Key_Expiration

Last updated by | Lisa Liu | Nov 6, 2020 at 10:35 AM PST

Issue

Key Expiration In all these cases Database becomes unavailable and you will receive generic 'unable to connect' errors from applications

Examples:

Message: mysqli::real_connect(): (HY000/9002): The server name you tried cannot be found. Please use the correct name and retry. Please check your server name mdb-sgrass-uat-az1-ccfasvr.

FATAL: Cannot connect to the server mytestdbpk

SSL SYSCALL error: EOF detected

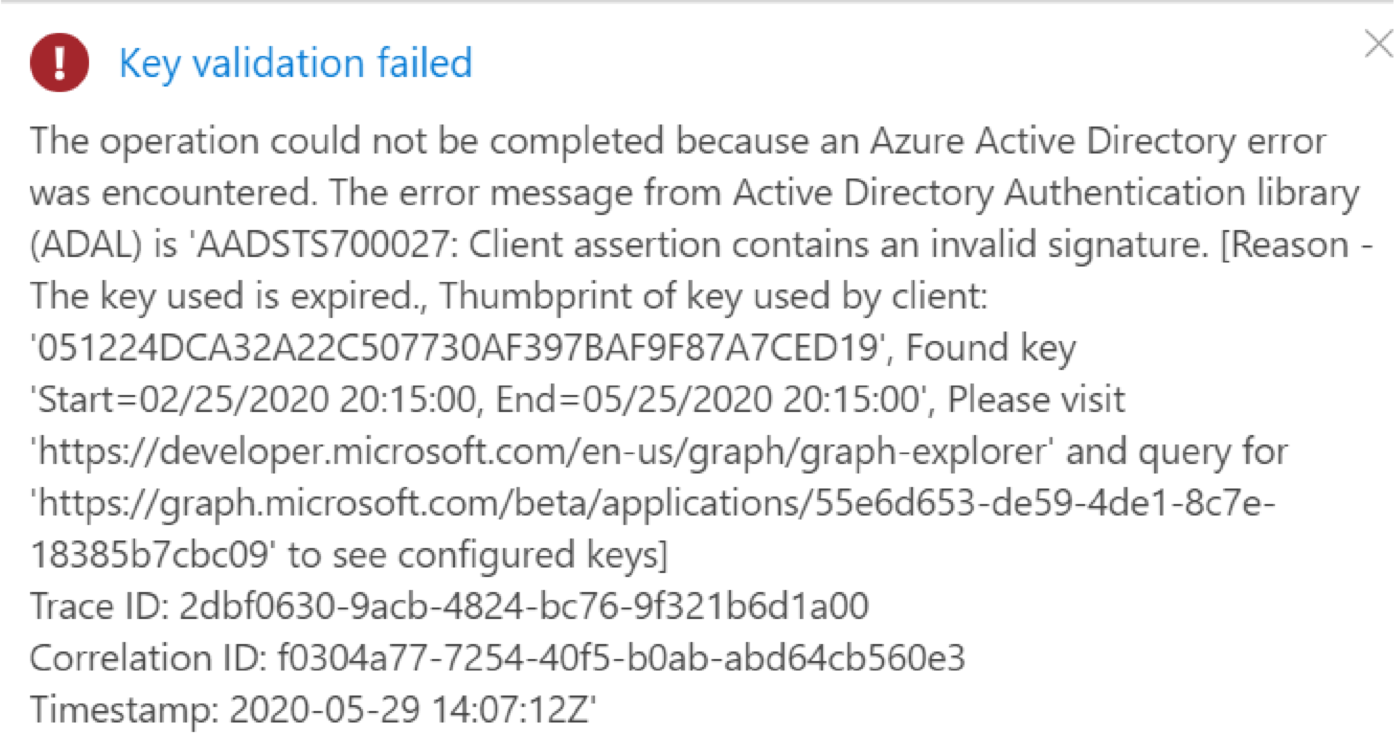
Unexpected error occurred while connecting.: Error: Unexpected error occurred while connecting.

Investigation/Analysis

The key used in Azure key vault may not have an expiration date set in Azure Key Vault. If the key had an expiration date set previously, the user must set the expiration date to '12/31/9999' in order to use the key.

If an expiration date aside from that is set, the service will reject the key. (We want to minimize the number of accidentally set expiration dates)

It is possible to add the expiration date after adding it as the BYOK key, and if that BYOK key expires, it will become disabled, and the encrypted database will become unavailable.



Key validation failed

The operation could not be completed because an Azure Active Directory error was encountered. The error message from Active Directory Authentication library (ADAL) is 'AADSTS700027: Client assertion contains an invalid signature. [Reason - The key used is expired., Thumbprint of key used by client: '051224DCA32A22C507730AF397BAF9F87A7CED19', Found key 'Start=02/25/2020 20:15:00, End=05/25/2020 20:15:00', Please visit 'https://developer.microsoft.com/en-us/graph/graph-explorer' and query for 'https://graph.microsoft.com/beta/applications/55e6d653-de59-4de1-8c7e-18385b7cbc09' to see configured keys]
Trace ID: 2dbf0630-9acb-4824-bc76-9f321b6d1a00
Correlation ID: f0304a77-7254-40f5-b0ab-abd64cb560e3
Timestamp: 2020-05-29 14:07:12Z'

The following are requirements for configuring the customer-managed key: • The customer-managed key to be used for encrypting the DEK can be only asymmetric, RSA 2048. • The key activation date (if set) must be a date and time in the past. The expiration date (if set) must be a future date and time. • The key must be in the Enabled state. If you're importing an existing key into the key vault, make sure to provide it in the supported file formats (.pfx, .byok, .backup).

Mitigation

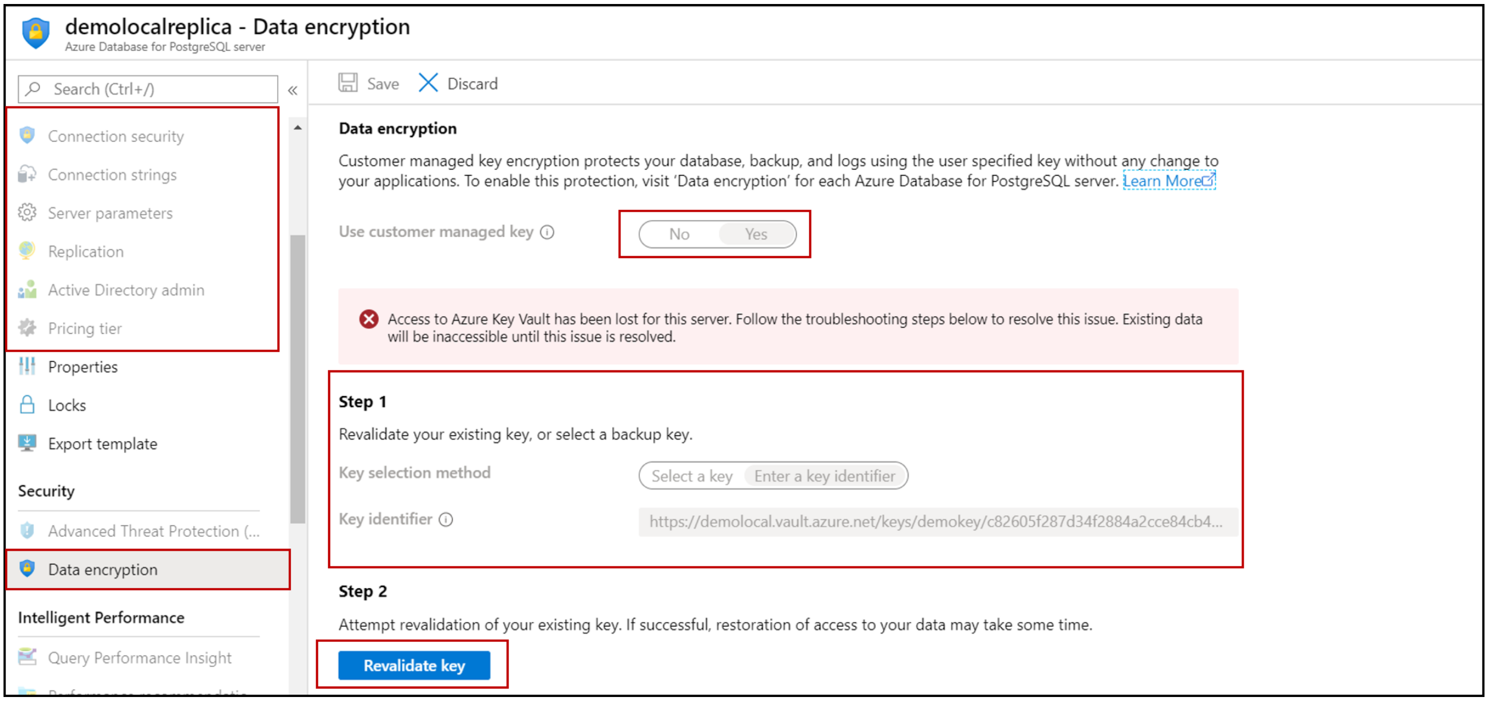
If the key stored in the Azure KeyVault expires, the key will become invalid and the Azure Database for PostgreSQL Single server will transition into Inaccessible state. Extend the key expiry date using CLI and then revalidate the data encryption to make the server Available.

https://docs.microsoft.com/en-us/cli/azure/keyvault/key?view=azure-cli-latest#az-keyvault-key-set-attributes

The update key operation changes specified attributes of a stored key and can be applied to any key type and key version stored in Azure Key Vault.

az keyvault key set-attributes [--enabled {false, true}] [--expires] [--id] [--name] [--not-before] [--ops {decrypt, encrypt, import, sign, unwrapKey, verify, wrapKey}] [--subscription] [--tags] [--vault-name] [--version] --expires Expiration UTC datetime (Y-m-d'T'H:M:S'Z').

After this you will need to revalidate the key



Data encryption

Customer managed key encryption protects your database, backup, and logs using the user specified key without any change to your applications. To enable this protection, visit 'Data encryption' for each Azure Database for PostgreSQL server. Learn More

Use customer managed key: No | Yes

Access to Azure Key Vault has been lost for this server. Follow the troubleshooting steps below to resolve this issue. Existing data will be inaccessible until this issue is resolved.

Step 1

Revalidate your existing key, or select a backup key.

Key selection method: Select a key | Enter a key identifier

Key identifier: https://demolocal.vault.azure.net/keys/demokey/c82605f287d34f2884a2cce84cb4...

Step 2

Attempt revalidation of your existing key. If successful, restoration of access to your data may take some time.

More Information (optional)

Monitor access to Customer Managed Key

Public Doc Reference (optional)

See Above

Root Cause Classification

Cases resolved by this TSG should be coded to the following root cause: Azure Open Source DB V2\Security\User Issue/Error\Data Encryption\Key Expiration

How good have you found this content?

🙂 🙁