Deploy failed for PGFS´s geo-redundant server due to BYOK errors

Last updated by | Hamza Aqel | Mar 8, 2023 at 2:32 AM PST

Contents

- Issue
- Investigation/Analysis
- Mitigation

Issue

Customer receiving errors in deployments like "The 'serverResource.properties.authConfig' segment in the url is invalid."

Investigation/Analysis

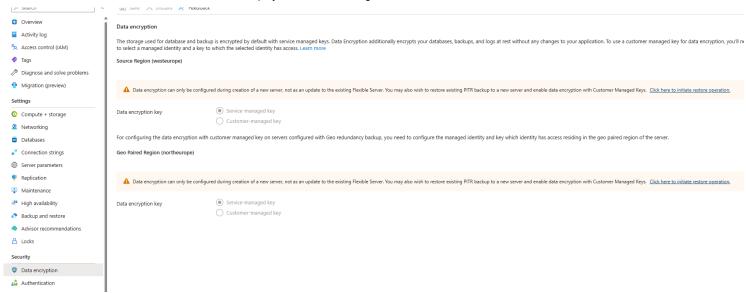After checking deployment error (by example using this TSG:https://dev.azure.com/Supportability/AzureDBPostgreSQL/_wiki/wikis/AzureDBPostgreSQL/688324/Provisioning-operations-breakdown-single-Kusto-query ↗) you observe errors when trying to deploy server with geo-redundant and BYOK like this: "Data encryption for geo-redundant backup enabled server have to specify 2 different user assign identities…"

Mitigation

Customer should review the deployment properties to specify two different user assigned identities.

Currently, PGFS only allows Data encryption with user managed key during creation of a new server.

For configuring the data encryption with customer managed key on servers configured with Geo redundancy backup, customer needs to configure the managed identity and key which identity has access residing in the geo paired region of the server:

Search

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Migration (preview)

Settings

- Compute + storage
- Networking
- Databases
- Connection strings
- Server parameters
- Replication
- Maintenance
- High availability
- Backup and restore
- Advisor recommendations
- Locks

Security

- Data encryption
- Authentication

Save   Discard   Feedback

Data encryption

The storage used for database and backup is encrypted by default with service managed keys. Data Encryption additionally encrypts your databases, backups, and logs at rest without any changes to your application. To use a customer managed key for data encryption, you'll ne to select a managed identity and a key to which the selected identity has access. Learn more

Source Region (westeurope)

⚠ Data encryption can only be configured during creation of a new server, not as an update to the existing Flexible Server. You may also wish to restore existing PITR backup to a new server and enable data encryption with Customer Managed Keys. Click here to initiate restore operation.

Data encryption key   ◉ Service-managed key
                           ○ Customer-managed key

For configuring the data encryption with customer managed key on servers configured with Geo redundancy backup, you need to configure the managed identity and key which identity has access residing in the geo paired region of the server.

Geo Paired Region (northeurope)

⚠ Data encryption can only be configured during creation of a new server, not as an update to the existing Flexible Server. You may also wish to restore existing PITR backup to a new server and enable data encryption with Customer Managed Keys. Click here to initiate restore operation.

Data encryption key   ◉ Service-managed key
                           ○ Customer-managed key

How good have you found this content?

🙂 🙁