Dbcopy issues with custom managed key

Last updated by | Soma Jagadeesh | Jan 10, 2021 at 9:46 PM PST

Contents

Issue

Unable to copy database to target server when TDE enabled with custom managed key in source and Target

CREATE DATABASE [DB-TestDba-qa] AS COPY OF [cbcrc-dev].[DB-TestDba-dev]

Customer receives following error when attempting to copy a database from source to destination server, both servers are using TDE encryption with Customer managed key, both servers have individual keys associated with them. Both source and Target key vaults in same region Command used:- (Execute on the master database of the target server (server2) to start copying from Server1 to Server2)

"The encryption protectors for all servers linked by GeoDR must be in the same region as their respective servers. Please upload key 'https://cbcrc-qa-key-vault.vault.azure.net/keys/Cbcrc-qa-sql-azure-key/f2a1a2bc123d408aa155b1bbf9fbe86a' to a Key Vault in the region 'Canada East' as server 'cbcrc-dev'. (https://aka.ms/sqltdebyokgeodr)"

Cause

Customer need to configure the source and target server with the same key material in order to copy/restore/Geodr database, without the key copy cannot be successful.

This is a limitation in the product and there are workarounds available.

Mitigation

1. Customer can disable TDE encryption at Database level, drop the DEK key on the Database (reference link provided below), and then copy the Database to destination server. TDE Encryption on the source and destination databases need to be manually enabled.
2. Customert can use same encryption key on source and destination servers when using Customer managed key and the DB copy should happen without issues. Link for the article providing details about dropping DEK key: https://docs.microsoft.com/en-us/sql/t-sql/statements/drop-database-encryption-key-transact-sql?view=sql-server-ver15#feedback

Public Document reference: https://docs.microsoft.com/en-us/azure/azure-sql/database/transparent-data-encryption-byok-overview https://docs.microsoft.com/en-us/azure/azure-sql/database/transparent-data-encryption-tde-overview?tabs=azure-portal

Classification

Root cause tree – Security/ TDE / BYOK / Custom Managed key.

How good have you found this content?

🙂 🙁