Segurança de Dados no SQL Server

Por: José Antônio da Cunha

Nesta atividade você vai experimentar uma característica existente no SQL Server a partir da 2005: O armazenamento dos dados de forma segura. Tem-se notado que os Developers possuem muitas dúvidas sobre esse tema e, então você vai testar essa nova característica de segurança do SQL Server. No SQL Server não se faz mais necessário utilizar soluções de terceiros para encriptar/decriptar dados.

Infra-Estrutura de segurança

O SQL Server fornece uma infra-estrutura para encriptação de dados, um nível de segurança não existente em versões anteriores do SQL Server. Essa nova característica encontra-se disponível em todas as edições do produto (Express, Standard, Workgroup, Developer e Datacenter).

Baseado no modelo de encriptação do SQL Server, responda as seguintes questões?

1. Que tipo(s) de chave(s) é/são utiliza(s) pelo SQL Server?
2. Qual é o serviço responsável em manter essa(s) chave(s)?
3. Qual é o usuário que pode abrir essa(s) chave(s)?
4. Existe a possibilidade de ter um backup da "service master key" ? Se Sim, escreva as linhas de comando para gerenciar o backup e restore.
5. Quais são os usuários e permissões que podem utilizar os comandos que você escreveu no item 4.

Como se trata de uma hierarquia de chaves de encriptação, o próximo nível é o "database master key" que, como o próprio nome diz, trabalha a nível de banco de dados. Você pode criar uma chave simétrica no nível do banco de dados para encriptar certificados e chaves.

6. Escreva o código para criar o 'database master key'.

Segurança a nível de dados

O próximo nível na hierarquia, é a encriptação a nível da dados, que fornece duas opções de encriptação: chave simétrica e chave assimétrica.

Uma chave simétrica é um mecanismo de encriptação mais rápido para encriptar e decriptar dados. Você pode utilizar chave simétrica para dados que são constantemente acessados.

7. Escreva o comando para criar uma chave simétrica.
8. Qual é o comando utilizado para encriptar e decriptar dados simétricos?
9. O algoritmo utilizado acima (AES_256) é o único (sim/não)? Se não quais os outros?
10. Escreva o comando para se criar uma chave assimétrica.
11. Qual é o comando utilizado para encriptar e decriptar dados assimétricos?

Certificado Digital

Certificado Digital é o mecanismo mais "forte" disponível no SQL Server. Um certificado de chave pública é assinado digitalmente e associado uma identidade de usuário, dispositivo ou serviço que armazena a chave privada. Ou seja, a chave pública, como o próprio nome informa é de conhecimento público e serve para decriptar. Esse modelo é amplamente utilizado e segue as normas X.509. Por ser extremamente seguro, o impacto na performance também é sentida devido ao overhead quando se encripta e decripta os dados.

12. Escreva a linha de código para criação do certificado.
13. Quais são as funções usadas para encriptar e decriptar dados usando certificado digital?
14. Explique o que cada comando a seguir faz?

USE ADVENTUREWORKS

GO

CREATE MASTER KEY ENCRYPTION BY PASSOWRD = '1234567890'

GO

CREATE CERTIFICATE MeuCertificado

WITH SUBJECT = 'Comentarios do candidato'

GO

CREATE SYMMETRIC KEY ChaveComentario

WITH ALGORITHM = DES

ENCRYPTION BY CERTIFICATE MeuCertificado

GO

ALTER TABLE HumanResources.JobCandidate

ADD Comentarios varbinary(4000)

GO

OPEN SYMMETRIC KEY ChaveComentario

DECRYPTION BY CERTIFICATE MeuCertificado

```
UPDATE HumanResources.JobCandidate

SET Comentarios = EncryptByKey(Key_GUID(´ChaveComentario'), 'Esta
informacao será encriptada e decriptada')


SELECT JobCandidateID, Comentários FROM HumanResources.JobCandidate


OPEN SYMMETRIC KEY ChaveComentario

DECRYPTION BY CERTIFICATE MeuCertificado


SELECT JobCandidateID, CONVERT(VARCHAR, DecryptByKey(Comentários))

FROM HumanResources.JobCandidate


CREATE VIEW vJobCandidate

AS

SELECT JobCandidateID, CONVERT(VARCHAR, DecryptByKey(Comentários))

FROM HumanResources.JobCandidate


SELECT * FROM vJobCandidate
```