Restore_Replicate_withCMK

Last updated by | Lisa Liu | Nov 6, 2020 at 10:36 AM PST

Issue

Restore and Replicate with CMK in Key Vault

Investigation/Analysis

This is a how-to scenario. For any issues with Database not accessible /Key Revalidation issues for the TSG's

Issues with Key Vault Outage/Permissions

Key Revalidation Issues

Mitigation

After Azure Database for PostgreSQL Single server is encrypted with a customer's managed key stored in Key Vault, any newly created copy of the server is also encrypted. You can make this new copy either through a local or geo-restore operation, or through read replicas. However, the copy can be changed to reflect a new customer's managed key for encryption. When the customer-managed key is changed, old backups of the server start using the latest key.

To avoid issues while setting up customer-managed data encryption during restore or read replica creation, it's important to follow these steps on the master and restored/replica servers:

1. Initiate the restore or read replica creation process from the master Azure Database for PostgreSQL Single server.
2. Keep the newly created server (restored/replica) in an inaccessible state, because its unique identity hasn't yet been given permissions to Key Vault.
3. On the restored/replica server, revalidate the customer-managed key in the data encryption settings. This ensures that the newly created server is given wrap and unwrap permissions to the key stored in Key Vault.

Public Doc Reference (optional)

Restore and Replicate with CMK in Key Vault

Internal Reference (optional)

BYOK Scenarios

Root Cause Classification

Cases resolved by this TSG should be coded to the following root cause: Azure Open Source DB V2\Security\User Request\Data Encryption\How-to questions

How good have you found this content?