Microsoft SQL Server Database Security

--Narendra Srivastava

Index

Transparent Data Encryption

TDE is designed to protect the data in the physical data and log files at all times. Data is encrypted as it's written to disk, and decrypted as it's read into memory for use. TDE is enabled at the database level not at object level.

The database encryption key (DEK) is stored on the database server. To restore to another server, or use an HA/DR technology like Availability Groups or log shipping, you must restore the key to the second server as well.

Advantage:

- Performs real-time I/O encryption and decryption of the data and log files
- Encrypts the Entire Database in rest
- No architectural changes needed
- No application code changes are required and the user experience is the same
- Works with high availability features, such as mirroring, AlwaysOn.
- The performance impact of TDE is minor. Estimated to be around 3-5%

Disadvantage:

- No protection for data in memory
- Not granular – Cannot just encrypt specific tables/columns
- Not protected through communication/networks

Backup Encryption

Backup Encryption is designed to ensure the data in backup files is protected by encryption. Is it applied at the database level. The WITH ENCRYPTION clause can be used with full, differential, and log backups.

When taking the backup, a certificate or asymmetric key must be specified. When restoring the backup, the certificate or key must be present as well.

Advantage:

- It's available in Standard Edition.
- In addition to on-premises databases, it can also be used with SQL Server Managed Backup , which means offsite backups are more secure.

Disadvantage:

- You can't restore an encrypted backup to an earlier version of SQL Server.
- Because this encrypts the backup only, it won't protect the data at rest on your SQL Server.

Always Encrypted

Always Encrypted is a new feature in SQL Server 2016. It is designed to protect the data at all times by encrypting and decrypting within the client. The actual, unencrypted data is never known to SQL Server.

This Encryption happens at the column level, so it is a very targeted process. Because the data is encrypted and decrypted at the client, the more data that is encrypted will mean more work and slower performance. Don't try to encrypt the entire database!

The encryption keys are generated on the database server. A driver that encrypts and decrypts the data as it is sent to the database server is installed on the client.

Advantage:

- The application connection string must be changed, which may not be possible with all applications.
- Since this is a two-step encryption process, no one can get a copy of the database files or backup files and automatically have access to the encrypted data.

Disadvantage:

- The application connection string must be changed, which may not be possible with all applications.
- It is a first-version feature right now, which means there are limitations. For example, only equality comparisons (=) are allowed on the encrypted columns when using deterministic encryption, and no comparisons are allowed when using randomized encryption.

Row –Level Security

It is part of the on-premises product in SQL Server 2016. With this feature, the data is not encrypted, but based on a user's security level, they may not be able to see sensitive information.

it is applied at row level. The data that is sensitive is marked at the row level. Individual users or groups are given rights to see the data. Note, this only applies to SELECT, UPDATE, and DELETE operations. Any user can INSERT data into the table.

Row-level security is based on a table-valued function which users are evaluated against, and a security policy that is applied to the table. No master keys or certificates are needed.

Advantage:

- You can now control access to certain data within the database itself, rather than at the client level.

Disadvantage:

- Row level Security requires a table-valued function, and functions are terrible for performance. If you use this feature, write your functions well and test them thoroughly.
- Also, if a user has direct access to the server, they will be able to see the data.

SSL Encryption

Microsoft SQL Server can use Secure Socket Layer (SSL) to encrypt the data that is transmitted across a network between an instance of SQL Server and Client application, Enabling SSL Encryption increase the security of data transmitted across networks between instances of SQL Server and Applications

---

Advantage:

- SSL effectively encrypts this vital information, making sure it's unreadable by everyone except the receiving server.
- SSL certificates also provide proper authentication, which ensures information being sent over the web only goes to the right server.
- SSL can also protect customers and businesses from phishing scams.

Disadvantage:

- Cost of Certificate
- Need to remember the renewal of SSL Certificate

Best Practice to Secure Database

Below are the best practice for making your database secure

- Isolate the Database Server.
- Keep it updated with latest patching.
- Encrypt the database backup
- Secure the database backup folder by removing unwanted users
- Use window authentication instead of SQL Authentication.
- Disable SA account and rename it and donot use this account
- Enable Audits.
- Turn of the SQL Server Browser Services or hide SQL server Instances
- Change the Default port.
- Disable unused sql server feature.
- Enforce Password Policies and Password Expiration for SQL Server Logins

Extensible Key Management System

An Extensible Key Management system (EKM) is a system that allows for the creation and management of keys away from the database. Traditionally any symmetric and asymmetric keys used by SQL Server reside in the databases themselves. EKM allows key creation, storage, encryption and decryption to be done outside the database using a Hardware Security Module, or HSM. An HSM is a hardware device that stored keys in hardware or software modules. This is ultimately more secure since they keys then don't reside with the encrypted data. There are a variety of vendors that provide HSM systems (Townsend Security, SafeNet, Thales, etc.).