CMK and Azure Key Vault (AKV) Enhancements - Public Preview

Last updated by | Vitor Tomaz | Jun 8, 2022 at 5:35 AM PDT

Contents

TDE and CMK New Public Preview feature ETA on 08/10 and public documentation will be released on same date for customers

Support for RBAC-enabled key vaults

- To provision server identity (system-assigned or user-assigned) access to the key vault, in addition to creating an access policy with Get, WrapKey, UnwrapKey permissions, users can also choose to enable RBAC permission model on the key vault. In this case, to assign the required permissions to the server identity, user needs to create a new RBAC role assignment on the key vault by assigning the role “Key Vault Crypto Service Encryption User” to the server identity. Assigning this role is equivalent to creating an access policy with Get, WrapKey, UnwrapKey permissions.

Mandatory check for purge protection when adding an encryption key to the server

- When adding a new encryption key to the server or setting the key as TDE Protector, SQL will now check if Purge Protection is enabled on the key vault, if not the key addition operation fails. The requirement to enable purge protection is in addition to the soft-delete check that already exists today. Users should therefore ensure purge protection is enabled on their key vaults prior to adding a new encryption key to the server. Purge Protection on key vault can be enabled from Portal or from PS/CLI, etc. Once enabled, purge protection cannot be disabled. Note – This doesn’t impact existing encryption keys in use.

Removal of server and key-vault co-location (same region) requirement

- The restriction that server and key vault should be located in the same region has been removed. A server in any region can now be connected to a key vault in any other region.

Public Doc Reference (optional)

During Public Preview launch, documentation will be published for customers.

Internal Reference (optional)

Currently all the new features are in Public Preview

Root Cause Classification

Cases resolved by this TSG should be coded to the following root cause:
Root cause Tree - Security/TDE and CMK/How-to/advisory

How good have you found this content?