Encrypt Those Connections!: Setting Up SQL Server to Use Encrypted Connections

Sharon Reid

sharon.reid.harris@gmail.com

https://github.com/InfoJunkie1/EncryptConnections

St. Louis SQL Server and Power BI User Group

11 June 2024

About Me

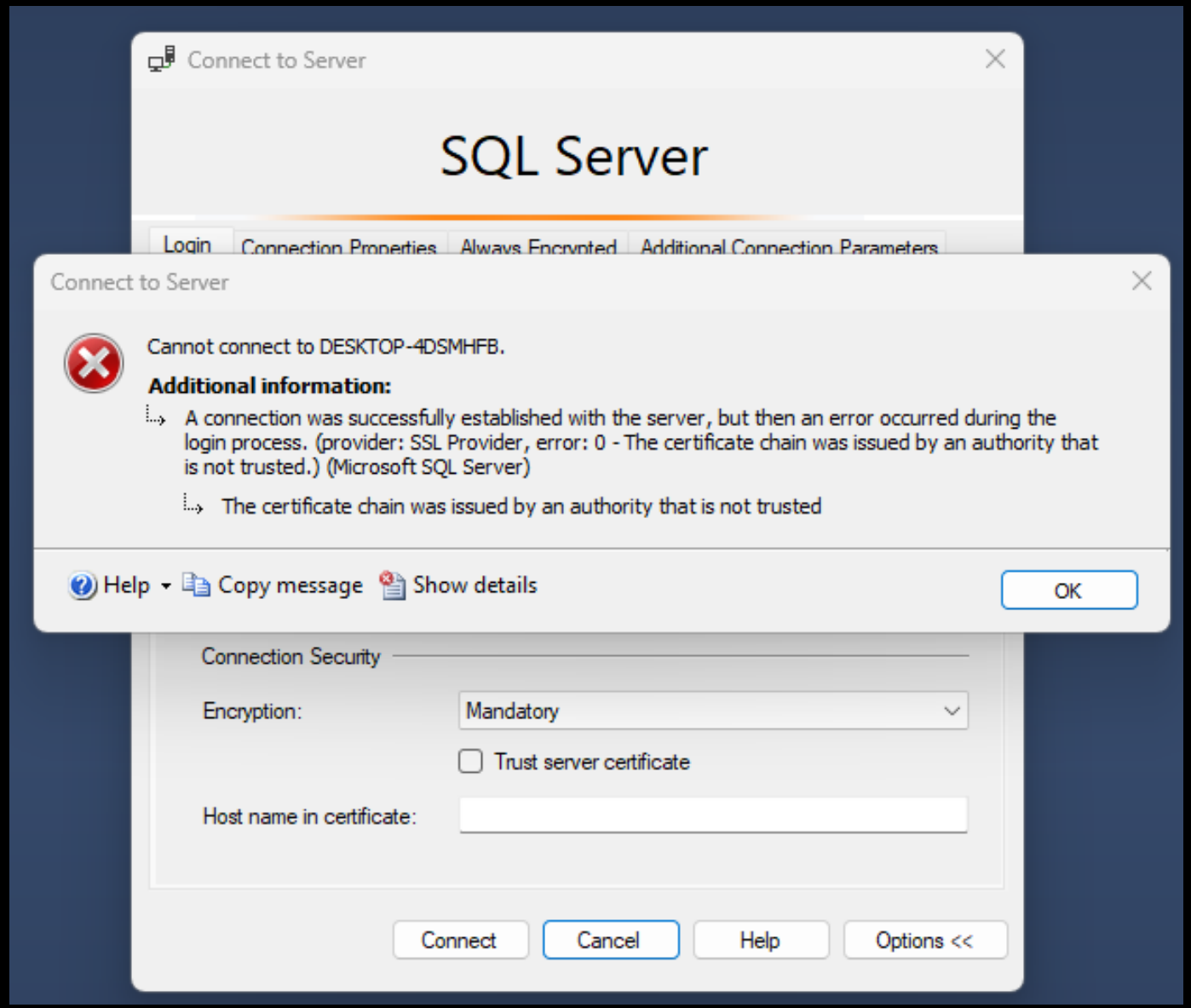
- High school and then college writing instructor
- Needed full-time job!
- Went through LaunchCode SQL cohort
- Hired at NISA!
- Asked to come back and TA and then be a lead mentor
- Passionate about database security

(Everglades)

Expectations

- Not introductory, not in the weeds—passion to help others on the journey to improve database security
- Familiar with SQL Server but haven't yet set up environment to use encrypted connections
- Your friendly DBA is now after you to use encrypted connections, and you want to understand what you're doing

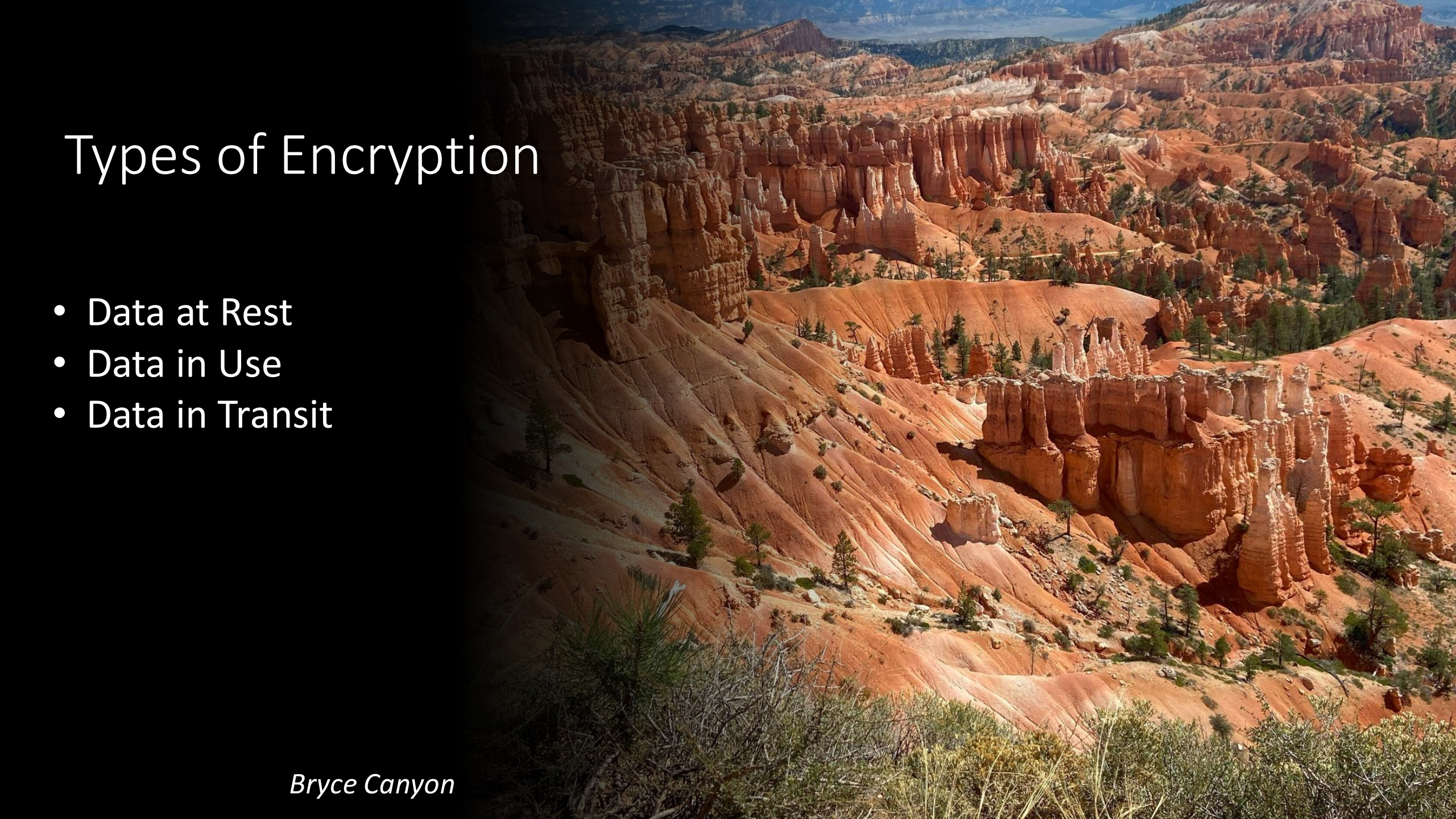
(Yellowstone)


Connect to Server
SQL Server
Login
Connection Properties
Always Encrypted
Additional Connection Parameters
Connect to Server
Cannot connect to DESKTOP-4DSMHFB.
Additional information:
A connection was successfully established with the server, but then an error occurred during the login process. (provider: SSL Provider, error: 0 - The certificate chain was issued by an authority that is not trusted.) (Microsoft SQL Server)
The certificate chain was issued by an authority that is not trusted
Help
Copy message
Show details
OK
Connection Security
Encryption:
Mandatory
Trust server certificate
Host name in certificate:
Connect
Cancel
Help
Options <<

Whaaaatttt?????

Types of Encryption

- Data at Rest
- Data in Use
- Data in Transit



Bryce Canyon

Data at Rest

- Where the database is stored
- TDE (Microsoft encryption option)
- Slight performance hit
- Storage layer partially addresses

Yellowstone—The Narrows

Data in Use

- While data is actively used
- Always Encrypted (Microsoft encryption option)
- Can be by column
- Performance hit

Yellowstone

Data in Transit

- Bytes of information go from one device or system to another
- Inherently vulnerable
- Seal the envelope
- Connection strings
- Slight performance hit—not noticeable
- Best practice!

Zion—Allison Harris at Angel's Landing

SSL

- Secure Sockets Layer
- Used to encrypt data between SQL Server and the client application on the network
- Uses certificates to validate the server
- Used pre SQL Server 2016

Valles Caldera National Preserve, New Mexico

TLS

- SSL>TLS
- Newer version of SSL with increased security
- TLS/SSL handshake
- Microsoft link re authentication

Bryce Canyon

Can we use encrypted connections?

- No—environment not set up
- Sometimes—allows for use of encrypted connections
  - SQL Server security certs required
  - Connection strings updated
- Yes—forces use of encrypted connections
  - Goal!

Allison Harris at Grand Canyon

Create a security cert

- Self-signed
  - Encrypts connection but still must check Trust Server
  - Not signed by a trusted authority
- Company's own cert authority
  - Active Directory domain
- 3rd party Certificate Authority such as DigiCert

(Bryce Canyon)

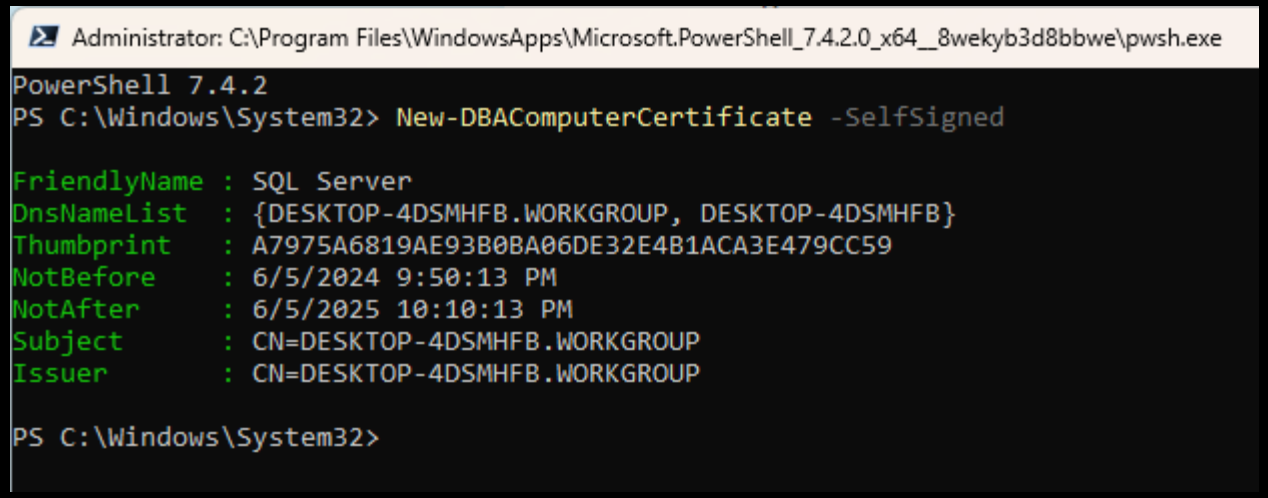
Steps to create a security cert

- Create the cert
- Grant SQL Server rights to read private key
- Configure SQL Server to use this cert

- *(Horseshoe Bend)*

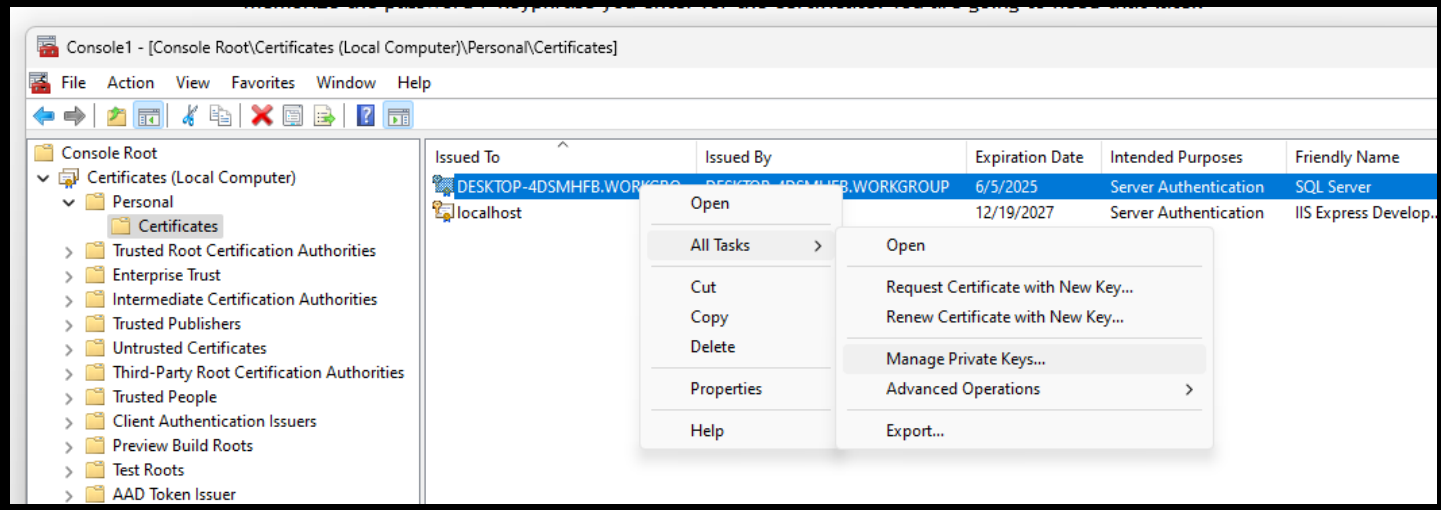
Creating self-signed cert in PowerShell

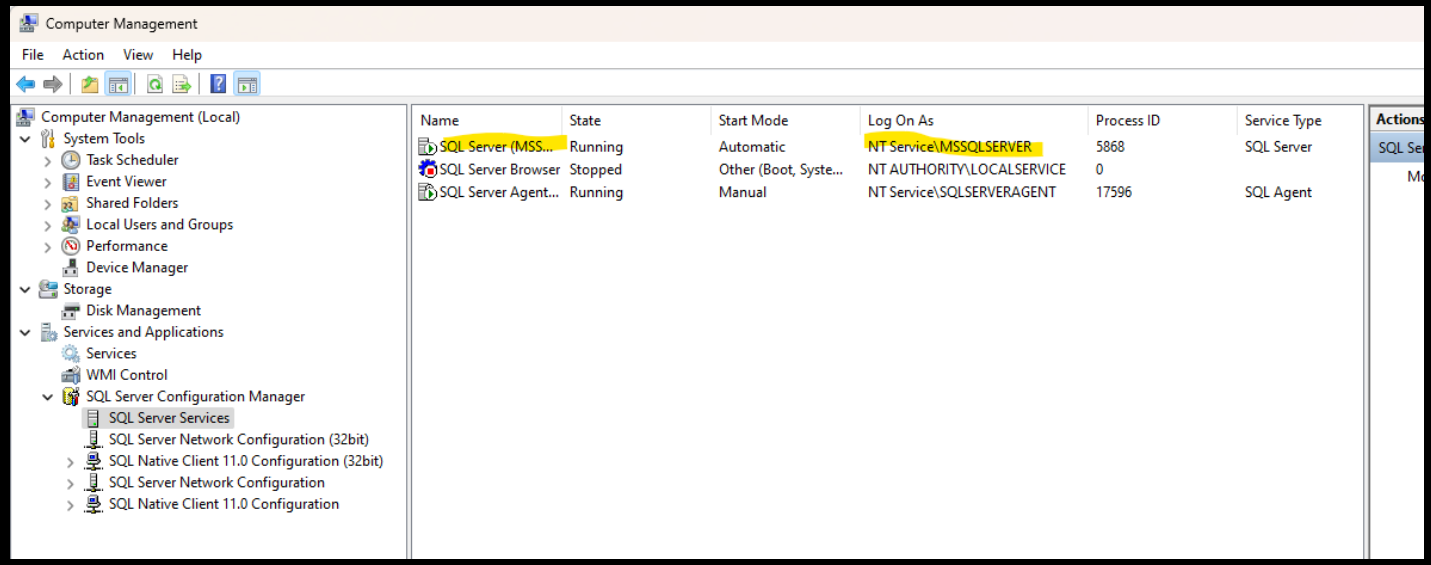
- Use DBATools!



Grant SQL Server rights to read private key

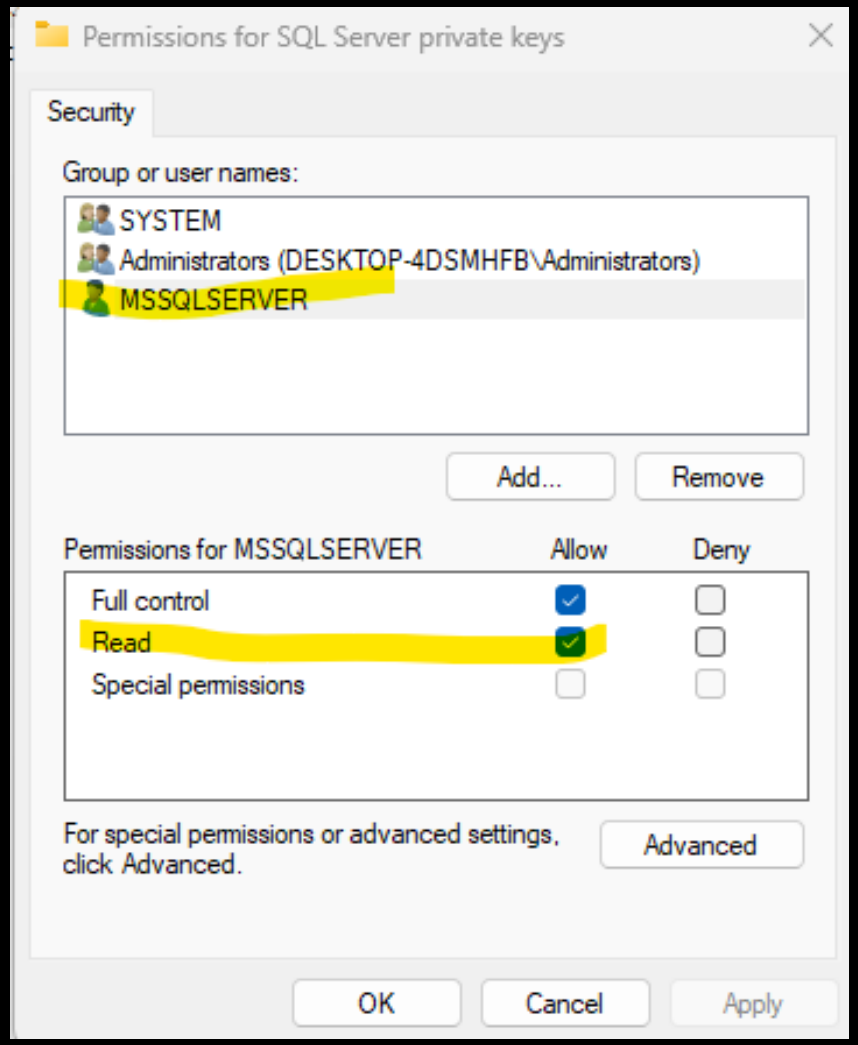
- Super important step!
- SQL Server service can’t start otherwise
- MMC>Personal>Certificates
- Certificate>rt click>All Tasks>Manage Private Keys
- Confirm in Configuration Manager the service account for your instance

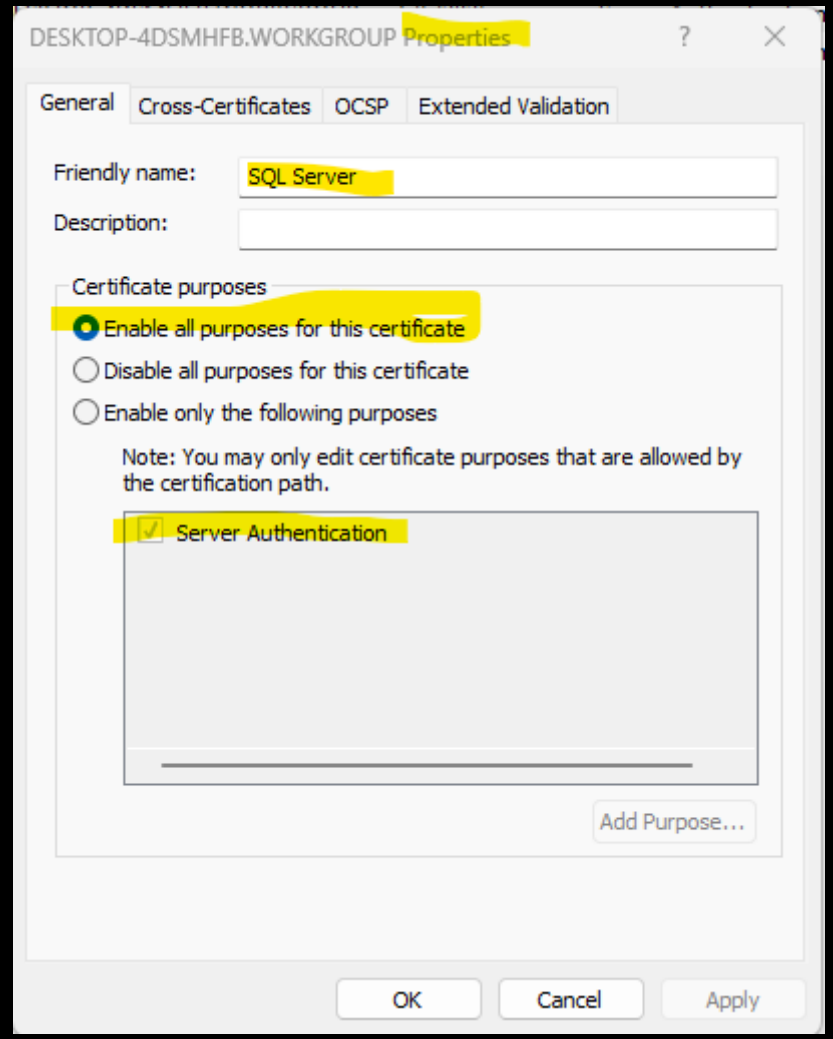




Grant SQL Server rights to read private key (pt. 2)

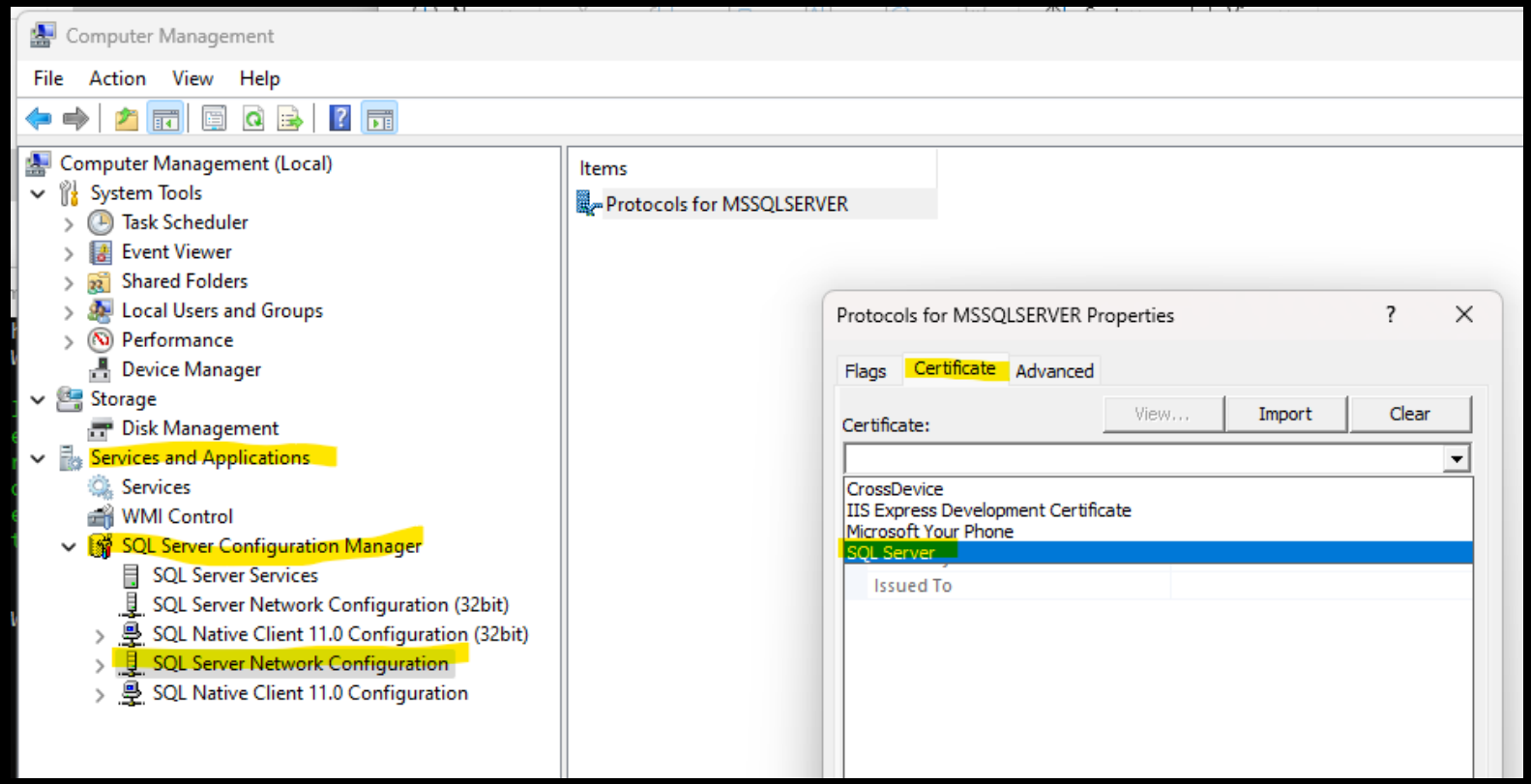
- Give service account Read permissions
- Make sure Server Authentication is selected in Properties

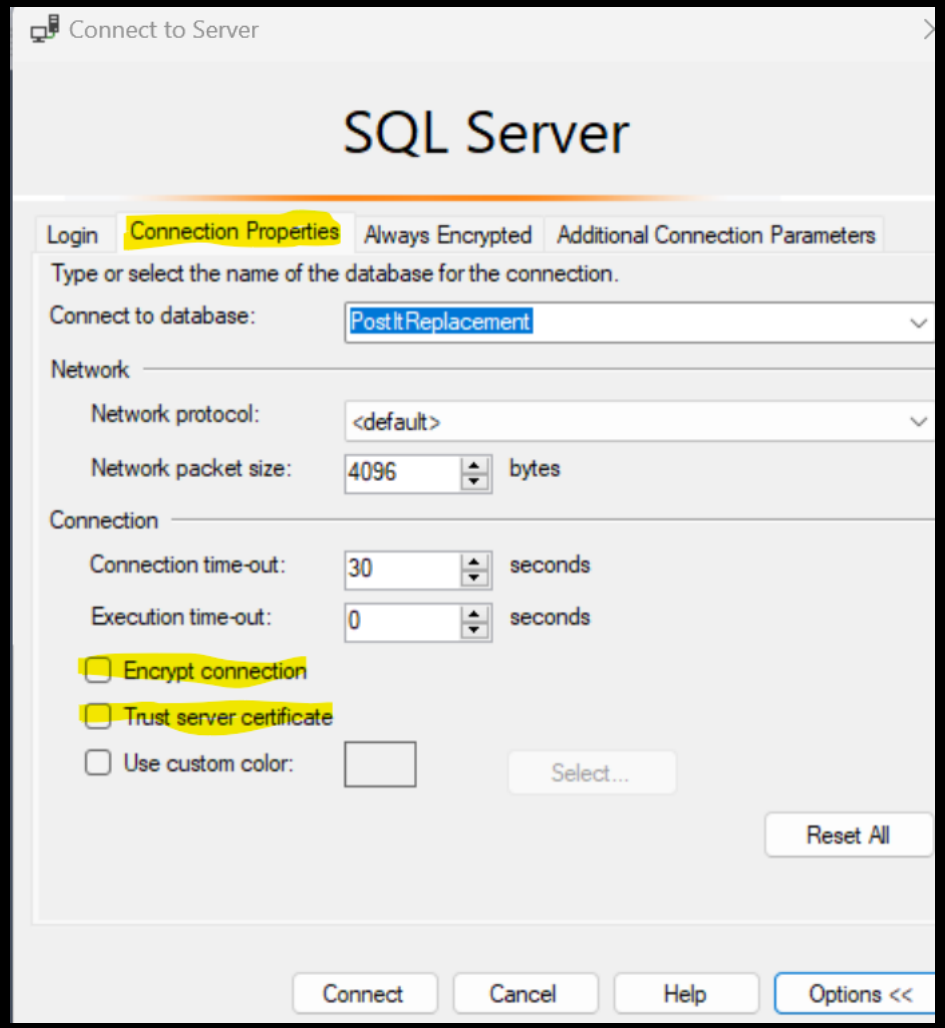




Configure SQL Server to use our new cert

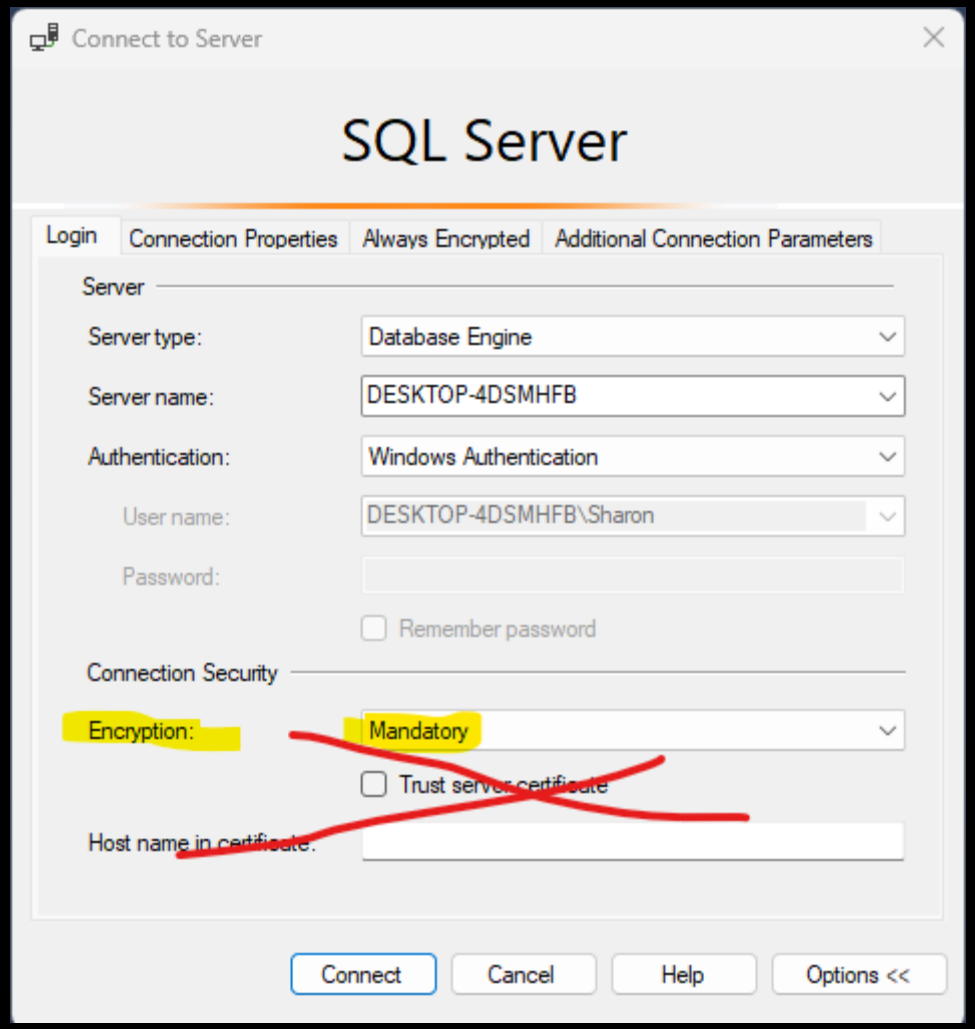
- SQL Server Configuration Manager
- SQL Server Network Configuration
- Select instance
- Rt click>Properties>Certificate
- Choose cert
- Restart service





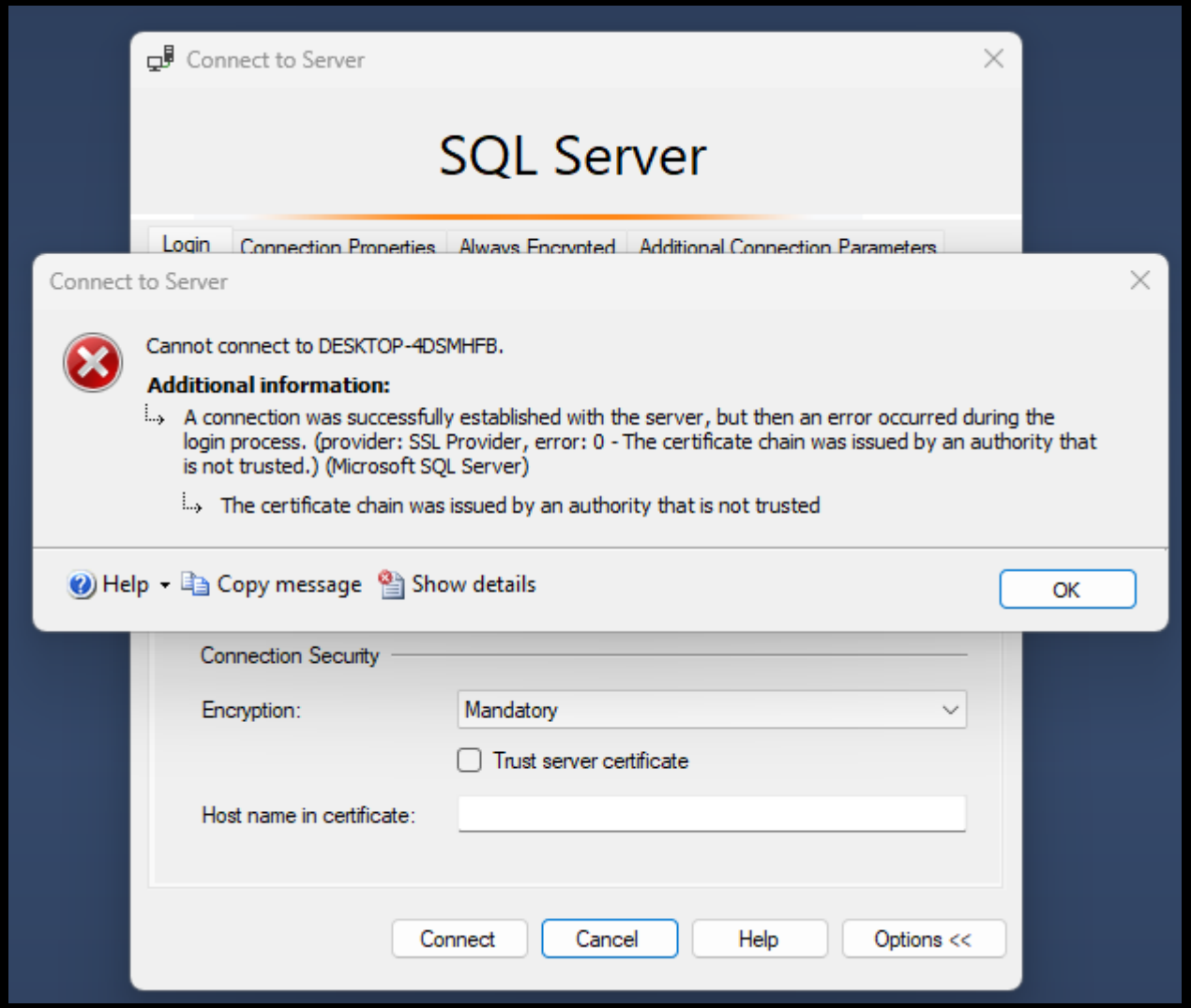
SSMS 18 or 19

- Encryption options on 2nd tab
- Defaults to not using Encrypt Connection
- Offers Trust Server option



SSMS 20

- Moved Encryption checkbox to first tab
- Defaults to Mandatory
  - Means to encrypt that connection
- Offers Trust Server option
  - Not secure
  - Susceptible to man-in-the-middle attacks

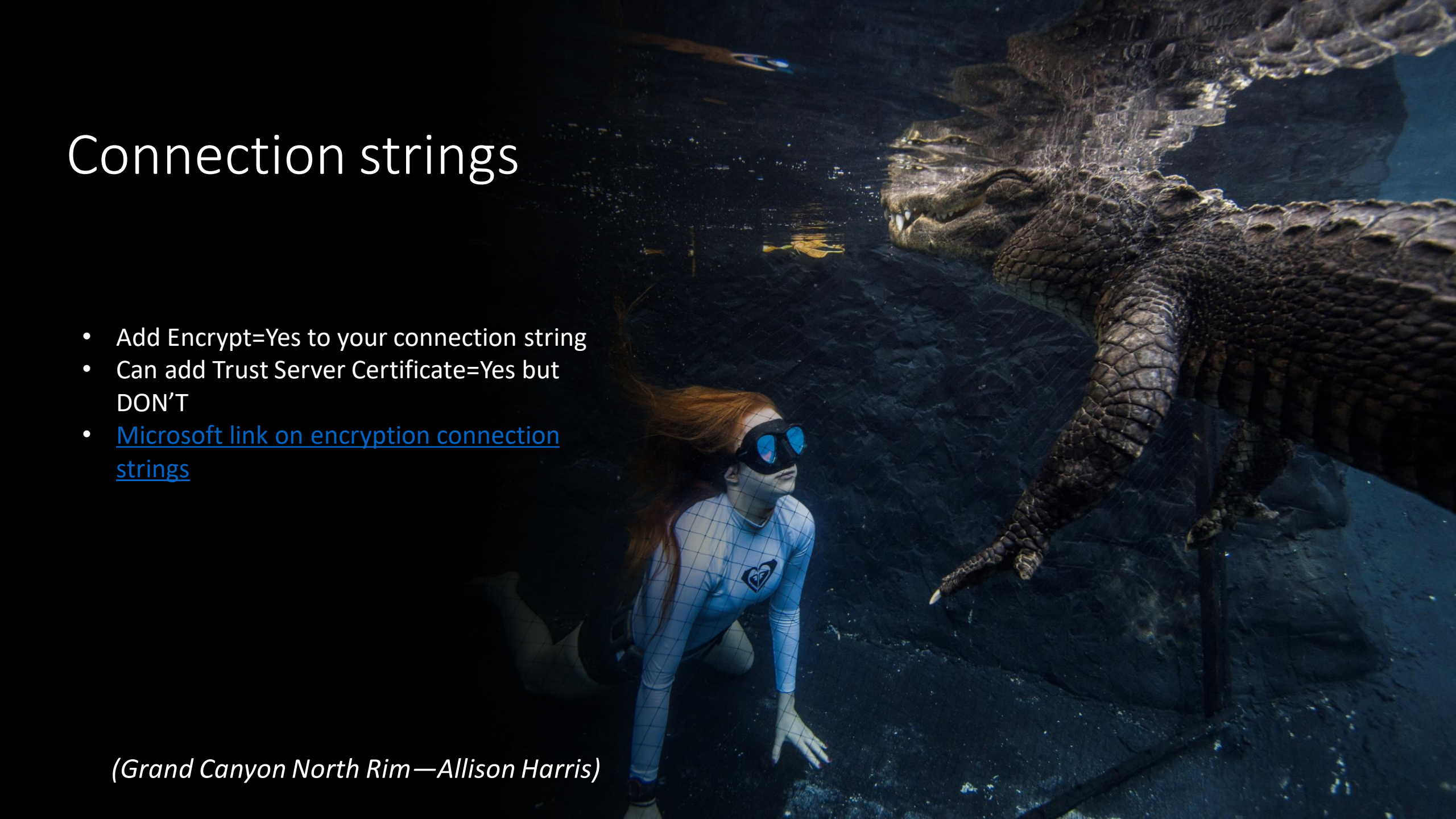


SSMS 20

- Not set up for encrypted connections
- Can switch to Encryption Optional
- Can check Trust Server option

Connection strings

- Add Encrypt=Yes to your connection string
- Can add Trust Server Certificate=Yes but DON’T
- Microsoft link on encryption connection strings



(Grand Canyon North Rim—Allison Harris)

Resources

www.sqlshack.com/how-to-set-and-use-encrypted-sql-server-connections
www.mssqltips.com/sqlservertip/3299/how-to-configure-ssql-encryption-in-sql-server
www.mssqltips.com/sqlservertip/3408/how-to-troubleshoot-ssl-encryption-issues-in-sql-server
www.dataversity.net/securing-data-in-transit-for-analytics-operations
www.digicert.com/faq/cryptography/what-is-ssl-cryptography
msurasky.wordpress.com/2017/02/27/encryption-in-transit/

(Grand Canyon—my daughter Allison Harris)

Contact info

- sharon.reid.harris@gmail.com
- https://github.com/InfoJunkie1/EncryptConnections
- @Edudiva on Twitter
- @edudiva@dataplatform.social on Mastodon
- @edudiva.bsky.social on Bluesky
- linkedin.com/in/Sharon-reid-44433654 on LinkedIn

(Grand Canyon—North Rim)