DB2 10.5 for Linux, UNIX, and Windows

DB2 native encryption

Last Updated: 2021-03-01

23

DB2® native encryption encrypts your DB2 database, requires no hardware, software, application, or schema changes, and provides transparent and secure key management.

Encryption is the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process. It is an effective way of protecting sensitive information that is stored on media or transmitted through untrusted communication channels. Encryption is mandatory for compliance with many government regulations and industry standards.

In an encryption scheme, the data requiring protection is transformed into an unreadable form by applying a cryptographic algorithm and an encryption key. A *cryptographic algorithm* is a mathematical function that is used in encryption and decryption processes. An *encryption key* is a sequence that controls the operation of a cryptographic algorithm and enables the reliable encryption and decryption of data.

23

Some data encryption solutions for protecting data at rest are suitable in cases of physical theft of disk devices, and some can protect against privileged user abuse. With *native database encryption*, the database system itself encrypts the data before it calls the underlying file system to write that data to disk. This means that not only your current data is protected, but also data in new table space containers or table spaces that you might add in the future. Native database encryption is suitable for protecting data in cases of either physical theft of disk devices or privileged user abuse.

A local or external key manager is typically used to manage the keys. A *database data encryption key* (DEK) is the encryption key with which actual user data is encrypted. A *master key* is a "key encrypting key": It is used to protect the DEK. Although the DEK is stored and managed by the database, the master key is stored and managed outside of the database.

These keys are shown in Figure 1, which provides an overview of DB2 native encryption.

Figure 1. An overview of DB2 native encryption