Customer_accidentaly_deleted_key

Last updated by | Hamza Aqel | Feb 11, 2022 at 6:20 AM PST

Issue

Customer deleted a key or Key Vault accidentally

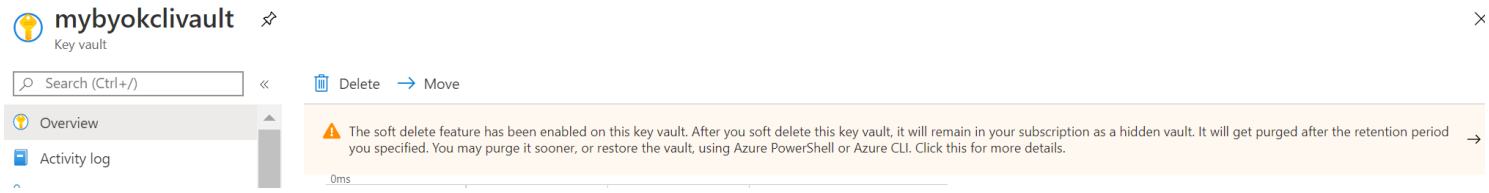
Investigation/Analysis

When you configure data encryption with a customer-managed key in Key Vault, continuous access to this key is required for the server to stay online. If the server loses access to the customer-managed key in Key Vault, the server begins denying all connections within 10 minutes. Customer will receive login errors and Server not accessible generic errors from application.

Mitigation

If you delete the KeyVault, the Azure Database for PostgreSQL Single server will be unable to access the key and will move to **Inaccessible** state. Recover the Key Vault and revalidate the data encryption to make the server Available.

One of the requirements for setting up BYOK with a Key Vault is taht Soft Delete and & Purge Protection needs to be enabled for AKV



If key is dropped from AKV, we (Orcas BYOK Design) do not handle recovery of that key. This will result in data loss – either from live database or database backups. In our documentation, we encourage users to create their keys on-prem first and import those keys into AKV so they are backed up.

Key Vault's **soft-delete feature allows recovery of the deleted vaults** and **vault objects**, known as soft-delete.

Specifically, we address the following scenarios:

- Support for recoverable deletion of a key vault
- Support for recoverable deletion of key vault objects (ex. keys, secrets, certificates)

When **soft-delete is enabled**, resources marked as deleted resources are retained for a specified period (90 days by default).

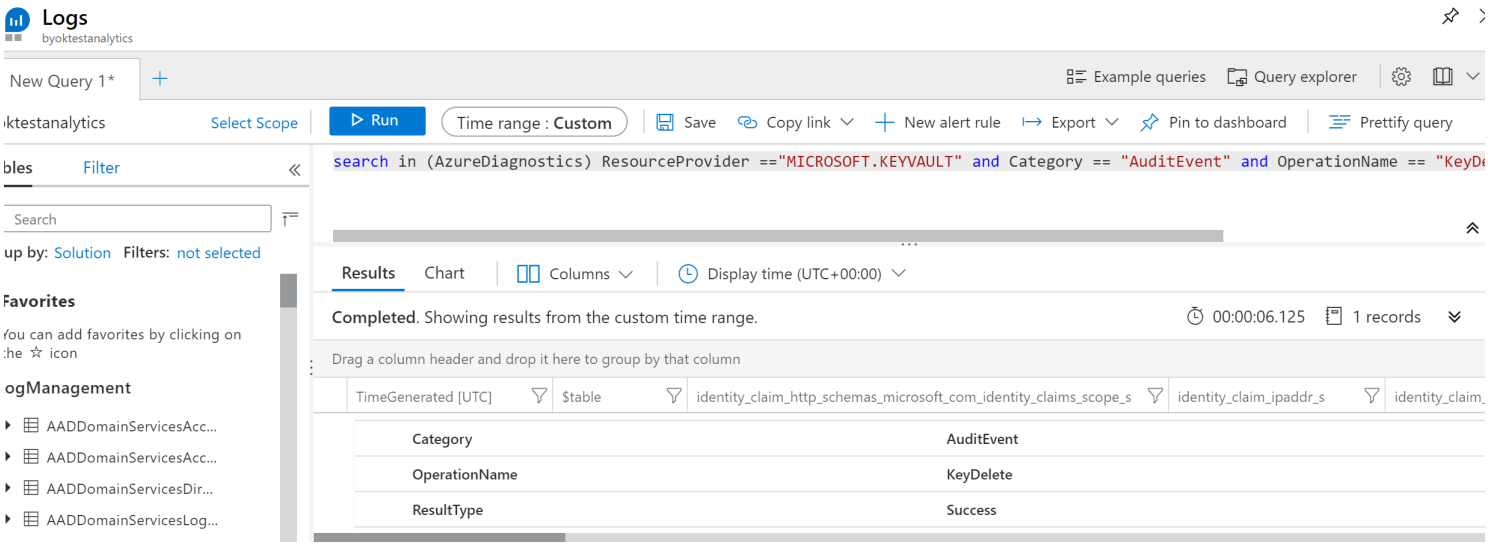
When **purge protection** is on, a vault or an object in the deleted state cannot be purged until the retention period has passed. Soft-deleted vaults and objects can still be recovered, ensuring that the retention policy will be followed. The default retention period is 90 days,

Read more Overview Soft Delete

RCA (optional)

The key vault administrator can also enable logging of Key Vault audit events, so they can be audited later.

You can check if auditing is enabled for Key Vault you will be able to see when or by whom the Key was Deleted



To determine since when the server is Inaccessible based on Kusto telemetry:

```
MonAnalyticsElasticServersSnapshot
| where name == "{REPLACE_HERE}"
| summarize min(TIMESTAMP), max(TIMESTAMP) by ['state'], bin(TIMESTAMP, 1h)
```

Here are recommendations for configuring a customer-managed key:

- Keep a copy of the customer-managed key in a secure place, or escrow it to the escrow service.
- If Key Vault generates the key, create a key backup before using the key for the first time. You can only restore the backup to Key Vault. For more information about the backup command, see Backup-AzKeyVaultKey.
- Set a resource lock on Key Vault to control who can delete this critical resource and prevent accidental or unauthorized deletion.

Once you recover the key , you will need to revalidate to bring back database to Available state For issues with Revalidation check here Revalidation Stuck issues

More Information (optional)

Requirements for BYOK - Soft-delete and Purge Protection need to be turned on for the Key vault used to enable BYOK

Public Doc Reference (optional)

Inaccessible customer key condition

Requirements for Configuring Data Encryption

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\Customer **Accidentally Deleted a Key**

Note:

if the customer failed to recover the deleted key , feel free to open an ICM here to help this customer.

How good have you found this content?