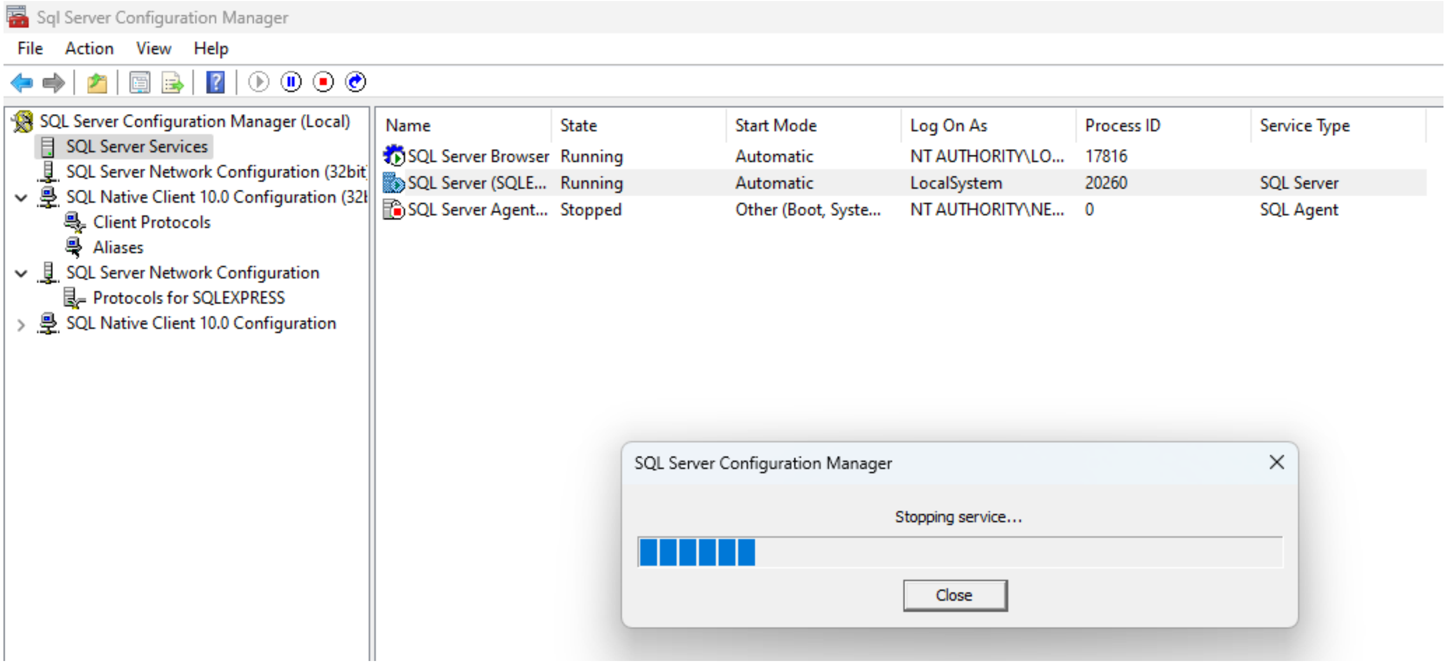

Microsoft SQL Server Management Studio
File Edit View Debug Tools Window Community Help
New Query
Object Explorer
Connect
VN\SQLEXPRESS (SQL Server 10.50.4000 - VN\sri)
Databases
System Databases
DVTA VNANDITHA
Security
Server Objects
Replication
Management

Got Created


Sql Server Configuration Manager
File Action View Help
SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration (32bit
SQL Native Client 10.0 Configuration (32b
Client Protocols
Aliases
SQL Server Network Configuration
Protocols for SQLEXPRESS
SQL Native Client 10.0 Configuration

Protocol Name	Status
Shared Memory	Enabled
Named Pipes	Disabled
TCP/IP	Enabled
VIA	Disabled

Restarting Service



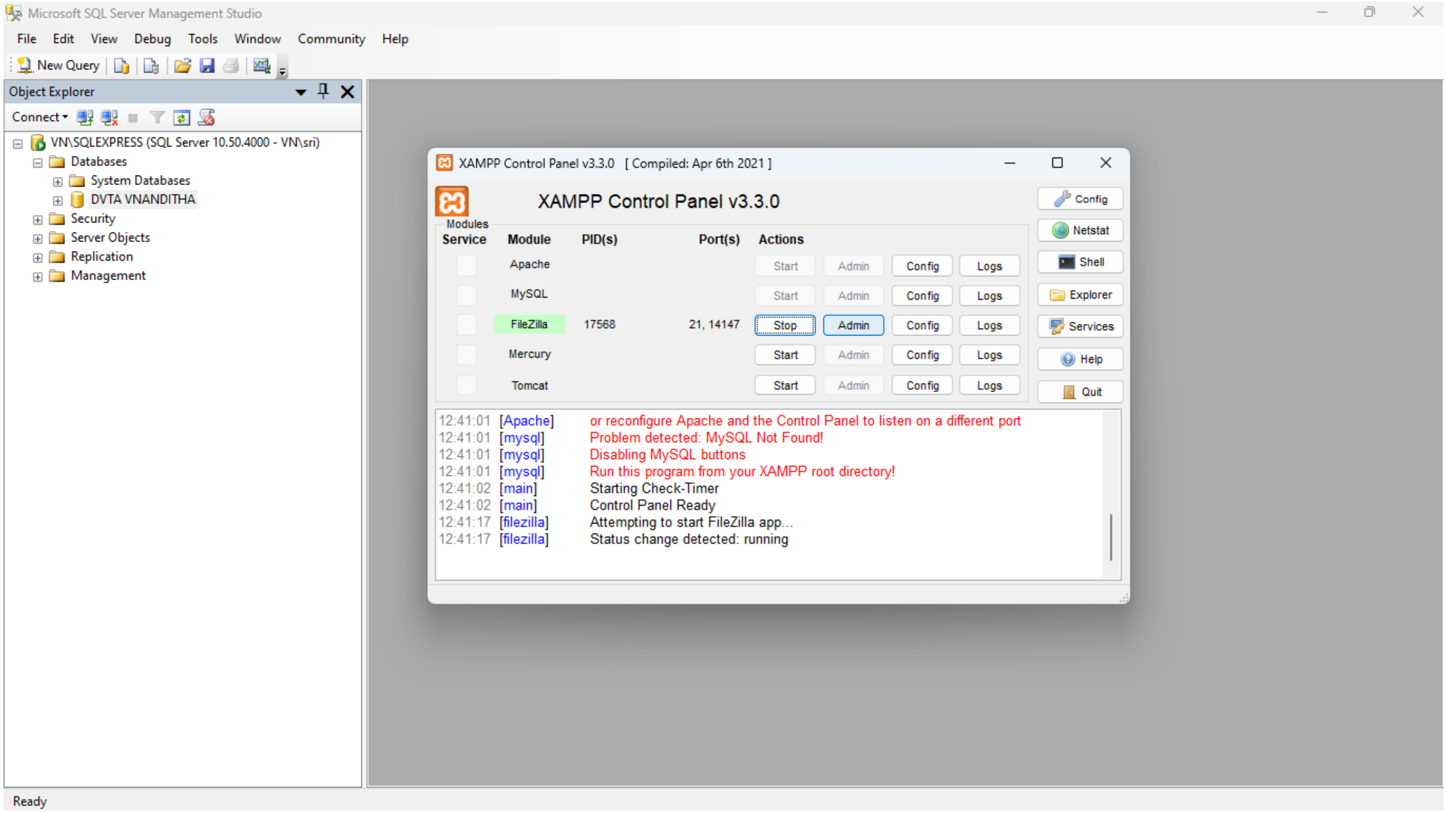
Sql Server Configuration Manager
File Action View Help
SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration (32bit
SQL Native Client 10.0 Configuration (32t
Client Protocols
Aliases
SQL Server Network Configuration
Protocols for SQLEXPRESS
SQL Native Client 10.0 Configuration

Name	State	Start Mode	Log On As	Process ID	Service Type
SQL Server Browser	Running	Automatic	NT AUTHORITY\LO...	17816	
SQL Server (SQLE...	Running	Automatic	LocalSystem	20260	SQL Server
SQL Server Agent...	Stopped	Other (Boot, Syste...	NT AUTHORITY\NE...	0	SQL Agent

SQL Server Configuration Manager

Stopping service...

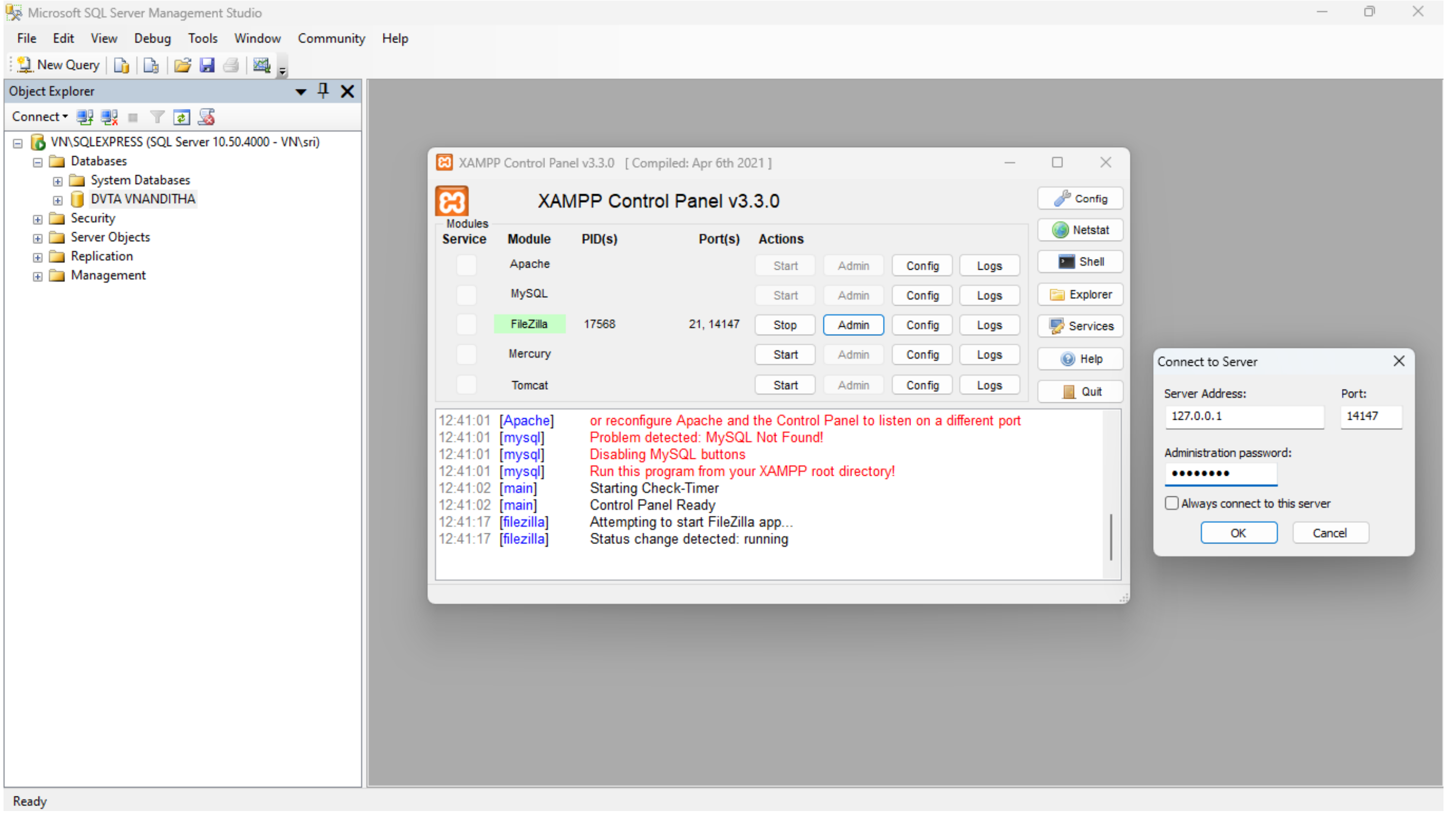
Open FileZilla > Start > Admin



Microsoft SQL Server Management Studio
File Edit View Debug Tools Window Community Help
New Query
Object Explorer
Connect
VN\SQLEXPRESS (SQL Server 10.50.4000 - VN\sri)
Databases
System Databases
DVTA VNANDITHA
Security
Server Objects
Replication
Management
Ready
XAMPP Control Panel v3.3.0 [Compiled: Apr 6th 2021]
XAMPP Control Panel v3.3.0
Config
Netstat
Shell
Explorer
Services
Help
Quit

Modules Service	Module	PID(s)	Port(s)	Actions			
	Apache			Start	Admin	Config	Logs
	MySQL			Start	Admin	Config	Logs
	FileZilla	17568	21, 14147	Stop	Admin	Config	Logs
	Mercury			Start	Admin	Config	Logs
	Tomcat			Start	Admin	Config	Logs

```
12:41:01  [Apache]     or reconfigure Apache and the Control Panel to listen on a different port
12:41:01  [mysql]      Problem detected: MySQL Not Found!
12:41:01  [mysql]      Disabling MySQL buttons
12:41:01  [mysql]      Run this program from your XAMPP root directory!
12:41:02  [main]       Starting Check-Timer
12:41:02  [main]       Control Panel Ready
12:41:17  [filezilla]  Attempting to start FileZilla app...
12:41:17  [filezilla]  Status change detected: running
```


Microsoft SQL Server Management Studio
File Edit View Debug Tools Window Community Help
New Query
Object Explorer
Connect
VN\SQLEXPRESS (SQL Server 10.50.4000 - VN\sri)
Databases
System Databases
DVTA VNANDITHA
Security
Server Objects
Replication
Management
XAMPP Control Panel v3.3.0 [Compiled: Apr 6th 2021]
XAMPP Control Panel v3.3.0
Config
Netstat
Shell
Explorer
Services
Help
Quit
Ready

Modules Service	Module	PID(s)	Port(s)	Actions			
	Apache			Start	Admin	Config	Logs
	MySQL			Start	Admin	Config	Logs
	FileZilla	17568	21, 14147	Stop	Admin	Config	Logs
	Mercury			Start	Admin	Config	Logs
	Tomcat			Start	Admin	Config	Logs

```
12:41:01  [Apache]    or reconfigure Apache and the Control Panel to listen on a different port
12:41:01  [mysql]     Problem detected: MySQL Not Found!
12:41:01  [mysql]     Disabling MySQL buttons
12:41:01  [mysql]     Run this program from your XAMPP root directory!
12:41:02  [main]      Starting Check-Timer
12:41:02  [main]      Control Panel Ready
12:41:17  [filezilla] Attempting to start FileZilla app...
12:41:17  [filezilla] Status change detected: running
```

Connect to Server

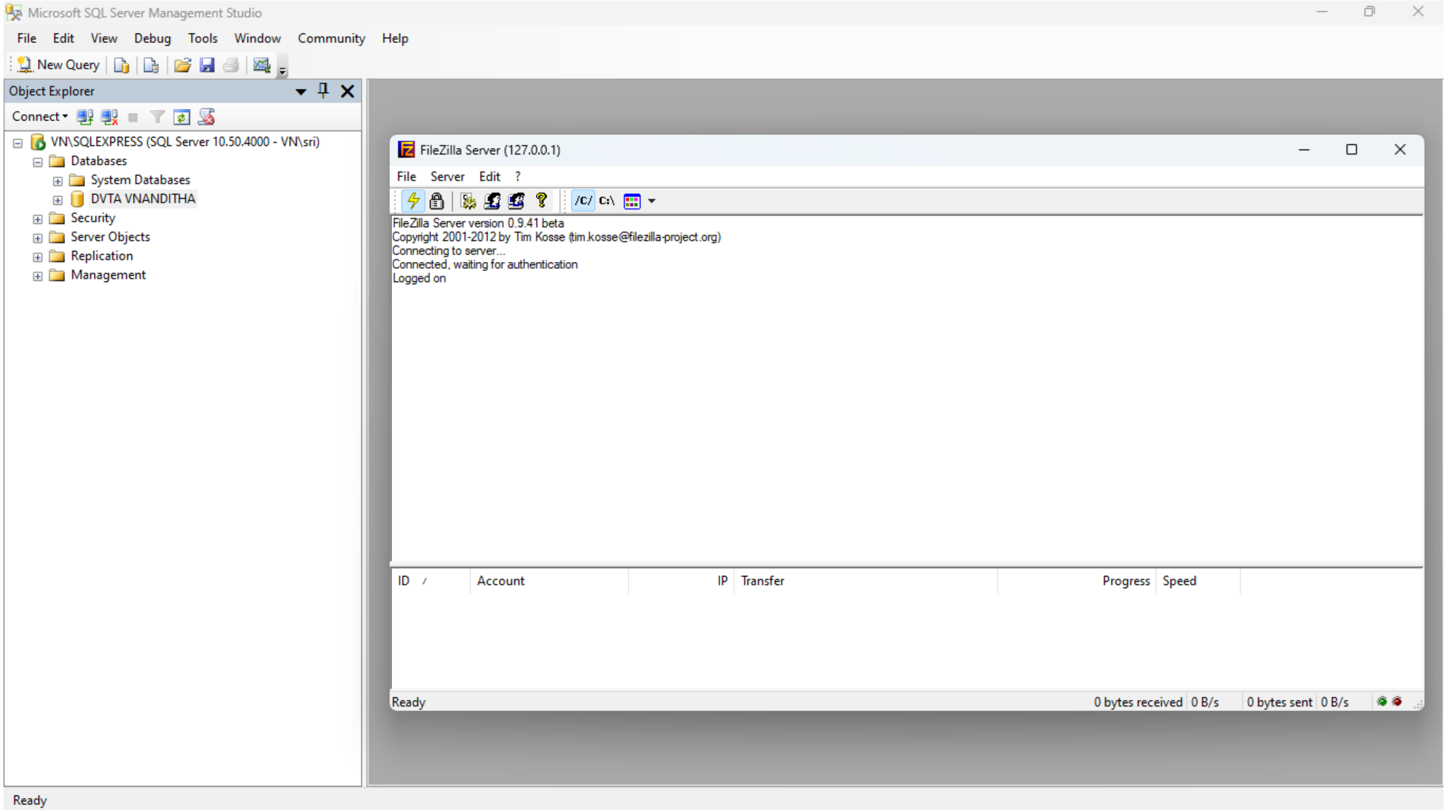
Server Address: 127.0.0.1

Port: 14147

Administration password: ••••••••

☐ Always connect to this server

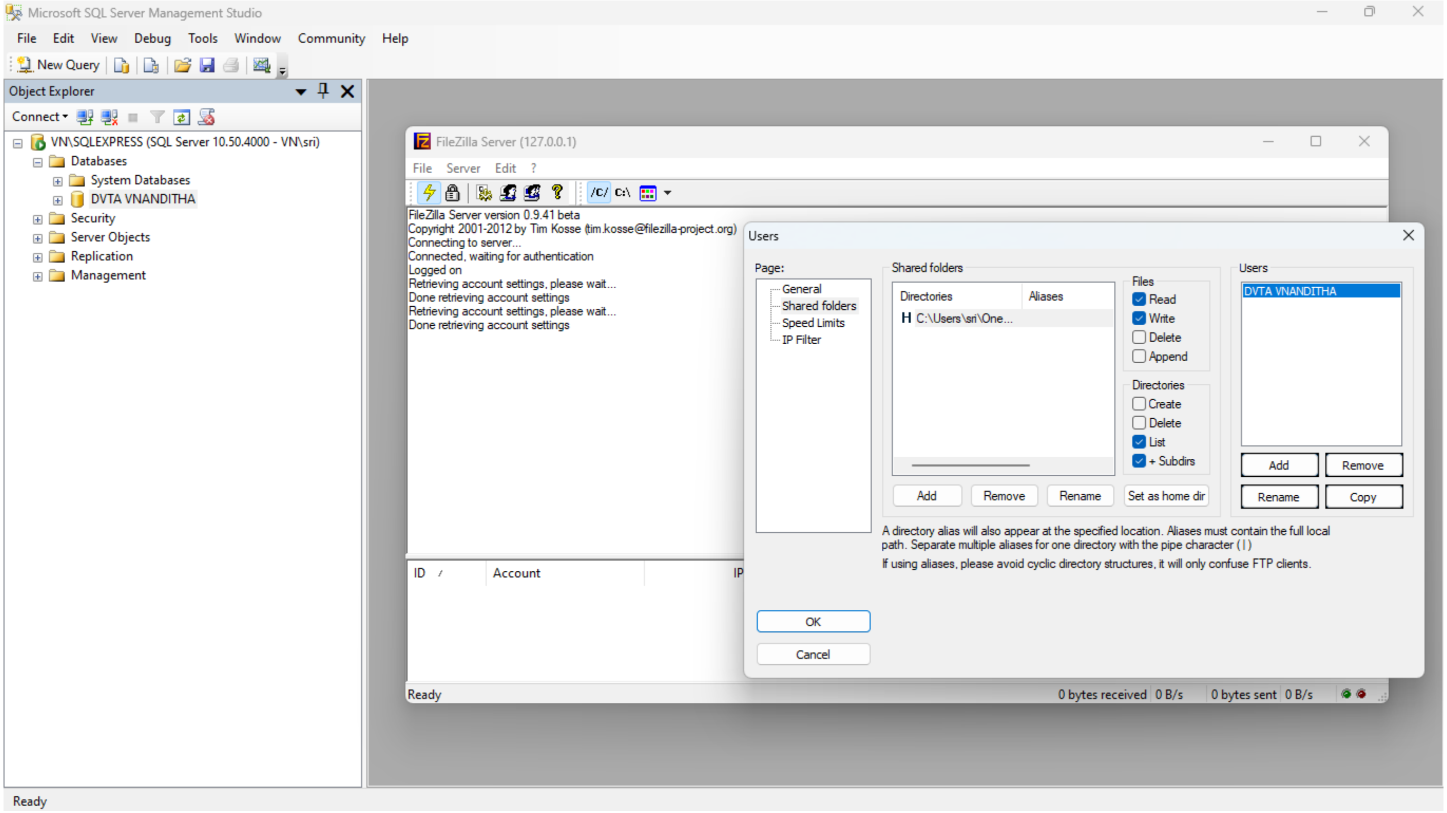
Connected


Microsoft SQL Server Management Studio
File Edit View Debug Tools Window Community Help
New Query
Object Explorer
Connect
VN\SQLEXPRESS (SQL Server 10.50.4000 - VN\sri)
Databases
System Databases
DVTA VNANDITHA
Security
Server Objects
Replication
Management
FileZilla Server (127.0.0.1)
File Server Edit ?
/C/ C:\
Ready

```
FileZilla Server version 0.9.41 beta
Copyright 2001-2012 by Tim Kosse (tim.kosse@filezilla-project.org)
Connecting to server...
Connected, waiting for authentication
Logged on
```

ID	Account	IP	Transfer	Progress	Speed

Ready 0 bytes received 0 B/s 0 bytes sent 0 B/s


Microsoft SQL Server Management Studio
File Edit View Debug Tools Window Community Help
New Query
Object Explorer
Connect
VN\SQLEXPRESS (SQL Server 10.50.4000 - VN\sri)
Databases
System Databases
DVTA VNANDITHA
Security
Server Objects
Replication
Management
FileZilla Server (127.0.0.1)
File Server Edit ?
ID / Account IP
Ready

```
FileZilla Server version 0.9.41 beta
Copyright 2001-2012 by Tim Kosse (tim.kosse@filezilla-project.org)
Connecting to server...
Connected, waiting for authentication
Logged on
Retrieving account settings, please wait...
Done retrieving account settings
Retrieving account settings, please wait...
Done retrieving account settings
```

Users

Page: General, **Shared folders**, Speed Limits, IP Filter

Shared folders

Directories	Aliases
H C:\Users\sri\One...	

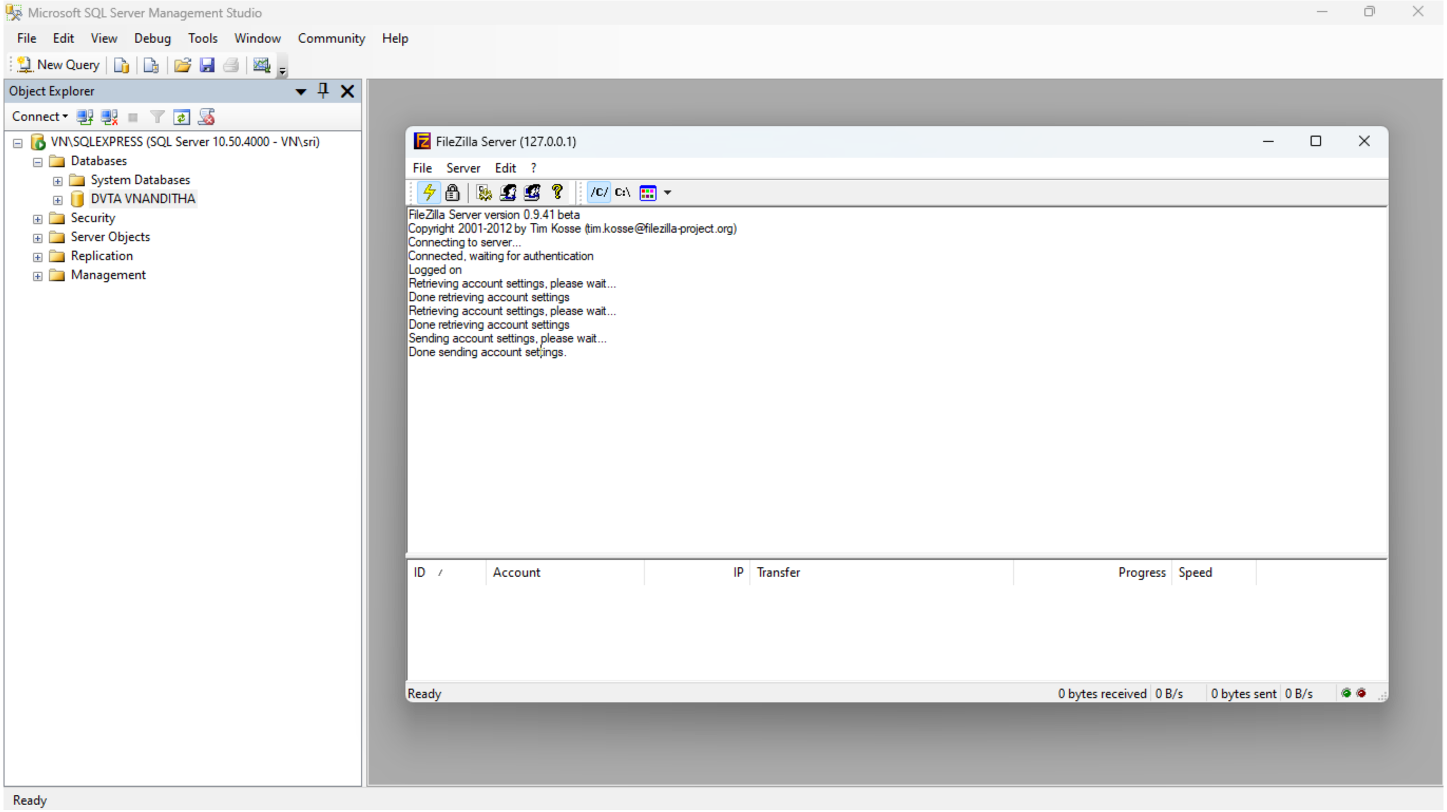
Files: ☑ Read ☑ Write ☐ Delete ☐ Append

Directories: ☐ Create ☐ Delete ☑ List ☑ + Subdirs

Users: DVTA VNANDITHA

A directory alias will also appear at the specified location. Aliases must contain the full local path. Separate multiple aliases for one directory with the pipe character (|)

If using aliases, please avoid cyclic directory structures, it will only confuse FTP clients.


Microsoft SQL Server Management Studio
File Edit View Debug Tools Window Community Help
New Query
Object Explorer
Connect
VN\SQLEXPRESS (SQL Server 10.50.4000 - VN\sri)
Databases
System Databases
DVTA VNANDITHA
Security
Server Objects
Replication
Management
FileZilla Server (127.0.0.1)
File Server Edit ?

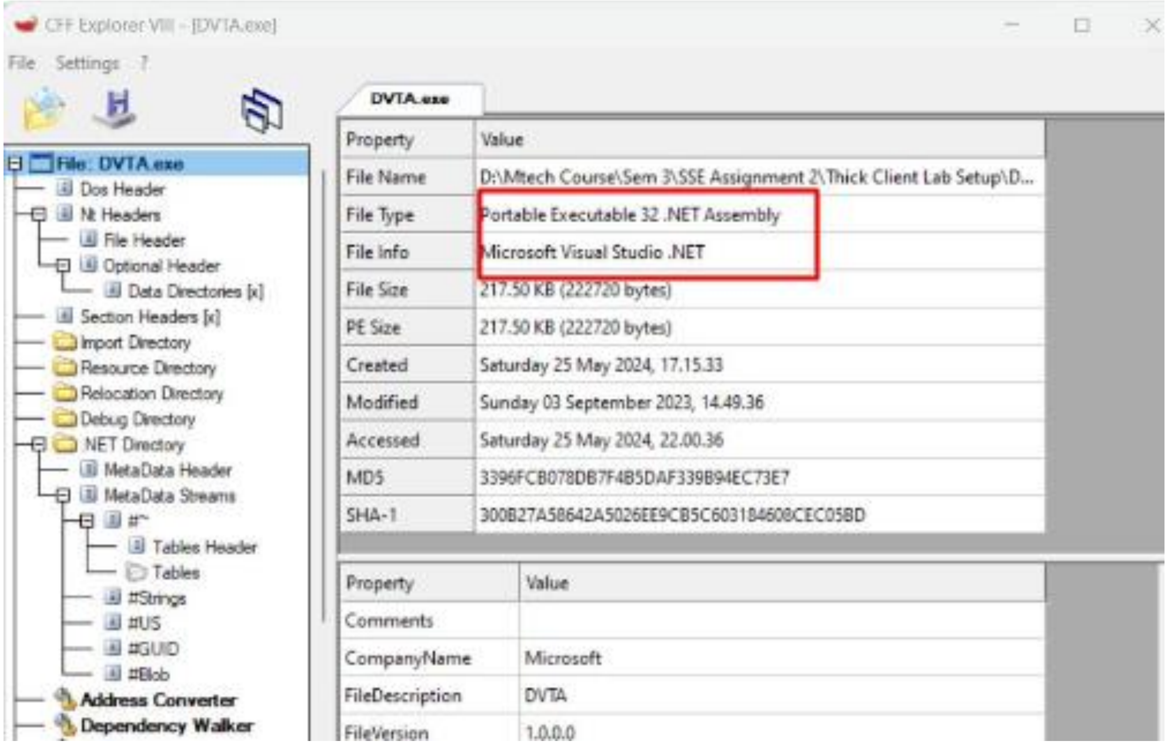
```
FileZilla Server version 0.9.41 beta
Copyright 2001-2012 by Tim Kosse (tim.kosse@filezilla-project.org)
Connecting to server...
Connected, waiting for authentication
Logged on
Retrieving account settings, please wait...
Done retrieving account settings
Retrieving account settings, please wait...
Done retrieving account settings
Sending account settings, please wait...
Done sending account settings.
```

1. **Identify the Application architecture, languages, and frameworks used**

- Start by running Dependency Walker on the executable to list all dependencies and get an overview of the architecture.
- Use PEiD to detect the compiler and possibly the language used.
- For .NET applications, use dotPeek to inspect assemblies.
- For Java applications, use JD-GUI to inspect JAR files.

Opening the .exe file in CFF-explorer, we can identify the following information

- Architecture 32bit & 2 tier (As it's communicating with the Database)
- Language used : .NET Assembly
- Frameworks : .NET Framework



Property	Value
File Name	D:\Mtech Course\Sem 3\SSE Assignment 2\Thick Client Lab Setup\D...
File Type	Portable Executable 32 .NET Assembly
File Info	Microsoft Visual Studio .NET
File Size	217.50 KB (222720 bytes)
PE Size	217.50 KB (222720 bytes)
Created	Saturday 25 May 2024, 17.15.33
Modified	Sunday 03 September 2023, 14.49.36
Accessed	Saturday 25 May 2024, 22.00.36
MD5	3396FCB078DB7F4B5DAF339B94EC73E7
SHA-1	300B27A58642A5026EE9CB5C603184608CEC05BD

Property	Value
Comments	
CompanyName	Microsoft
FileDescription	DVTA
FileVersion	1.0.0.0

POC:

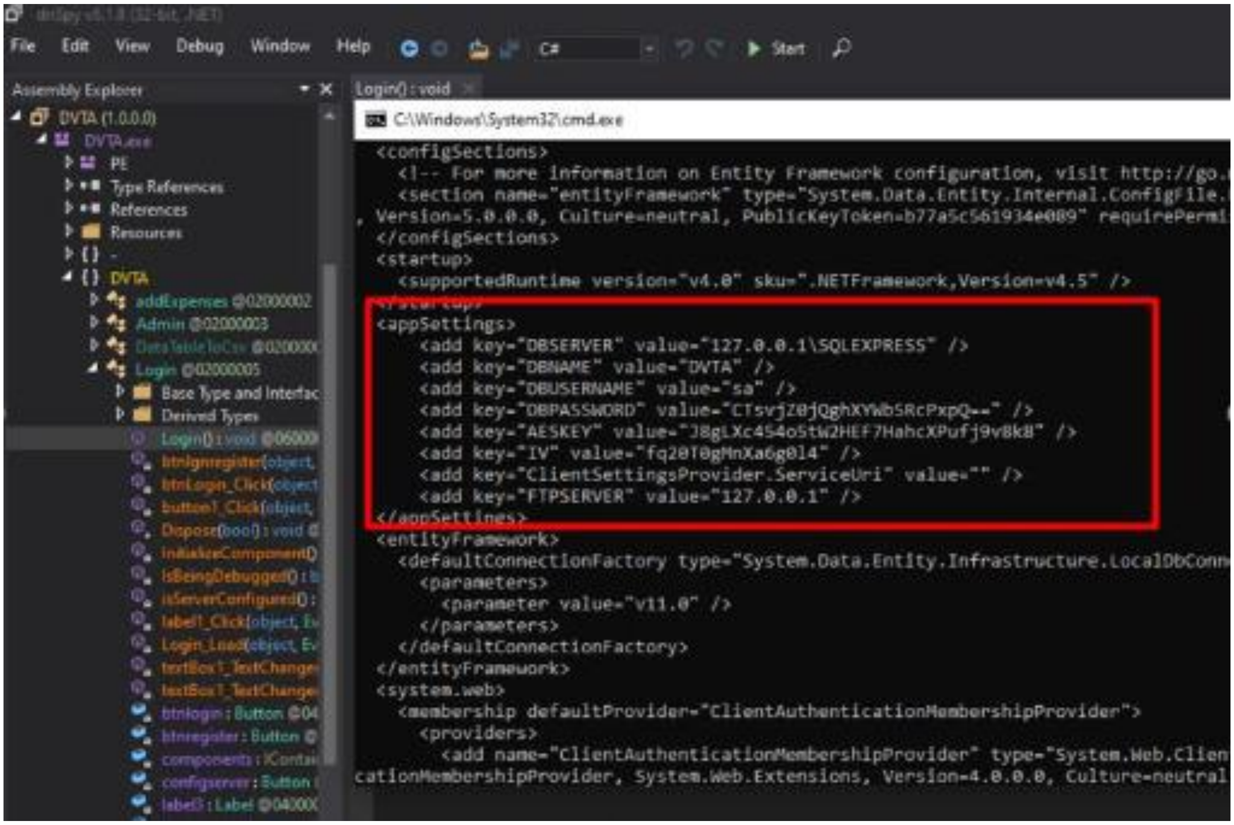
Tools: Dependency Walker, PEiD, dotPeek (for .NET applications), JD-GUI (for Java applications), and manual inspection of installation directories.

Methodology: Use these tools to inspect the executable files and libraries to determine the architecture (e.g., client-server, microservices), languages (e.g., C#, Java), and frameworks (e.g., .NET, Spring).

2. Decompile and try to retrieve the source code of the application. Also, check if any hardcoded sensitive information is found?

- Decompile the application binaries with appropriate tools (dotPeek for .NET, JD-GUI for Java).
- Search through the decompiled code for hardcoded credentials or sensitive information.

By Decompiling the Application using DNSpy or MS Visual Studio Tools, we can see the Source Code of the Application.



```
  <configSections>
    <!-- For more information on Entity Framework configuration, visit http://go.
    <section name="entityFramework" type="System.Data.Entity.Internal.ConfigFile.
, Version=5.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" requirePermi
  </configSections>
  <startup>
    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5" />
  </startup>
  <appSettings>
      <add key="DBSERVER" value="127.0.0.1\SQLEXPRESS" />
      <add key="DBNAME" value="DVTA" />
      <add key="DBUSERNAME" value="sa" />
      <add key="DBPASSWORD" value="CTsvjZ0jQghXYWbSRcPxpQ==" />
      <add key="AESKEY" value="J8gLXc454o5tW2HEF7HahcXPufj9v8k8" />
      <add key="IV" value="fq20T0gMnXa6g0l4" />
      <add key="ClientSettingsProvider.ServiceUri" value="" />
      <add key="FTPSERVER" value="127.0.0.1" />
  </appSettings>
  <entityFramework>
    <defaultConnectionFactory type="System.Data.Entity.Infrastructure.LocalDbConn
      <parameters>
        <parameter value="v11.0" />
      </parameters>
    </defaultConnectionFactory>
  </entityFramework>
  <system.web>
    <membership defaultProvider="ClientAuthenticationMembershipProvider">
      <providers>
        <add name="ClientAuthenticationMembershipProvider" type="System.Web.Clien
cationMembershipProvider, System.Web.Extensions, Version=4.0.0.0, Culture=neutral
```

POC:

Tools: dotPeek (for .NET), JD-GUI (for Java), Ghidra, and Hex Editors.

Methodology: Decompile the application binaries to source code using the appropriate decompilers. Search the code for hardcoded sensitive information such as passwords, API keys, and connection strings.

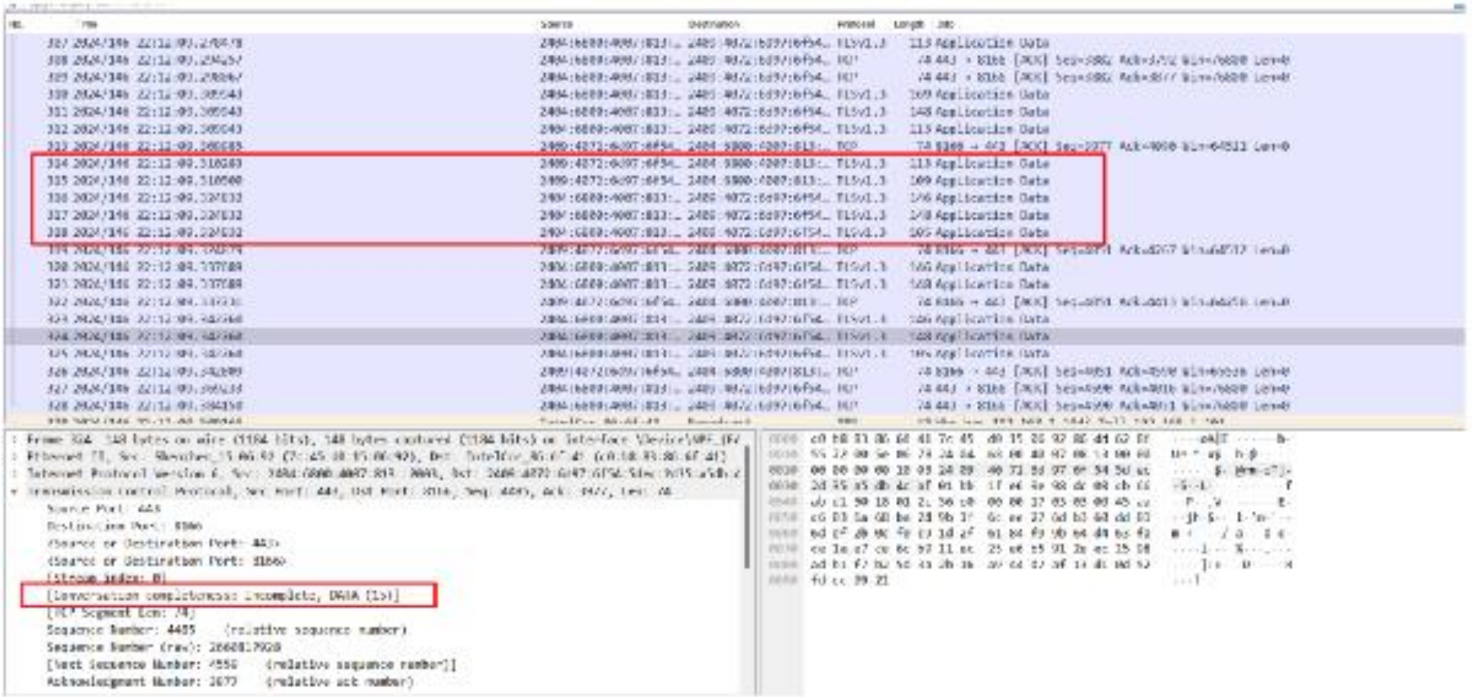
3. Sniff the traffic between client and server. Identify which protocol is being used for communication?

- Capture network traffic using Wireshark or tcpdump while the application communicates with the server.
- Identify protocols and look for any unencrypted data transmissions.

With Wireshark we can sniff the client and server

Next inspect the contents of the packets to determine whether the app is using TCP/UDP protocol for its communication

In the packet inspection window, we can see that the protocol used by the DVTA is TCP Protocol.



```
    Source Port: 443
    Destination Port: 8166
    [Source or Destination Port: 443]
    [Source or Destination Port: 8166]
    [Stream index: 0]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 74]
    Sequence Number: 4485    (relative sequence number)
    Sequence Number (raw): 2868817928
    [Next Sequence Number: 4559    (relative sequence number)]
    Acknowledgment Number: 3077    (relative ack number)
```

POC:

Tools: Wireshark, tcpdump.

Methodology: Capture network traffic while the application is in use to identify the protocol (e.g., HTTP, HTTPS, TCP, UDP) and analyze the data packets.

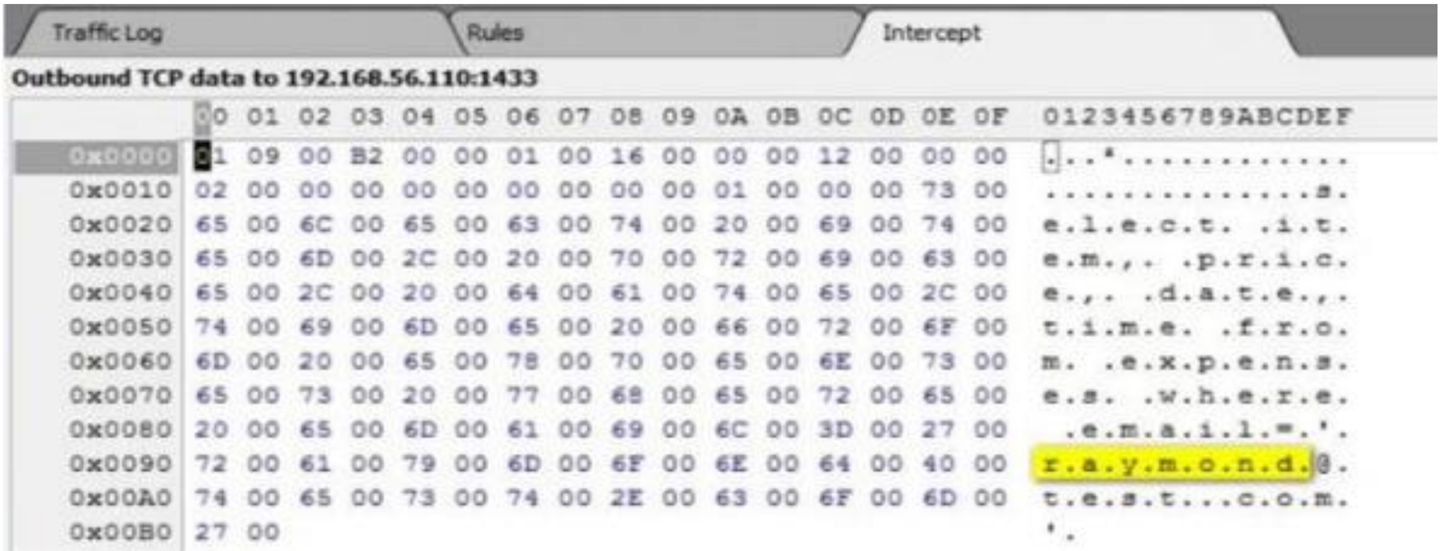
4. **Identify if unencrypted communication is happening between client and server?**

- Analyze the captured traffic in Wireshark to ensure sensitive data is transmitted over encrypted channels (e.g., HTTPS).

In this case we ca use either ECHIMIRAGE / Wireshark.

We are using ECHIMIRAGE here.

From the Output we can see that when we login to DVTA, the data is sent as Plain Text format to the Database



Outbound TCP data to 192.168.56.110:1433

```
        00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  0123456789ABCDEF
0x0000  01 09 00 B2 00 00 01 00 16 00 00 00 12 00 00 00  ...²............
0x0010  02 00 00 00 00 00 00 00 00 00 01 00 00 00 73 00  ..............s.
0x0020  65 00 6C 00 65 00 63 00 74 00 20 00 69 00 74 00  e.l.e.c.t. .i.t.
0x0030  65 00 6D 00 2C 00 20 00 70 00 72 00 69 00 63 00  e.m.,. .p.r.i.c.
0x0040  65 00 2C 00 20 00 64 00 61 00 74 00 65 00 2C 00  e.,. .d.a.t.e.,.
0x0050  74 00 69 00 6D 00 65 00 20 00 66 00 72 00 6F 00  t.i.m.e. .f.r.o.
0x0060  6D 00 20 00 65 00 78 00 70 00 65 00 6E 00 73 00  m. .e.x.p.e.n.s.
0x0070  65 00 73 00 20 00 77 00 68 00 65 00 72 00 65 00  e.s. .w.h.e.r.e.
0x0080  20 00 65 00 6D 00 61 00 69 00 6C 00 3D 00 27 00   .e.m.a.i.l.=.'.
0x0090  72 00 61 00 79 00 6D 00 6F 00 6E 00 64 00 40 00  r.a.y.m.o.n.d.@.
0x00A0  74 00 65 00 73 00 74 00 2E 00 63 00 6F 00 6D 00  t.e.s.t...c.o.m.
0x00B0  27 00                                            '.
```

POC:

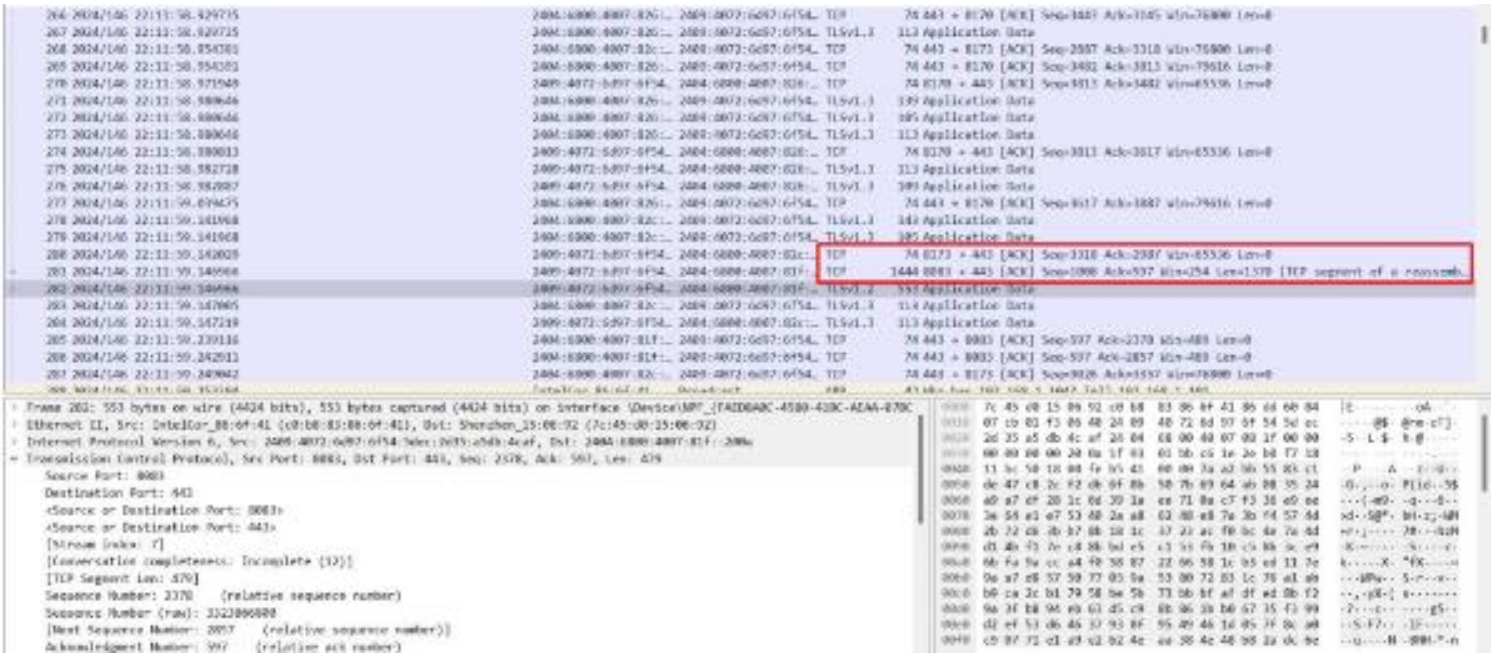
Tools: Wireshark.

Methodology: Inspect the captured traffic to check if sensitive information is being sent over unencrypted protocols (e.g., HTTP instead of HTTPS).

5. Capture and analyze the communication using proxy tools (e.g., Burp Suite, Echo Mirage)

- Configure Burp Suite as a proxy and capture the HTTP/HTTPS traffic from the application.
- Examine the requests and responses for sensitive data being sent in plaintext.

From the below, we can observe that using Wireshark we are able to capture and analyses the requests that are being sent to the Database and to the server.



```
266 2024/146 22:11:58.929735   2404:6800:4007:826:…  2409:4072:6d97:6f54…  TCP      74 443 → 8170 [ACK] Seq=3447 Ack=3145 Win=76800 Len=0
267 2024/146 22:11:58.929735   2404:6800:4007:826:…  2409:4072:6d97:6f54…  TLSv1.3  113 Application Data
268 2024/146 22:11:58.954381   2404:6800:4007:82c:…  2409:4072:6d97:6f54…  TCP      74 443 → 8173 [ACK] Seq=2887 Ack=3318 Win=76800 Len=0
269 2024/146 22:11:58.954381   2404:6800:4007:826:…  2409:4072:6d97:6f54…  TCP      74 443 → 8170 [ACK] Seq=3482 Ack=3813 Win=79616 Len=0
270 2024/146 22:11:58.971949   2409:4072:6d97:6f54…  2404:6800:4007:826:…  TCP      74 8170 → 443 [ACK] Seq=3813 Ack=3482 Win=65536 Len=0
271 2024/146 22:11:58.980646   2404:6800:4007:826:…  2409:4072:6d97:6f54…  TLSv1.3  139 Application Data
272 2024/146 22:11:58.980646   2404:6800:4007:826:…  2409:4072:6d97:6f54…  TLSv1.3  105 Application Data
273 2024/146 22:11:58.980646   2404:6800:4007:826:…  2409:4072:6d97:6f54…  TLSv1.3  113 Application Data
274 2024/146 22:11:58.980813   2409:4072:6d97:6f54…  2404:6800:4007:826:…  TCP      74 8170 → 443 [ACK] Seq=3813 Ack=3617 Win=65536 Len=0
275 2024/146 22:11:58.982728   2409:4072:6d97:6f54…  2404:6800:4007:826:…  TLSv1.3  113 Application Data
276 2024/146 22:11:58.982887   2409:4072:6d97:6f54…  2404:6800:4007:826:…  TLSv1.3  109 Application Data
277 2024/146 22:11:59.079475   2404:6800:4007:826:…  2409:4072:6d97:6f54…  TCP      74 443 → 8170 [ACK] Seq=3617 Ack=3887 Win=79616 Len=0
278 2024/146 22:11:59.141968   2404:6800:4007:82c:…  2409:4072:6d97:6f54…  TLSv1.3  143 Application Data
279 2024/146 22:11:59.141968   2404:6800:4007:82c:…  2409:4072:6d97:6f54…  TLSv1.3  105 Application Data
280 2024/146 22:11:59.142029   2409:4072:6d97:6f54…  2404:6800:4007:82c:…  TCP      74 8173 → 443 [ACK] Seq=3318 Ack=2987 Win=65536 Len=0
281 2024/146 22:11:59.146968   2409:4072:6d97:6f54…  2404:6800:4007:81f:…  TCP    1444 8083 → 443 [ACK] Seq=1000 Ack=597 Win=254 Len=1370 [TCP segment of a reassemb…
282 2024/146 22:11:59.146968   2409:4072:6d97:6f54…  2404:6800:4007:81f:…  TLSv1.2  553 Application Data
283 2024/146 22:11:59.147005   2404:6800:4007:82c:…  2409:4072:6d97:6f54…  TLSv1.3  114 Application Data
284 2024/146 22:11:59.147219   2409:4072:6d97:6f54…  2404:6800:4007:82c:…  TLSv1.3  113 Application Data
285 2024/146 22:11:59.239116   2404:6800:4007:81f:…  2409:4072:6d97:6f54…  TCP      74 443 → 8083 [ACK] Seq=597 Ack=2370 Win=489 Len=0
286 2024/146 22:11:59.242911   2404:6800:4007:81f:…  2409:4072:6d97:6f54…  TCP      74 443 → 8083 [ACK] Seq=597 Ack=2857 Win=489 Len=0
287 2024/146 22:11:59.249042   2404:6800:4007:82c:…  2409:4072:6d97:6f54…  TCP      74 443 → 8173 [ACK] Seq=3026 Ack=3397 Win=76800 Len=0
```

```
> Frame 282: 553 bytes on wire (4424 bits), 553 bytes captured (4424 bits) on interface \Device\NPF_{FAIDBA0C-4580-420C-AEAA-870C
> Ethernet II, Src: IntelCor_88:6f:41 (c0:b0:83:88:6f:41), Dst: Shenzhen_15:06:92 (7c:45:d0:15:06:92)
> Internet Protocol Version 6, Src: 2409:4072:6d97:6f54:5dec:2695:a5db:4caf, Dst: 2404:6800:4007:81f::200a
v Transmission Control Protocol, Src Port: 8083, Dst Port: 443, Seq: 2378, Ack: 597, Len: 479
    Source Port: 8083
    Destination Port: 443
    <Source or Destination Port: 8083>
    <Source or Destination Port: 443>
    [Stream index: 7]
    [Conversation completeness: Incomplete (12)]
    [TCP Segment Len: 479]
    Sequence Number: 2378    (relative sequence number)
    Sequence Number (raw): 3322086800
    [Next Sequence Number: 2857    (relative sequence number)]
    Acknowledgment Number: 597    (relative ack number)
```

POC:

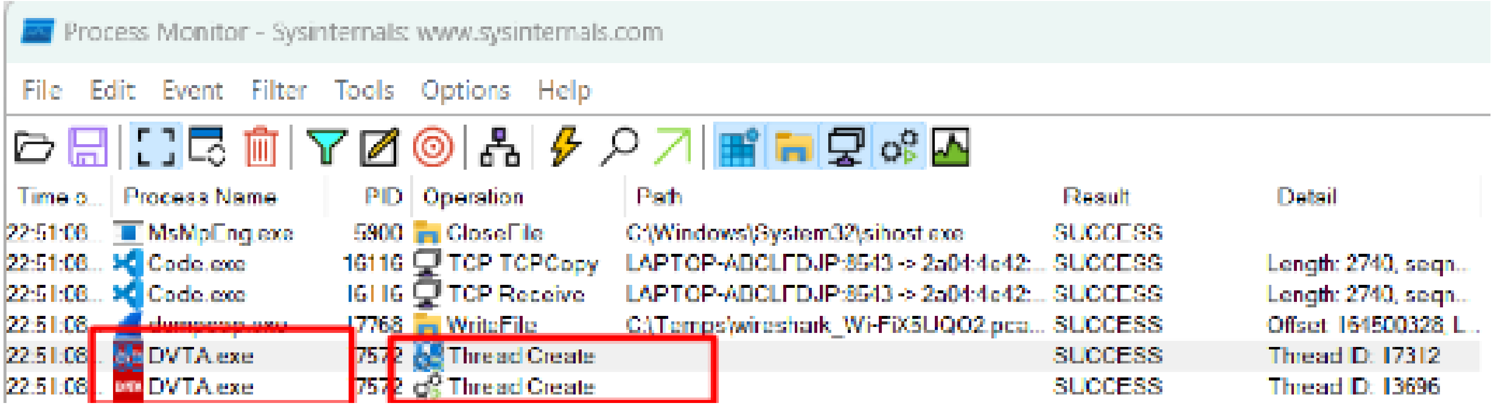
Tools: Burp Suite, Echo Mirage.

Methodology: Set up a proxy to intercept and analyze the application’s HTTP/HTTPS traffic. Look for sensitive data being transmitted in plaintext.

6. Analyze the application workflow and observe which all files/folders are being used by the application using Process Monitor

- Run Process Monitor to track all file and registry operations by the application.
- Analyze the logs to identify which files and directories are being accessed and modified.

With the help of tool called Process-Monitor can see that there are several files and folders being retrieved during the process of DVTA.exe.



Time o...	Process Name	PID	Operation	Path	Result	Detail
22:51:08...	MsMpEng.exe	5900	CloseFile	C:\Windows\System32\sihost.exe	SUCCESS	
22:51:08...	Code.exe	16116	TCP TCPCopy	LAPTOP-ADCLFDJP:8543 -> 2a04:4e42:...	SUCCESS	Length: 2740, seqn...
22:51:08...	Code.exe	16116	TCP Receive	LAPTOP-ADCLFDJP:8543 -> 2a04:4e42:...	SUCCESS	Length: 2740, seqn...
22:51:08...	dumpcap.exe	17768	WriteFile	C:\Temps\wireshark_Wi-FiX5UQO2.pca...	SUCCESS	Offset: 164500328, L...
22:51:08...	DVTA.exe	7572	Thread Create		SUCCESS	Thread ID: 17312
22:51:08...	DVTA.exe	7572	Thread Create		SUCCESS	Thread ID: 13696

POC:

Tools: Process Monitor (ProcMon).

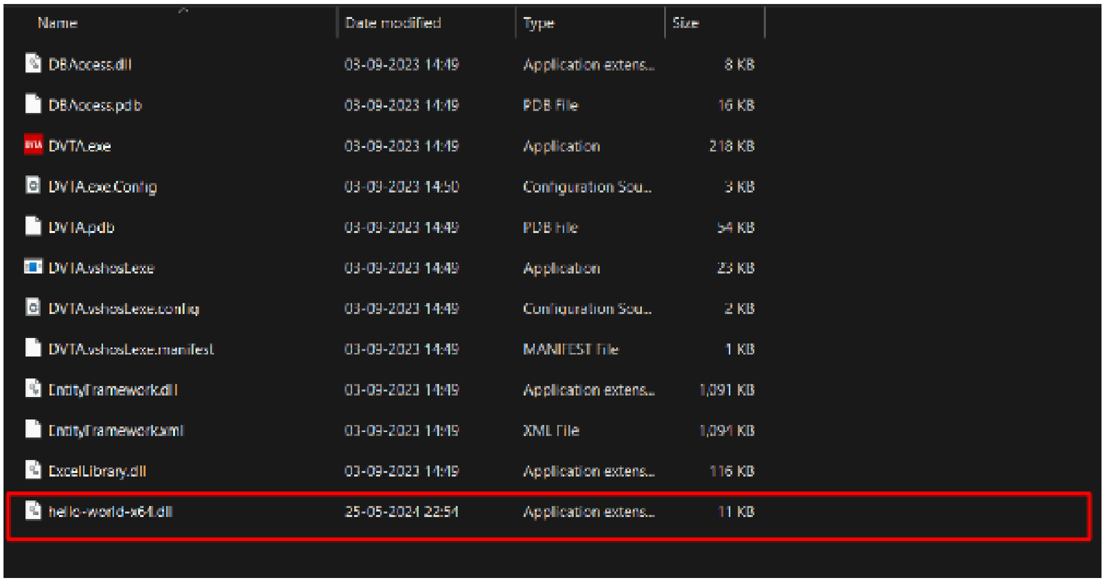
Methodology: Run ProcMon while using the application to log file system activity. Identify files and folders accessed by the application and analyze for sensitive information.

7. Exploit DLL Hijacking vulnerability (You can use a simple legitimate "Hello World" printing DLL)

- Identify DLLs loaded by the application using Dependency Walker.
- Replace a vulnerable DLL with a crafted DLL to test if the application loads it, demonstrating hijacking.

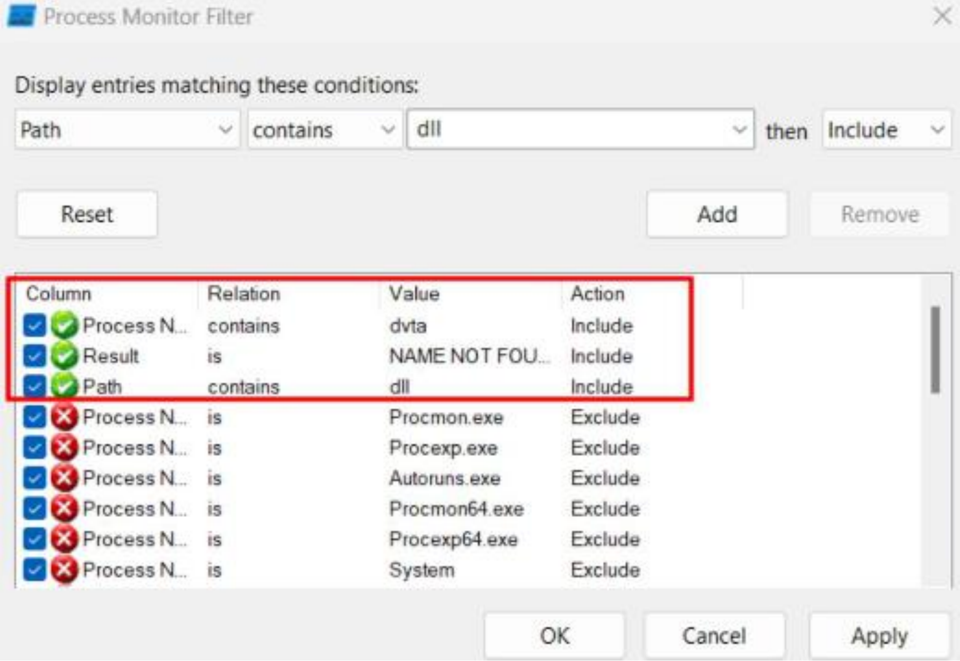
In order to hijack a DLL, we need to find which DLL's that are being loaded when the DVTA.exe run is not found

For this we need to open Promon & set the following 3 filters



Name	Date modified	Type	Size
DBAccess.dll	03-09-2023 14:49	Application extens...	8 KB
DBAccess.pdb	03-09-2023 14:49	PDB File	16 KB
DVTA.exe	03-09-2023 14:49	Application	218 KB
DVTA.exe.Config	03-09-2023 14:50	Configuration Sou...	3 KB
DVTA.pdb	03-09-2023 14:49	PDB File	54 KB
DVTA.vshost.exe	03-09-2023 14:49	Application	23 KB
DVTA.vshost.exe.config	03-09-2023 14:49	Configuration Sou...	2 KB
DVTA.vshost.exe.manifest	03-09-2023 14:49	MANIFEST File	1 KB
EntityFramework.dll	03-09-2023 14:49	Application extens...	1,091 KB
EntityFramework.xml	03-09-2023 14:49	XML File	1,091 KB
ExcelLibrary.dll	03-09-2023 14:49	Application extens...	116 KB
hello-world-x64.dll	25-05-2024 22:54	Application extens...	11 KB

Now Start the Process Monitor Filter



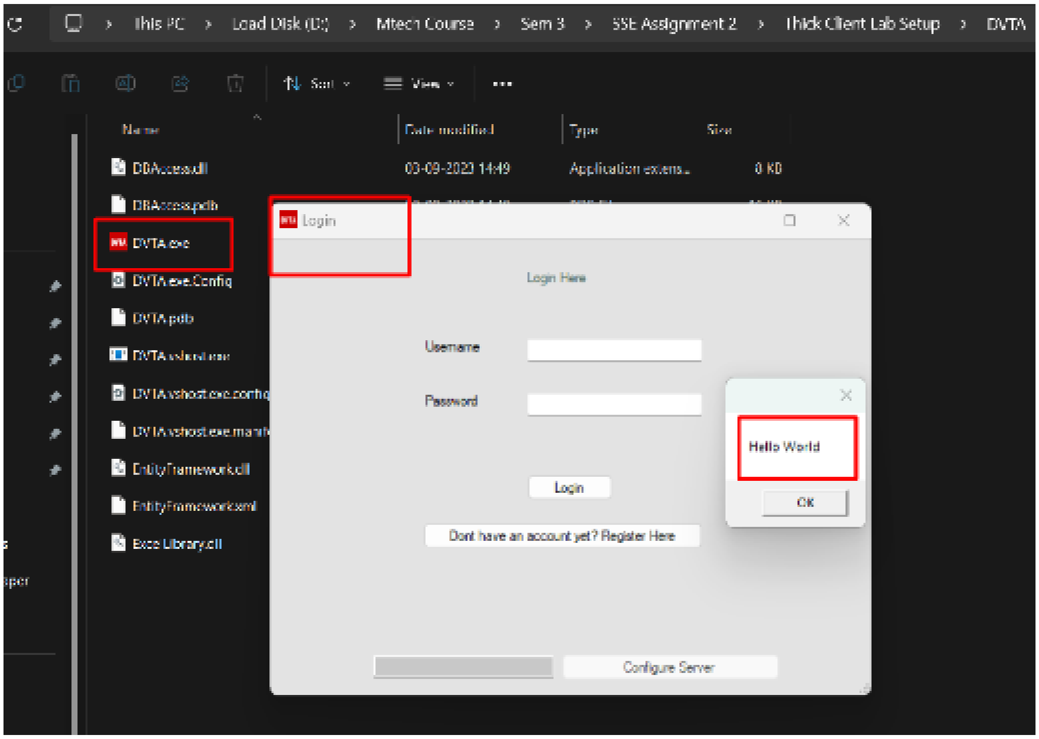
Process Monitor Filter

Display entries matching these conditions:

Path contains dll then Include

Column	Relation	Value	Action
☑ ✓ Process N...	contains	dvta	Include
☑ ✓ Result	is	NAME NOT FOU...	Include
☑ ✓ Path	contains	dll	Include
☑ ✗ Process N...	is	Procmon.exe	Exclude
☑ ✗ Process N...	is	Procexp.exe	Exclude
☑ ✗ Process N...	is	Autoruns.exe	Exclude
☑ ✗ Process N...	is	Procmon64.exe	Exclude
☑ ✗ Process N...	is	Procexp64.exe	Exclude
☑ ✗ Process N...	is	System	Exclude

When we click DVTA.exe automatically Hello World pops up and will appear with opening of the DVTA Login Page



This PC > Load Disk (D:) > Mtech Course > Sem 3 > SSE Assignment 2 > Thick Client Lab Setup > DVTA

Name	Date modified	Type	Size
DBAccess.dll	03-09-2023 14:49	Application extens...	8 KB
DBAccess.pdb			
DVTA.exe			
DVTA.exe.Config			
DVTA.pdb			
DVTA.vshost.exe			
DVTA.vshost.exe.config			
DVTA.vshost.exe.manif			
EntityFramework.dll			
EntityFramework.xml			
Excel Library.dll			

Hello World

As we can observe that now when the DVTA.exe runs, it loads our calc.dll along with the application. Thus we have hijacked the DLL.

POC:

Tools: Dependency Walker, Process Monitor.

Methodology: Identify DLLs loaded by the application. Replace a vulnerable DLL with a malicious one (e.g., a DLL that prints "Hello World") to exploit the hijacking vulnerability.

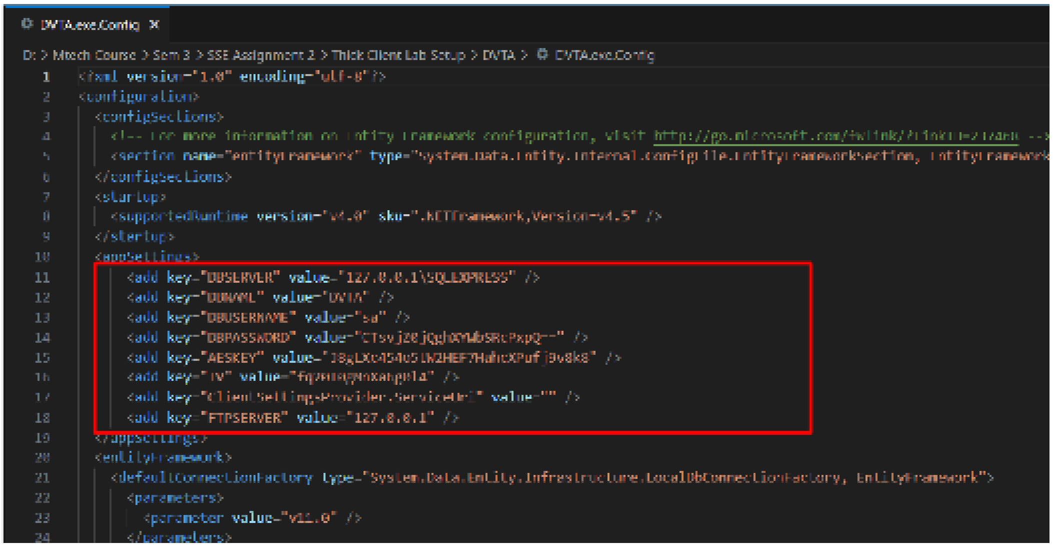
8. Check for sensitive information in the configuration files of the thick client application?

- Locate and open all configuration files associated with the application.
- Manually or using scripts, search for sensitive information such as plaintext passwords and API keys.

In the folder of DVTA, we have few files.

One of the files is App.config

It contains the following sensitive information (Have to open Visual Studio and analyze DVTA.exe.config)


DVTA.exe.Config ✕
D: > Mtech Course > Sem 3 > SSE Assignment 2 > Thick Client Lab Setup > DVTA > DVTA.exe.Config

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <configSections>
    <!-- For more information on Entity Framework configuration, visit http://go.microsoft.com/fwlink/?LinkID=237468 --
    <section name="entityFramework" type="System.Data.Entity.Internal.ConfigFile.EntityFrameworkSection, EntityFramework
  </configSections>
  <startup>
    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5" />
  </startup>
  <appSettings>
    <add key="DBSERVER" value="127.0.0.1\SQLEXPRESS" />
    <add key="DBNAME" value="DVTA" />
    <add key="DBUSERNAME" value="sa" />
    <add key="DBPASSWORD" value="CTsvjZ0jQghXYWbSRcPxpQ==" />
    <add key="AESKEY" value="J8gLXc454o5tW2HEF7HahcXPufj9v8k8" />
    <add key="IV" value="fq2i0pe8maxnqp1a" />
    <add key="ClientSettingsProvider.ServiceUri" value="" />
    <add key="FTPSERVER" value="127.0.0.1" />
  </appSettings>
  <entityFramework>
    <defaultConnectionFactory type="System.Data.Entity.Infrastructure.LocalDbConnectionFactory, EntityFramework">
      <parameters>
        <parameter value="v11.0" />
      </parameters>
```

POC:

Tools: Text editors, Config file analyzers.

Methodology: Locate and inspect configuration files (e.g., .config, .ini, .xml) for sensitive information such as passwords, connection strings, and other credentials.

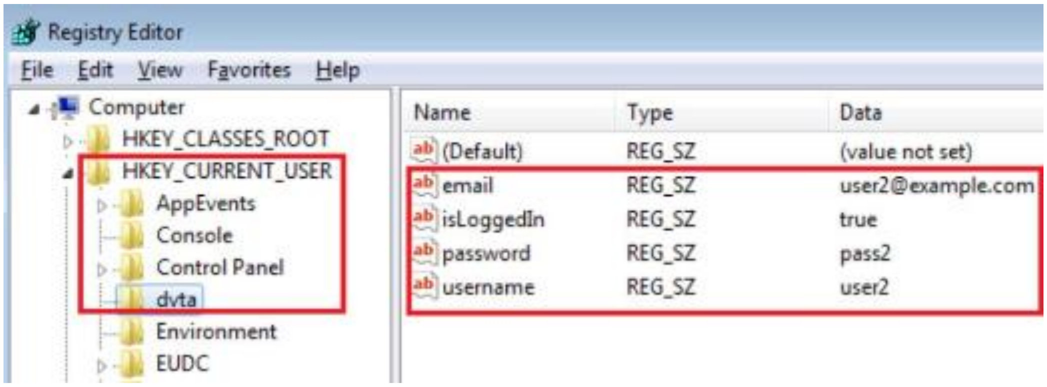
9. Identify sensitive information found in memory?

- Use Process Explorer to dump the memory of the running application.
- Analyze the memory dump with the Volatility Framework to find sensitive information like encryption keys and passwords.

From the Source code which we got from the DNSpy, we got to know that it stores the username and password in HKCU/dvta registry file

We can visit the registry to find the sensitu=ive information which is stored in the memory

We have to open registry editor to analyze dvta username and password



Name	Type	Data
(Default)	REG_SZ	(value not set)
email	REG_SZ	user2@example.com
isLoggedIn	REG_SZ	true
password	REG_SZ	pass2
username	REG_SZ	user2

POC:

Tools: Process Explorer, Volatility Framework.

Methodology: Use memory analysis tools to dump and inspect the application's memory while it is running. Look for sensitive information such as passwords, personal data, and encryption keys.