Error 45384 - The encryption protectors for all servers linked by GeoDR must be in the same region as their respective servers

Last updated by | Vitor Tomaz | Jun 8, 2022 at 5:37 AM PDT

Contents

Issue

Error 45384
The encryption protectors for all servers linked by GeoDR must be in the same region as their respective servers. Please upload key 'https://A.vault.azure.net/keys/B' to a Key Vault in the region 'C' as server 'D'. (https://aka.ms/sqltdebyokgeodr)

Investigation/Analysis

Documentation currently says that, to avoid issues while establishing or during geo-replication due to incomplete key material, it's important to follow these rules when configuring customer-managed TDE:

- All key vaults involved must have same properties, and same access rights for respective servers.
- All key vaults involved must contain identical key material. It applies not just to the current TDE protector, but to the all previous TDE protectors that may be used in the backup files.
- Both initial setup and rotation of the TDE protector must be done on the secondary first, and then on primary.

It's possible for customers to have the same key on both regions and still face this issue while trying to setup the protected on the secondary region because, despite key exists, it's not associated with the instance.

Mitigation

If you confirmed that key exists on both sides, and all requirements are met, the following steps should work:

1. *In the primary, set the key in the TDE blade but do not make it as the default protector yet (the goal of this step is to associate the key with the managed instance so key existence can be verified when trying to setup the protector on the secondary instance).*
2. Set TDE on secondary and make it the default protector.

3. Set TDE on the primary and make it the default protector.

Public Doc Reference

https://docs.microsoft.com/en-us/azure/azure-sql/database/transparent-data-encryption-byok-overview#geo-dr-and-customer-managed-tde

Root Cause Classification

Cases resolved by this TSG should be coded to the following root cause:
Azure SQL v3/Security/TDE and Customer Managed Key (CMK)

How good have you found this content?

🙂 🙁