Encryption with compression

Last Updated: 2021-03-05 6

6

You can use InfoSphere® Guardium Data Encryption to encrypt and compress your DB2® or IMS™ data.

By compressing your data, you can reduce the amount of disk space that it requires for storage. This size reduction can improve database encryption performance and reduce I/O. Data compression must be performed before the data is encrypted because encrypted data does not contain repeating patterns and does not compress well.

You can encrypt and compress data by customizing driver routines that are provided with InfoSphere Guardium Data Encryption. These driver routines link the DB2 or IMS compression routine with the encryption exit routine that you create by using this product. When an application processes a table or segment that is linked to the driver routine, the data is first compressed and then it is encrypted.

DB2 compression

DB2 has its own compression function, but you cannot attain the benefits of compression by using it on tables that are encrypted by InfoSphere Guardium Data Encryption. Therefore, you must use the edit procedure driver that is provided with this product.

This edit procedure driver ensures that compression is performed before encryption in DB2. When DB2 performs compression on a table, it runs any edit procedures that are linked with that table first. Therefore, if you link an encryption exit routine with a table and then use the DB2 compression function on it, encryption occurs before compression.

Compression provides storage benefits by replacing repeating bit strings with shorter strings. However, the encryption process replaces all repeating bit strings with non-repeating ciphertext. Therefore, when encryption occurs before compression, compression does not reduce the size of the data.

IMS compression

Prior to data encryption, existing compression routines can be combined with the supplied compression routine driver to perform compression.

Parent topic:

→ InfoSphere Guardium Data Encryption overview

Related tasks:

→ Implementing a DB2 encryption edit procedure with compression

→ Encrypting IMS data with compression