SQL Connection Encryption

โดยใช้ **Self sign Cert**

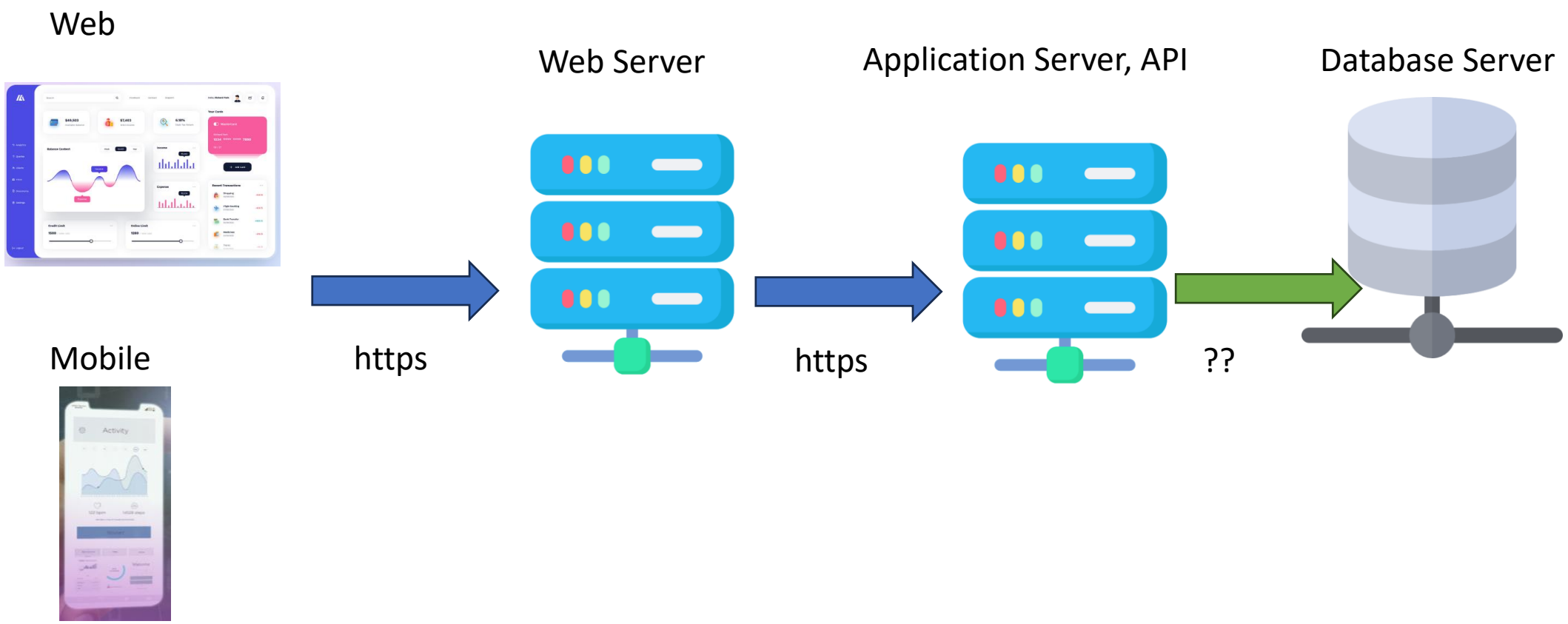
การทดสอบด้วย **Wireshark**

ว่า **Encrypt** กับ ไม่ **Encrypt** ถ้าโดย **Sniff** เป็นยังไง

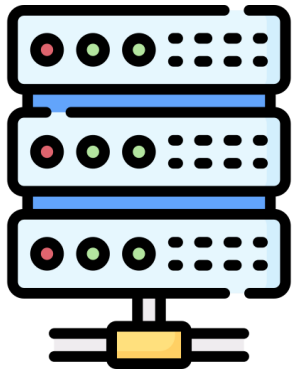
เนื้อหา

- Why need Connection Encryption
- Setup Self sign cert for SQL Connection Encryption
- Setup SQL Server Encryption Config
- Demo
  - Wireshark
  - Java application
- Best practices

Basic Application



Why need connection Encryption



SQL Client

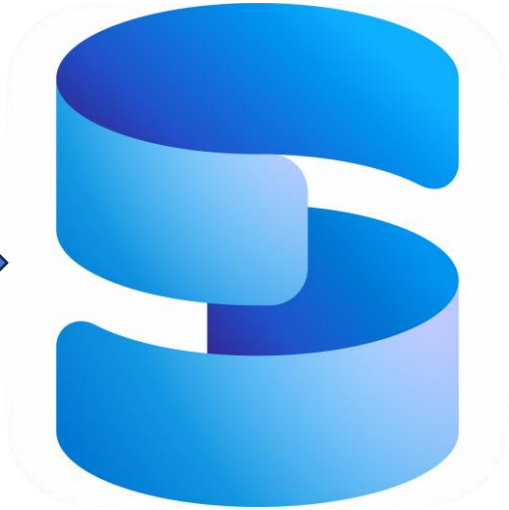
select * from

TCP:1433

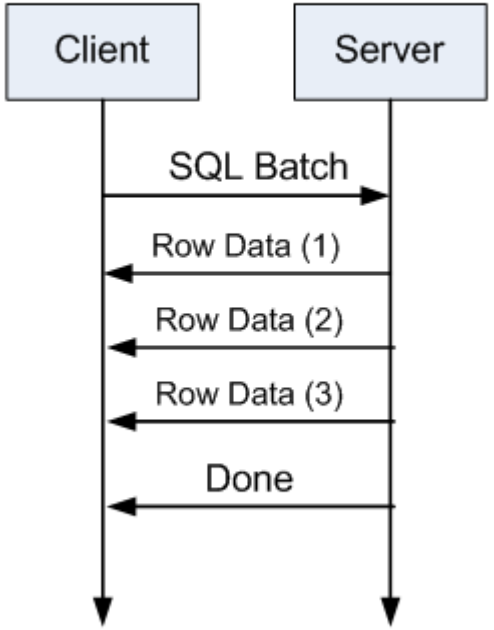
TDS

result

Microsoft SQL Server



Normal TDS Sequence

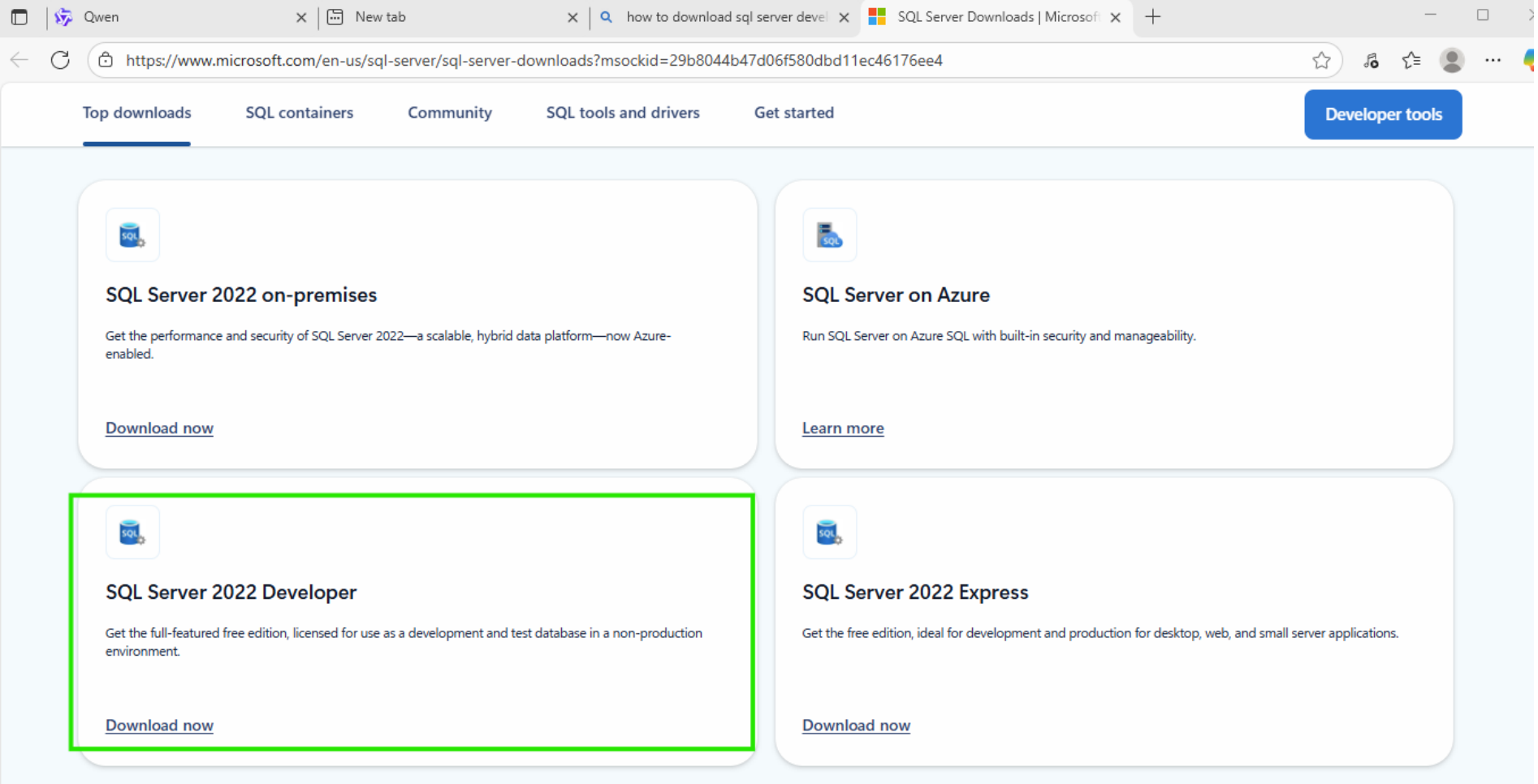


Tools and Basic Knowledge

- Tools:
  - SQL Server Installation
  - SQL Management Studio
  - VS Code
  - Wireshark
- Knowledge
  - Basic SQL
  - Basic Encryption
  - Basic Software Developement
  - Basic Java development
  - Basic Network

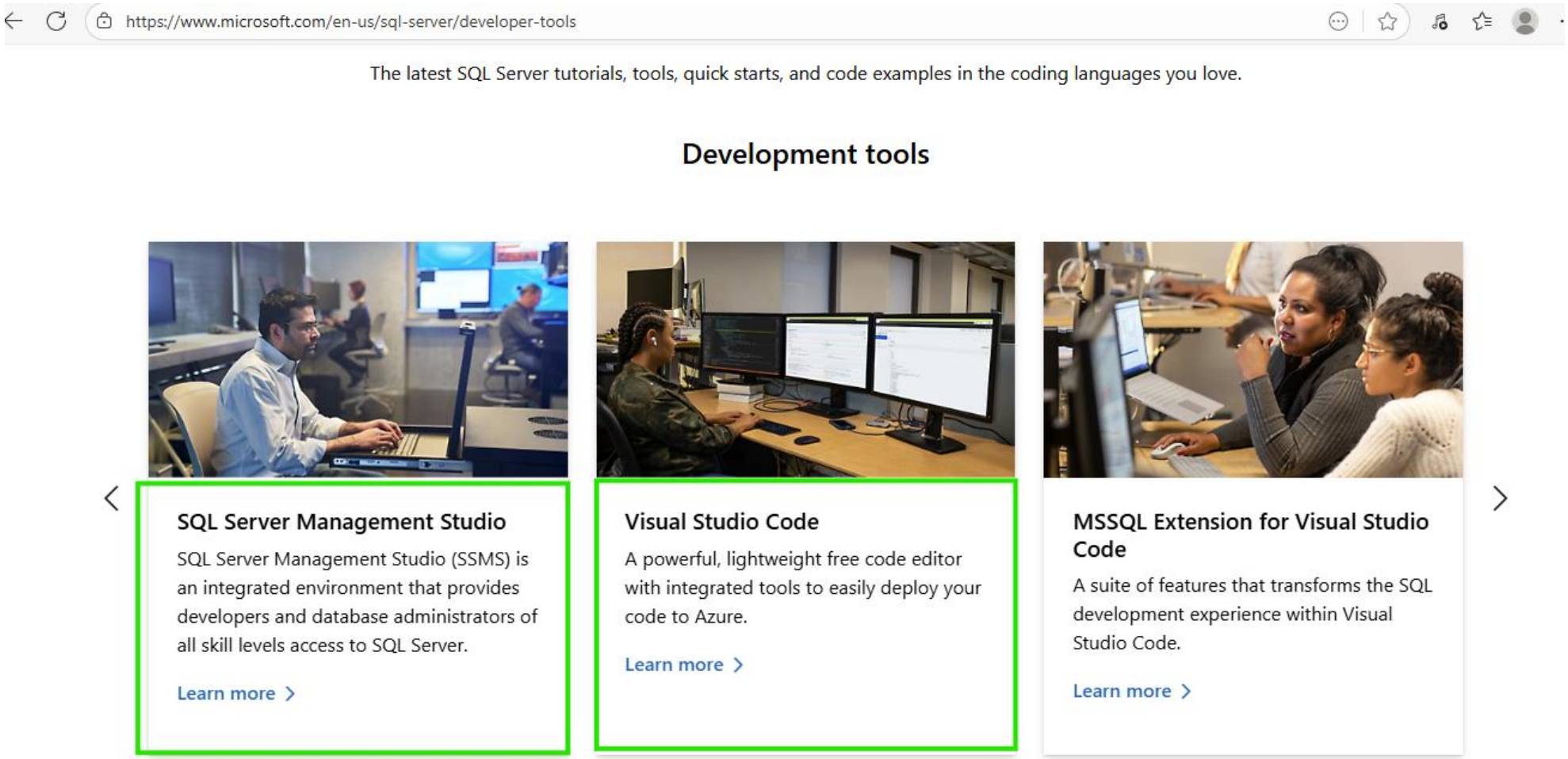
How to download

- https://www.microsoft.com/en-us/sql-server/sql-server-downloads



Tools

- https://www.microsoft.com/en-us/sql-server/developer-tools

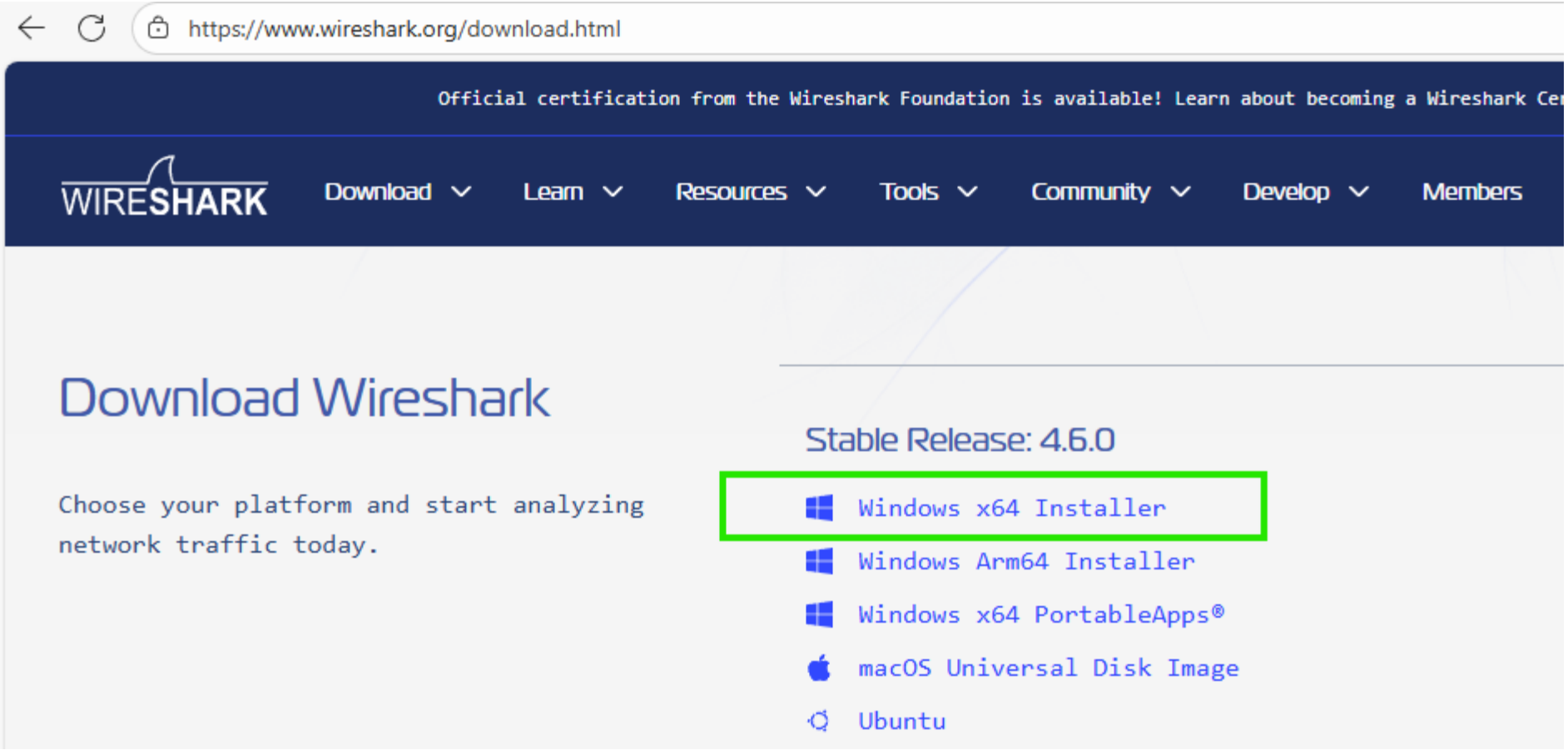


JDBC

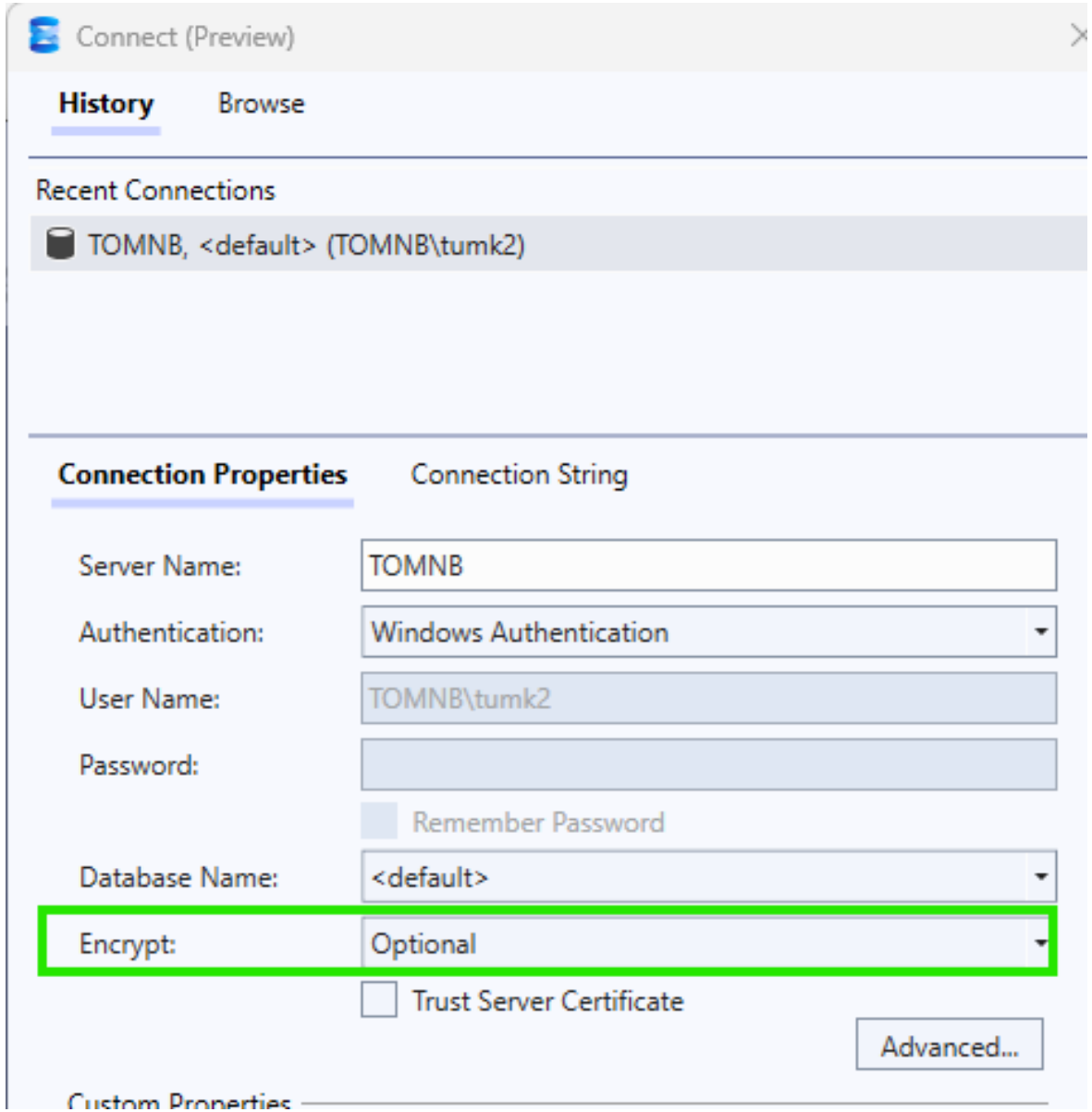
- https://learn.microsoft.com/en-us/sql/connect/jdbc/download-microsoft-jdbc-driver-for-sql-server?view=sql-server-ver17

Wireshark

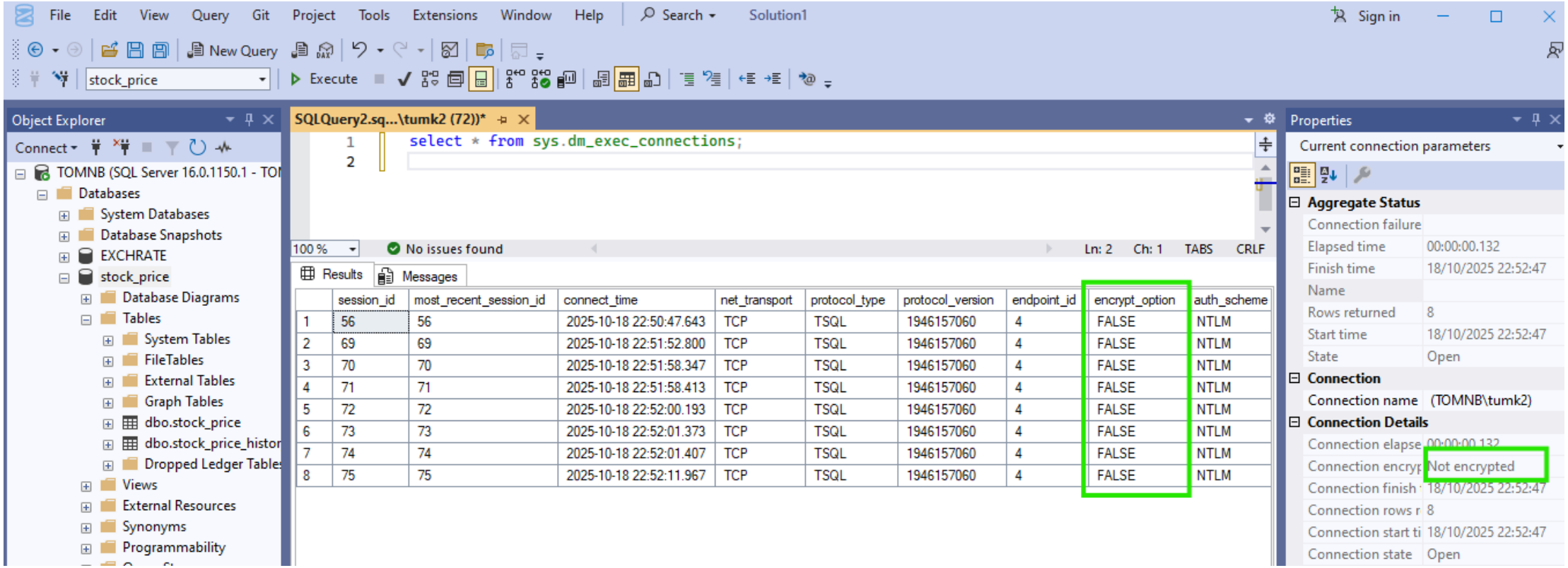
https://www.wireshark.org/download.html



ทดสอบเชื่อมต่อ plaintext

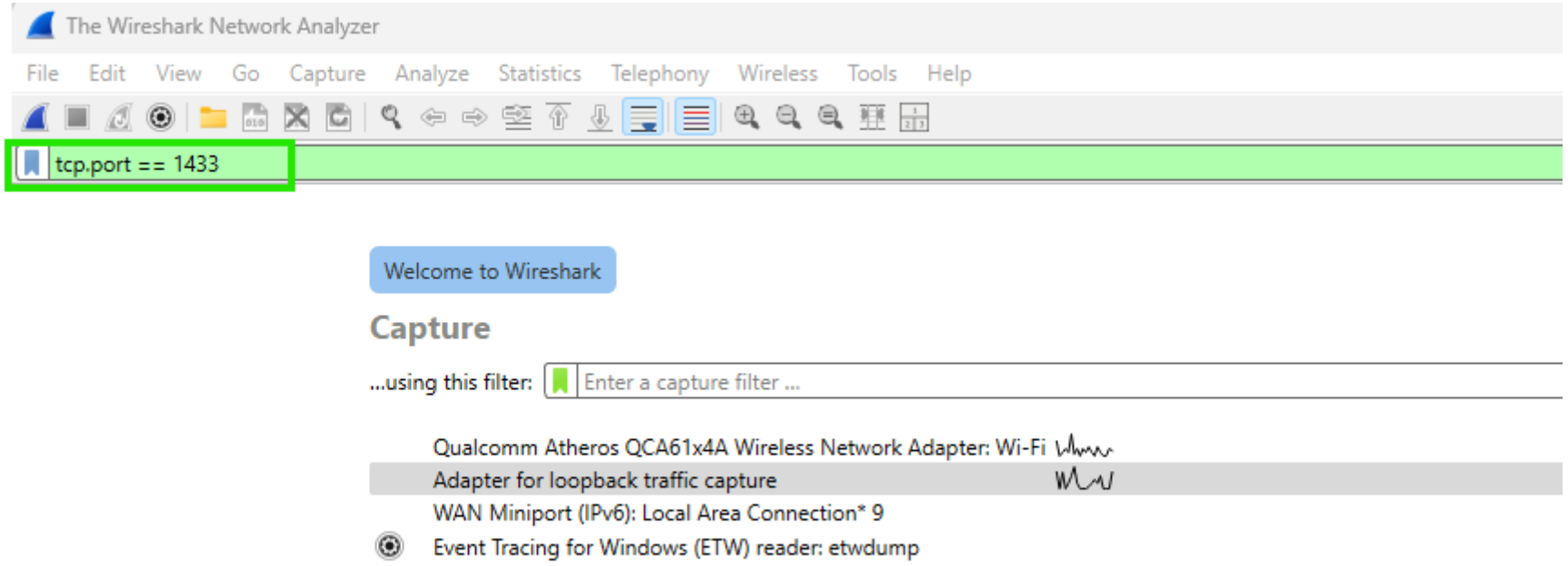


Encryption = Optional



Wireshark

- tcp.port==1433



Example Query

```
select top 3 * from dbo.stock_price;
```

SQLQuery2.sq...\tumk2 (72))*

```
1  select top 3 * from stock_price.dbo.stock_price;
2
```

100 % No issues found Ln: 1 Ch: 15 TABS CRLF

Results | Messages

	Symbol	Timestamp	Market	SecType	ZPrior	ZOpen	ZHigh	ZLow	ZLast	ZAverage	ZVolume	ZValue	LastUpda
1	1DIV	2025-10-14 16:21:10.047	SET	ETF	10.9800	NULL	10.9000	10.8000	10.8000	10.8314	NULL	NULL	2025-10-
2	1I01BSET50	2025-10-14 16:35:16.280	SET	ETF	4.9100	NULL	4.9900	4.9200	4.9900	4.9703	NULL	NULL	2025-10-
3	24CS	2025-10-14 16:35:16.197	mai	CS	1.4800	NULL	1.5300	1.4800	1.5200	1.5102	NULL	NULL	2025-10-

Properties

Current connection parameters

Aggregate Status	
Connection failure	
Elapsed time	00:00:00.067
Finish time	18/10/2025 22:56:3
Name	
Rows returned	3
Start time	18/10/2025 22:56:3
State	Open
Connection	
Connection name	(TOMNB\tumk2)
Connection Details	
Connection elapse	00:00:00.067
Connection encryp	Not encrypted

*Adapter for loopback traffic capture

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 1433

No.	Time	Source	Destination	Protocol	Length	Info
30	5.190038	fe80::4a8c:17d8:f69f:2758	fe80::4a8c:17d8:f69f:2758	TDS	204	SQL batch
31	5.190087	fe80::4a8c:17d8:f69f:2758	fe80::4a8c:17d8:f69f:2758	TCP	64	1433 → 57561 [ACK] Seq=1 Ack=141 Win=8420 Len=0
32	5.190343	fe80::4a8c:17d8:f69f:2758	fe80::4a8c:17d8:f69f:2758	TDS	611	Response[Malformed Packet]
33	5.190368	fe80::4a8c:17d8:f69f:2758	fe80::4a8c:17d8:f69f:2758	TCP	64	57561 → 1433 [ACK] Seq=141 Ack=548 Win=8435 Len=0

```
    Acknowledgment Number: 141    (relative ack number)
    Acknowledgment number (raw): 2468037932
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 8420
    [Calculated window size: 8420]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0xe042 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    [Client Contiguous Streams: 1]
    [Server Contiguous Streams: 1]
    TCP payload (547 bytes)
    [PDU Size: 547]
v Tabular Data Stream
    Type: Response (4)
  > Status: 0x01, End of message
    Length: 547
    Channel: 72
    Packet Number: 1
    Window: 0
  > Token - ColumnMetaData
v [Malformed Packet: TDS]
  v [Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]
      [Malformed Packet (Exception occurred)]
      [Severity level: Error]
      [Group: Malformed]
```

```
0030  a8 be f1 7a 93 1b 45 2c  50 18 20 e4 e0 42 00 00   ···z··E, P· ··B··
0040  04 01 02 23 00 48 01 00  81 0d 00 00 00 00 00 00   ···#·H·· ........
0050  00 08 00 a7 32 00 09 04  d0 00 34 06 53 00 79 00   ····2··· ··4·S·y·
0060  6d 00 62 00 6f 00 6c 00  00 00 00 00 09 00 6f 08   m·b·o·l· ......o·
0070  09 54 00 69 00 6d 00 65  00 73 00 74 00 61 00 6d   ·T·i·m·e ·s·t·a·m
0080  00 70 00 00 00 00 00 09  00 a7 0a 00 09 04 d0 00   ·p...... ........
0090  34 06 4d 00 61 00 72 00  6b 00 65 00 74 00 00 00   4·M·a·r· k·e·t···
00a0  00 00 09 00 a7 14 00 09  04 d0 00 34 07 53 00 65   ........ ···4·S·e
00b0  00 63 00 54 00 79 00 70  00 65 00 00 00 00 00 09   ·c·T·y·p ·e......
00c0  00 6c 11 12 04 06 5a 00  50 00 72 00 69 00 6f 00   ·l····Z· P·r·i·o·
00d0  72 00 00 00 00 00 09 00  6c 11 12 04 05 5a 00 4f   r····· l····Z·O
00e0  00 70 00 65 00 6e 00 00  00 00 00 09 00 6c 11 12   ·p·e·n·· ·····l··
00f0  04 05 5a 00 48 00 69 00  67 00 68 00 00 00 00 00   ··Z·H·i· g·h·····
0100  09 00 6c 11 12 04 04 5a  00 4c 00 6f 00 77 00 00   ··l····Z ·L·o·w··
0110  00 00 00 09 00 6c 11 12  04 05 5a 00 4c 00 61 00   ·····l·· ··Z·L·a·
0120  73 00 74 00 00 00 00 00  09 00 6c 11 12 04 08 5a   s·t····· ··l····Z
0130  00 41 00 76 00 65 00 72  00 61 00 67 00 65 00 00   ·A·v·e·r ·a·g·e··
0140  00 00 00 09 00 6c 11 14  02 07 5a 00 56 00 6f 00   ·····l·· ··Z·V·o·
0150  6c 00 75 00 6d 00 65 00  00 00 00 00 09 00 6c 11   l·u·m·e· ......l·
0160  18 02 06 5a 00 56 00 61  00 6c 00 75 00 65 00 00   ···Z·V·a ·l·u·e··
0170  00 00 00 08 00 3d 0a 4c  00 61 00 73 00 74 00 55   ·····=·L ·a·s·t·U
0180  00 70 00 64 00 61 00 74  00 65 00 d2 20 0c 04 00   ·p·d·a·t ·e·· ···
0190  31 44 49 56 08 76 b3 00  00 56 7c 0d 01 03 00 53   1DIV·v·· ·V|····S
01a0  45 54 03 00 45 54 46 05  01 e8 ac 01 00 05 01 c8   ET··ETF· ........
01b0  a9 01 00 05 01 e0 a5 01  00 05 01 e0 a5 01 00 05   ........ ........
01c0  01 1a a7 01 00 76 b3 00  00 67 0d 20 01 d2 20 0c   ·····v·· ·g· ·· ·
01d0  0a 00 31 49 30 31 42 53  45 54 35 30 08 76 b3 00   ··1I01BS ET50·v··
01e0  00 04 5c 11 01 03 00 53  45 54 03 00 45 54 46 05   ··\····S ET··ETF·
01f0  01 cc bf 00 00 05 01 ec  c2 00 00 05 01 30 c0 00   ........ ·····0··
0200  00 05 01 ec c2 00 00 05  01 27 c2 00 00 76 b3 00   ........ ·'···v··
0210  00 67 0d 20 01 d2 20 0c  04 00 32 34 43 53 08 76   ·g· ·· · ··24CS·v
0220  b3 00 00 eb 5b 11 01 03  00 6d 61 69 02 00 43 53   ····[··· ·mai··CS
0230  05 01 d0 39 00 00 05 01  c4 3b 00 00 05 01 d0 39   ···9···· ·;·····9
0240  00 00 05 01 60 3b 00 00  05 01 fe 3a 00 00 76 b3   ····`;·· ···:··v·
0250  00 00 67 0d 20 01 fd 10  00 c1 00 03 00 00 00 00   ··g· ··· ........
0260  00 00 00                                           ···
```

Expert Info (_ws.expert)

Packets: 46 · Displayed: 4 (8.7%) · Dropped: 0 (

Generate Self sign certificate

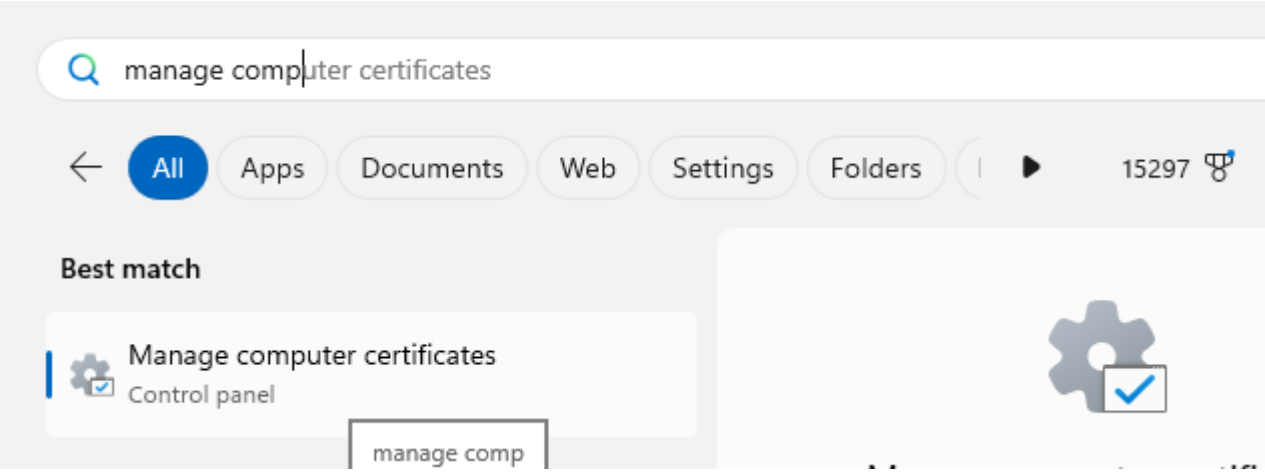
- In test environment
- production ให้ใช้ cert จาก CA ที่เชื่อถือได้

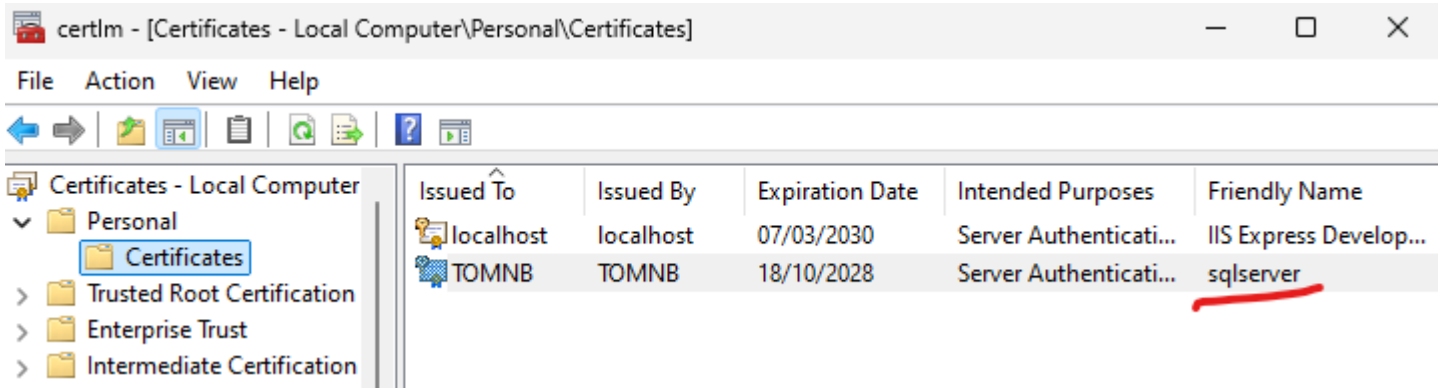
1. PowerShell Administrator
2. ใช้คำสั่ง New-SelfSignedCertificate

Administrator: PowerShell

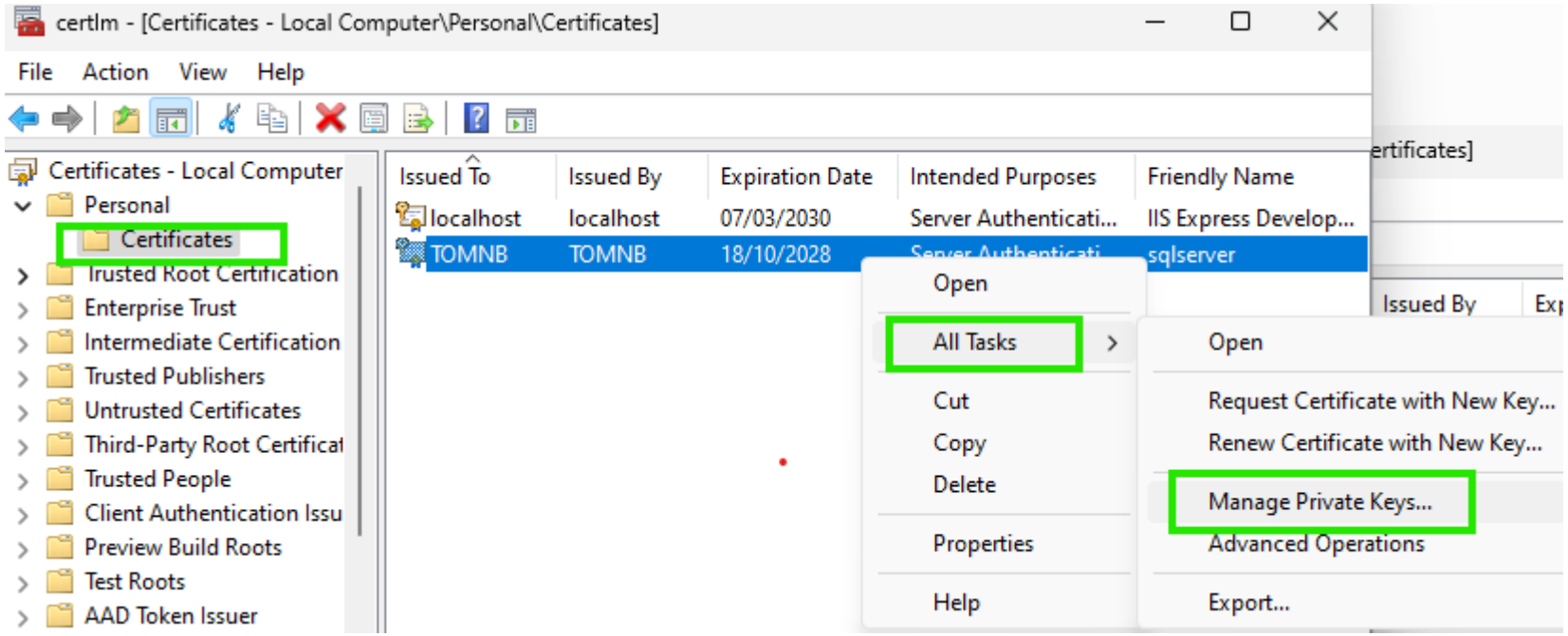
```
PowerShell 7.5.3
PS C:\Users\tumk2> $certificateParams = @{
>>     Type = "SSLServerAuthentication"
>>     Subject = "CN=$env:COMPUTERNAME"
>>     FriendlyName = "sqlserver"
>>     DnsName = @("$($env:COMPUTERNAME)", $([System.Net.Dns]::GetHostEntry('').HostName), 'localhost')
>>     KeyAlgorithm = "RSA"
>>     KeyLength = 2048
>>     HashAlgorithm = "SHA256"
>>     TextExtension = "2.5.29.37={text}1.3.6.1.5.5.7.3.1"
>>     NotAfter = (Get-Date).AddMonths(36)
>>     KeySpec = "KeyExchange"
>>     Provider = "Microsoft RSA SChannel Cryptographic Provider"
>>     CertStoreLocation = "cert:\LocalMachine\My"
>> }
PS C:\Users\tumk2> New-SelfSignedCertificate @certificateParams

   PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\My

Thumbprint                                Subject              EnhancedKeyUsageList
----------                                -------              --------------------
E612A1362091C661DFE293F070B7C86C04E9AE69  CN=TOMNB             Server Authentication
```

Check Certificate

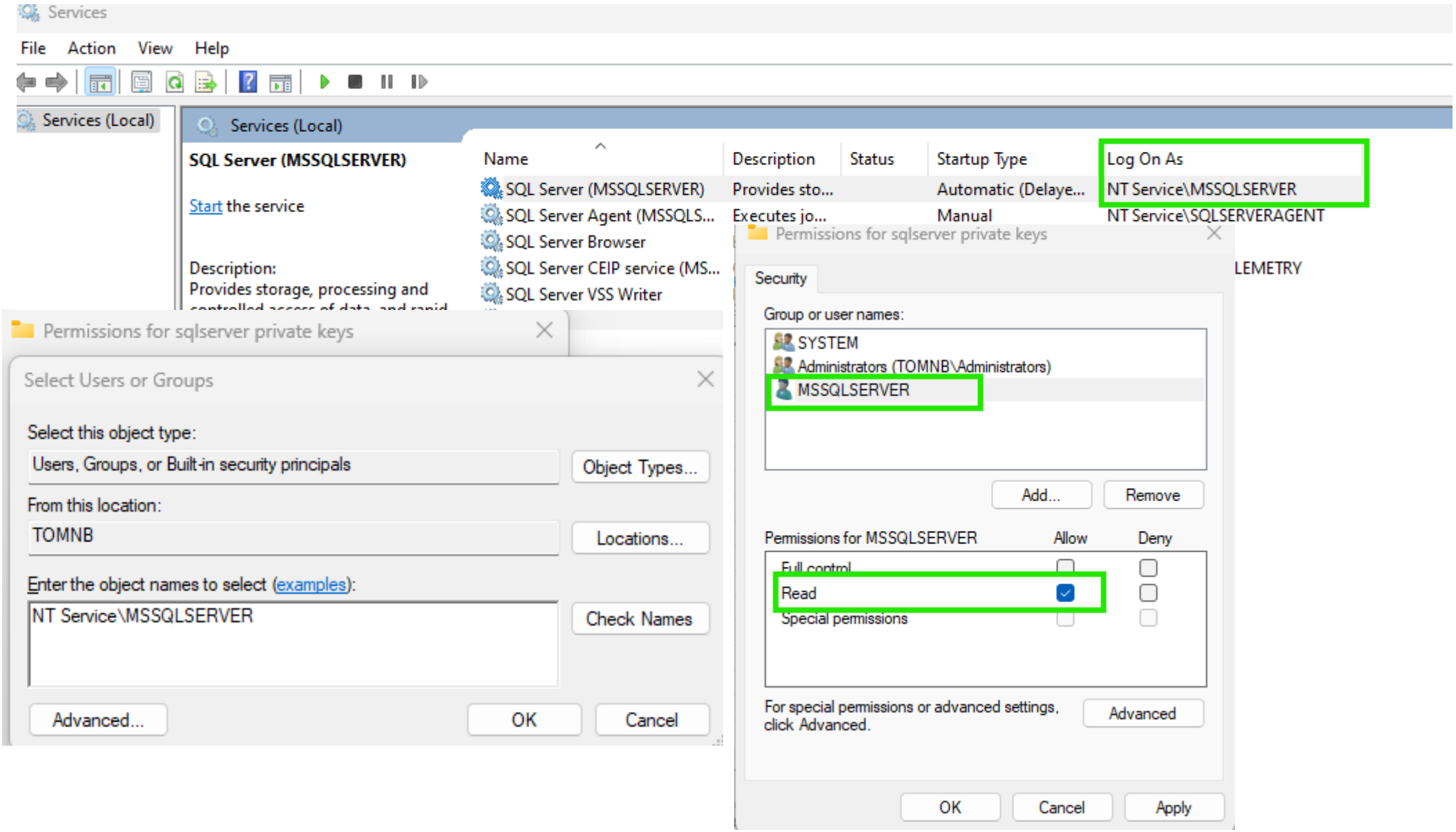




Set Cert Permission

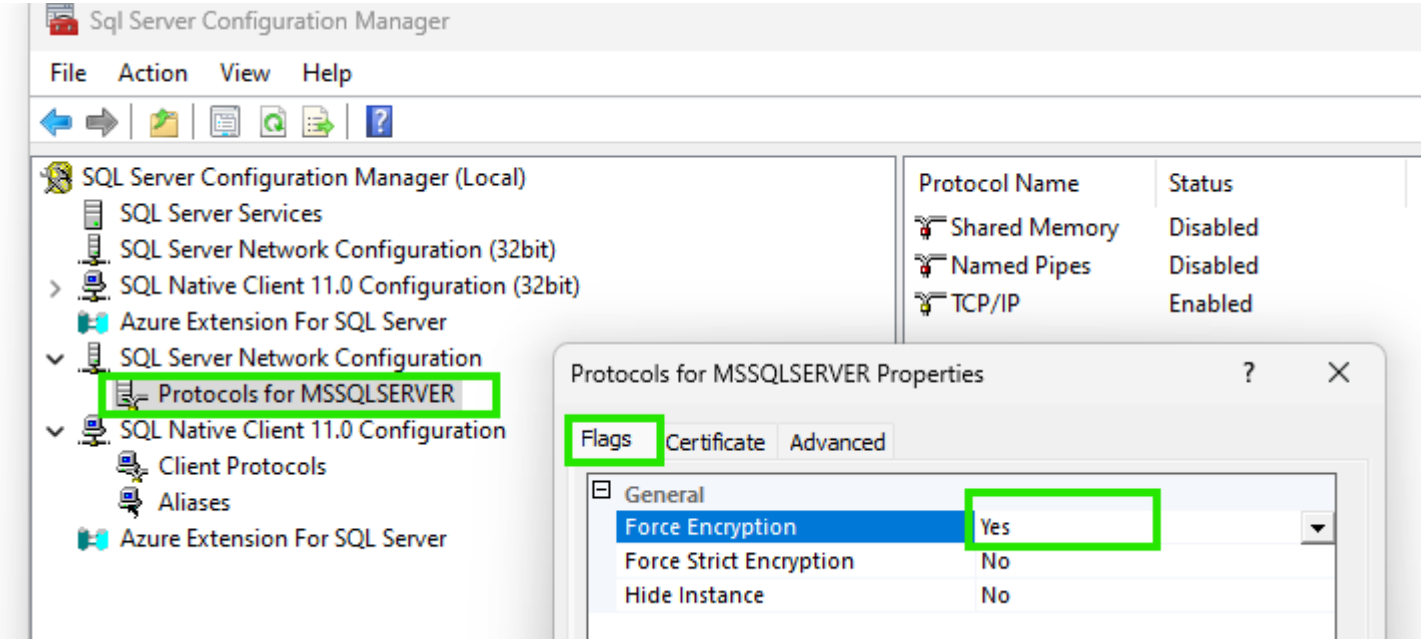


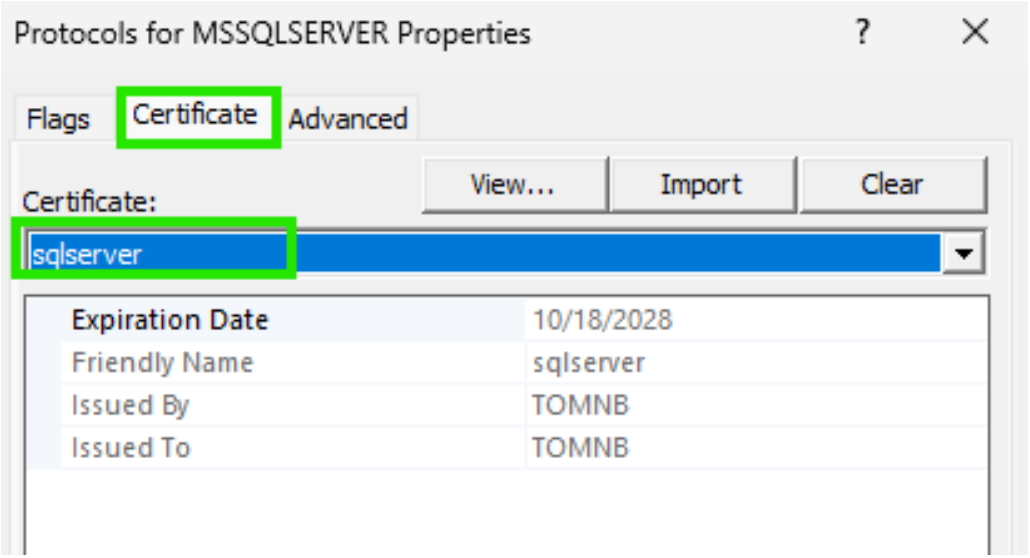
Add Permission Allow Read



Config SQL Server

- SQL Server Configuration Manager
  - Protocols for MSSQLSERVER
    - Flags -> Force Encryption = Yes
    - Certificate -> sqlserver

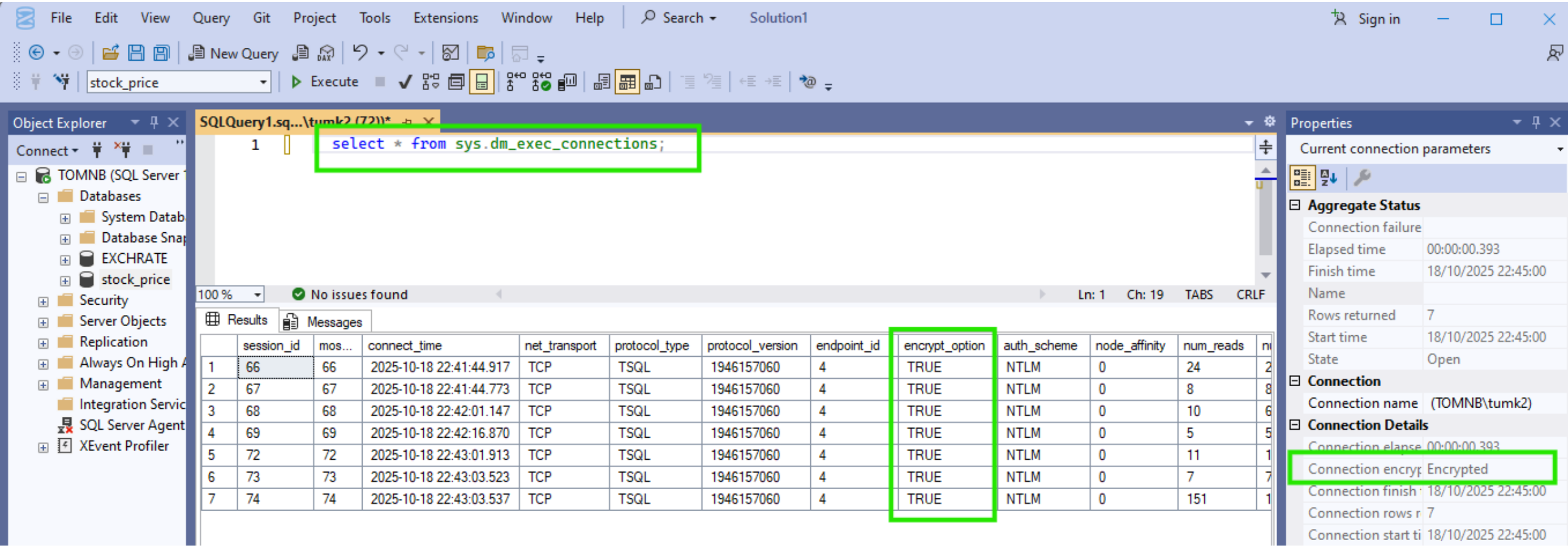




Test Connection

- Via SQL Management Studio

```
select * from sys.dm_exec_connections;
```



	session_id	mos...	connect_time	net_transport	protocol_type	protocol_version	endpoint_id	encrypt_option	auth_scheme	node_affinity	num_reads	n
1	66	66	2025-10-18 22:41:44.917	TCP	TSQL	1946157060	4	TRUE	NTLM	0	24	2
2	67	67	2025-10-18 22:41:44.773	TCP	TSQL	1946157060	4	TRUE	NTLM	0	8	8
3	68	68	2025-10-18 22:42:01.147	TCP	TSQL	1946157060	4	TRUE	NTLM	0	10	6
4	69	69	2025-10-18 22:42:16.870	TCP	TSQL	1946157060	4	TRUE	NTLM	0	5	5
5	72	72	2025-10-18 22:43:01.913	TCP	TSQL	1946157060	4	TRUE	NTLM	0	11	1
6	73	73	2025-10-18 22:43:03.523	TCP	TSQL	1946157060	4	TRUE	NTLM	0	7	7
7	74	74	2025-10-18 22:43:03.537	TCP	TSQL	1946157060	4	TRUE	NTLM	0	151	1

Wireshark on Encryption

*Adapter for loopback traffic capture

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 1433

No.	Time	Source	Destination	Protocol	Length	Info
2	1.033934	fe80::4a8c:17d8:f69f:2758	fe80::4a8c:17d8:f69f:2758	TCP	65	1433 → 63415 [ACK] Seq=1 Ack=1 Win=8371 Len=1
3	1.033951	fe80::4a8c:17d8:f69f:2758	fe80::4a8c:17d8:f69f:2758	TCP	76	63415 → 1433 [ACK] Seq=1 Ack=2 Win=1259 Len=0 SL
4	1.033951	fe80::4a8c:17d8:f69f:2758	fe80::4a8c:17d8:f69f:2758	TCP	65	[TCP Keep-Alive] 63415 → 1433 [ACK] Seq=0 Ack=2
5	1.033962	fe80::4a8c:17d8:f69f:2758	fe80::4a8c:17d8:f69f:2758	TCP	76	[TCP Keep-Alive ACK] 1433 → 63415 [ACK] Seq=2 Ac
32	2.703417	fe80::4a8c:17d8:f69f:2758	fe80::4a8c:17d8:f69f:2758	TLSv1.2	379	Application Data
33	2.703466	fe80::4a8c:17d8:f69f:2758	fe80::4a8c:17d8:f69f:2758	TCP	64	1433 → 54922 [ACK] Seq=1 Ack=316 Win=8420 Len=0
34	2.703713	fe80::4a8c:17d8:f69f:2758	fe80::4a8c:17d8:f69f:2758	TLSv1.2	307	Application Data
35	2.703751	fe80::4a8c:17d8:f69f:2758	fe80::4a8c:17d8:f69f:2758	TCP	64	54922 → 1433 [ACK] Seq=316 Ack=244 Win=8430 Len=

```
    [Stream Packet Number: 1]
  > [Conversation completeness: Incomplete (12)]
    [TCP Segment Len: 315]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3362344167
    [Next Sequence Number: 316    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 1616688639
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 8431
    [Calculated window size: 8431]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x8560 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
    [Client Contiguous Streams: 1]
    [Server Contiguous Streams: 1]
    TCP payload (315 bytes)
    [PDU Size: 315]
v Transport Layer Security
    [Stream index: 0]
  v TLSv1.2 Record Layer: Application Data Protocol: Application Data
      Content Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 310
      Encrypted Application Data [...]: 00000000000000765a3f4794b4a1ea
```

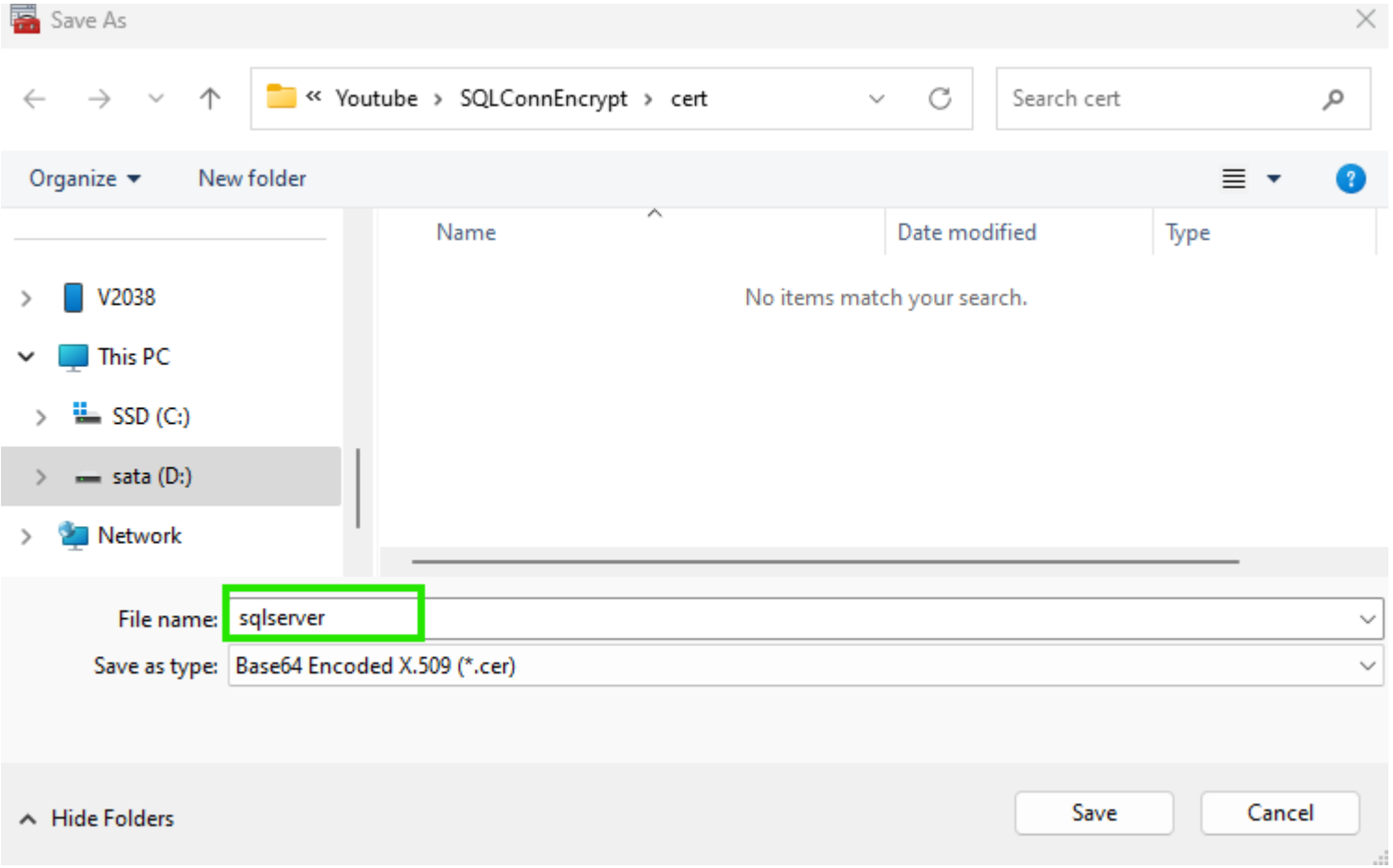
```
0000  18 00 00 00 60 0c 4f 36  01 4f 06 80 fe 80 00 00   ····`·O6 ·O······
0010  00 00 00 00 4a 8c 17 d8  f6 9f 27 58 fe 80 00 00   ····J··· ··'X····
0020  00 00 00 00 4a 8c 17 d8  f6 9f 27 58 d6 8a 05 99   ····J··· ··'X····
0030  c8 69 4c e7 60 5c b5 ff  50 18 20 ef 85 60 00 00   ·iL·`\·· P· ··`··
0040  17 03 03 01 36 00 00 00  00 00 00 00 07 65 a3 f4   ····6··· ·····e··
0050  79 4b 4a 1e a1 0f c7 bc  8d 9d 7d e4 88 43 eb 1a   yKJ····· ··}··C··
0060  76 2d f0 97 ca 25 75 18  6d 60 e7 05 b3 93 29 ce   v-···%u· m`····)·
0070  ad 23 2e 58 db 0d 92 d1  fe 2e cd 27 ba 72 d4 a4   ·#.X···· ·.·'·r··
0080  d9 fc c9 a0 33 c9 ad a0  16 09 2d 13 8c 6e 6c 59   ····3··· ··-··nlY
0090  ee 3c 8a e4 41 7d 2e d8  74 21 68 0b ea 54 7b b6   ·<··A}·· t!h··T{·
00a0  7f 00 93 80 40 8a cf b8  b1 1c b3 e6 d7 43 d1 d7   ····@··· ·····C··
00b0  cc 8b 0e 2a 40 72 69 dd  9d 72 df cb 4a bf fa 54   ···*@ri· ·r··J··T
00c0  cb 73 64 40 17 19 8d e9  3d 4b 20 28 a9 da 65 c3   ·sd@···· =K (··e·
00d0  65 06 ad 23 cf 1f db 35  73 a1 4e 87 71 40 85 71   e··#···5 s·N·q@·q
00e0  71 40 61 5e 6b 8a 84 0e  57 c5 c8 46 91 ee 0b e9   q@a^k··· W··F····
00f0  60 f0 6d 15 0d e6 6d 5e  dc 41 32 3b f9 a8 18 dd   `·m···m^ ·A2;····
0100  1a 46 d3 8a 90 88 e7 28  e9 d5 b8 a5 51 e6 79 1c   ·F·····( ····Q·y·
0110  05 69 f8 0d 85 12 b4 28  76 6a 81 60 49 1e 01 7a   ·i·····( vj·`I··z
0120  e5 d2 ef bc 99 95 be ec  b5 88 df 34 35 63 6c a5   ····· ··· ···45cl·
0130  63 05 72 2d 85 92 eb 68  92 d0 fa 2f 1a 35 d4 4b   c·r-···h ···/·5·K
0140  91 b3 72 1d 29 f1 c9 af  a7 be 2a f8 86 87 07 12   ··r·)··· ··*·····
0150  38 e3 61 ae 27 39 68 5b  c3 a8 3a 94 69 eb e0 3f   8·a·'9h[ ··:·i··?
0160  3e 28 91 4b 41 ba eb 25  84 3c 9a d7 7c 6b f1 e5   >(·KA··% ·<··|k··
0170  19 95 f7 09 20 b3 9d 78  1c d7 28                  ···· ··x ··(
```

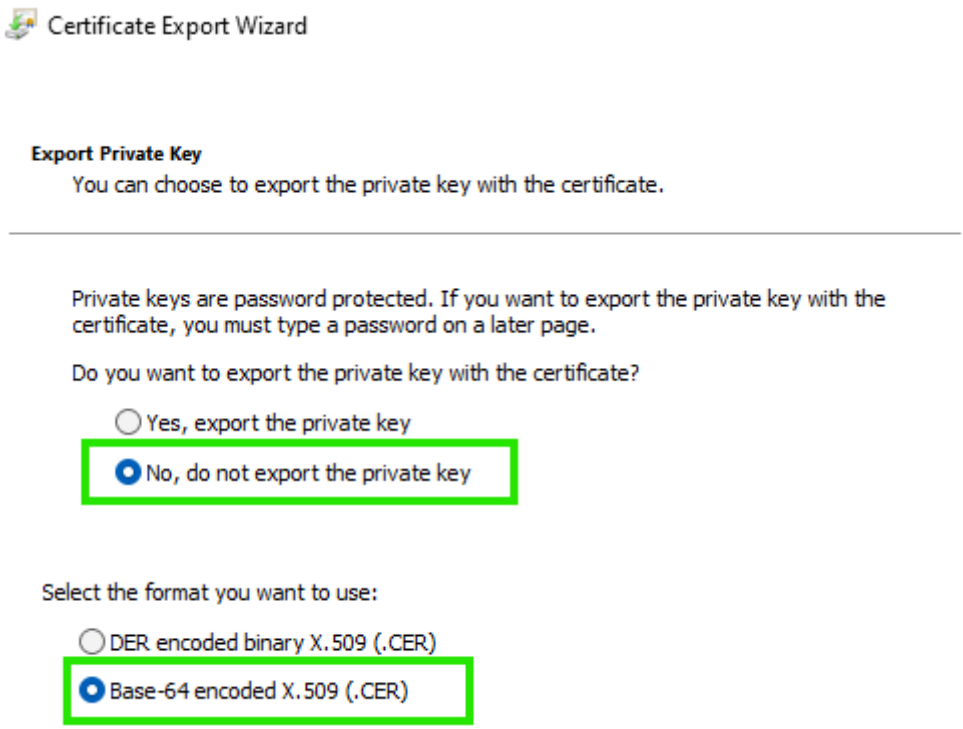
Payload is encrypted application data (tls.app_data), 310 bytes | Packets: 51 · Displayed: 8 (15.7%) · Dropped: 0 (0.0%) | Profile: Default

Java JDBC Config

- Export Cert
- Import cert to trust store (keytools)

Export Cert


Save As
« Youtube › SQLConnEncrypt › cert
Search cert
Organize
New folder
Name
Date modified
Type
No items match your search.
V2038
This PC
SSD (C:)
sata (D:)
Network
File name:
sqlserver
Save as type:
Base64 Encoded X.509 (*.cer)
Hide Folders
Save
Cancel


Certificate Export Wizard
Export Private Key
You can choose to export the private key with the certificate.
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.
Do you want to export the private key with the certificate?
Yes, export the private key
No, do not export the private key
Select the format you want to use:
DER encoded binary X.509 (.CER)
Base-64 encoded X.509 (.CER)

Keytools

```
>keytool -importcert -alias sqlserver -file sqlserver.cer -keystore
truststore.jks -storepass mypass –noprompt
```

Java Code Plain

```java
package client.java;

import java.sql.*;


public class TestPlain {

  public static void main(String[] args) throws Exception {

    String url = "jdbc:sqlserver://TOMNB:1433;databaseName=stock_price; encrypt=false; ";




    try (Connection c = DriverManager.getConnection(url, "stockuser", "!passstock")) {

      try (Statement s = c.createStatement();

           ResultSet rs = s.executeQuery("select top 3 Symbol,Timestamp,ZLast from dbo.stock_price;")) {

        while (rs.next()) System.out.println(rs.getString(1)+","+rs.getString(2)+ ","+rs.getString(3) );

      }

    }

  }

}
```

Java Code Encrypt

```java
package client.java;

import java.sql.*;


public class TestTLS {

  public static void main(String[] args) throws Exception {

    String url = "jdbc:sqlserver://TOMNB:1433;databaseName=stock_price;";
                 + "encrypt=true;trustServerCertificate=true;"
                 + "trustStore=truststore.jks;trustStorePassword=mypass;"
                 + "hostNameInCertificate=TOMNB";
    try (Connection c = DriverManager.getConnection(url, "stockuser", "!passstock")) {

      try (Statement s = c.createStatement();

           ResultSet rs = s.executeQuery("select top 3 Symbol,Timestamp,ZLast from dbo.stock_price;")) {

        while (rs.next()) System.out.println(rs.getString(1)+","+rs.getString(2)+ ","+rs.getString(3) );

      }

    }

  }

}
```

Run Java

- java -cp "mssql-jdbc-12.10.2.jre11.jar" TestPlain.java

- java -cp "mssql-jdbc-12.10.2.jre11.jar" TestTLS.java

ข้อควรรู้ / Best practices

- อย่าใช้ trustServerCertificate=true ใน production
- ใช้ cert จาก CA ที่เชื่อถือได้ (หรือ internal CA ที่แจก trust ไปยังเครื่อง client ทุกตัว)
- ใส่ hostNameInCertificate/ตั้ง SAN ให้ถูกต้อง เพื่อป้องกันการใช้ cert ผิด host
- จัดการ lifecycle ของ cert: หมดอายุ -> renew -> deploy ให้ client ใหม่
- ตรวจสอบ performance / connection pooling เมื่อเปิด TLS
- อย่าส่ง private key ของ server ให้คนอื่น

Reference

- Connection Encrypt

https://learn.microsoft.com/en-us/sql/database-engine/configure-windows/configure-sql-server-encryption?view=sql-server-ver17

- Keytools

https://docs.redhat.com/en/documentation/red_hat_jboss_data_virtualization/6.2/html/security_guide/add_a_certificate_to_a_truststore_using_keytool

- JDBC https://learn.microsoft.com/sql/connect/jdbc/download-microsoft-jdbc-driver-for-sql-server

🎯 Key takeaway

- 🔐 ข้อมูลระหว่างโปรแกรมกับ **SQL Server** อาจถูกดักได้ถ้าไม่เข้ารหัส
- ❓ การเปิดใช้ **Encryption** ช่วยป้องกันการดักฟัง (**Man-in-the-Middle Attack)**
- 🔑 **SQL Server** ใช้ **Certificate** เป็นตัวล็อก-ปลดล็อกข้อมูล
- ⚙️ **Client** และ **Server** ต้องตั้งค่าทั้งคู่
  - ฝั่ง **Server**: เปิด “Force Encryption = Yes”
  - ฝั่ง **Client (Java)**: ตั้งค่า encrypt=true;
- 🧠 **สรุปใจความสำคัญ**:

“การเข้ารหัสการเชื่อมต่อ (Connection Encryption) ไม่ได้ทำให้ระบบเร็วขึ้น แต่ทำให้ข้อมูลที่ส่งผ่านเครือข่ายปลอดภัยขึ้นมาก — ป้องกันการดักจับและขโมยข้อมูลสำคัญ”

ขอบคุณที่รับชม Thanks for watching

แชร์ Subscribe

SQL Connection Encryption

โดยใช้ Self sign Cert

การทดสอบด้วย Wireshark

ว่า Encrypt กับ ไม่ Encrypt ถ้าโดย Sniff เป็นยังไง

https://www.youtube.com/@t-live-code