CHAPTER

Database Encryption

2

INFORMATION IN THIS CHAPTER:

- Database Encryption
- Encrypting Data within Tables
- Encrypting Data at Rest
- Encrypting Data on the Wire
- Encrypting Data with MPIO Drivers
- Encrypting Data via HBAs
- Summary

DATABASE ENCRYPTION

A key way to protect the data within your database is to use database encryption. However, no one encryption solution is correct for every database. The encryption requirements of your application will dictate which encryption solution you select. One thing to remember about database encryption is that the more data you encrypt and the stronger the encryption, the more CPU power will be required in order to encrypt and decrypt the data that is needed. So, be sure to balance the encryption requirements with the increased system load.

Hashing versus Encryption

There are two techniques for protecting your data: hashing and encryption. Encryption is done using one of several different algorithms that give you a value that can be decrypted when using the correct decryption key. Each of the different encryption options provides you with a different strength of encryption. As you use a stronger level of encryption, you will be using more CPU load on the Microsoft SQL Server. Microsoft SQL Server only supports a subset of the available encryption algorithms; however, it does support some of the more popular algorithms, from weakest to strongest, which are DES, TRIPLE_DES, TRIPLE_DES_3KEY, RC2, RC4, RC4_128, DESX, AES_128, AES_192, and AES_256. The full list of available algorithms hasn't changed since Microsoft SQL Server 2005 and the newest

Securing SQL Server http://dx.doi.org/10.1016/B978-1-59-749947-7.00002-2