Monitoring_CMK_KeyVault

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

Monitor the customer-managed key in Key Vault

To monitor the database state, and to enable alerting for the loss of transparent data encryption protector access, configure the following Azure features:

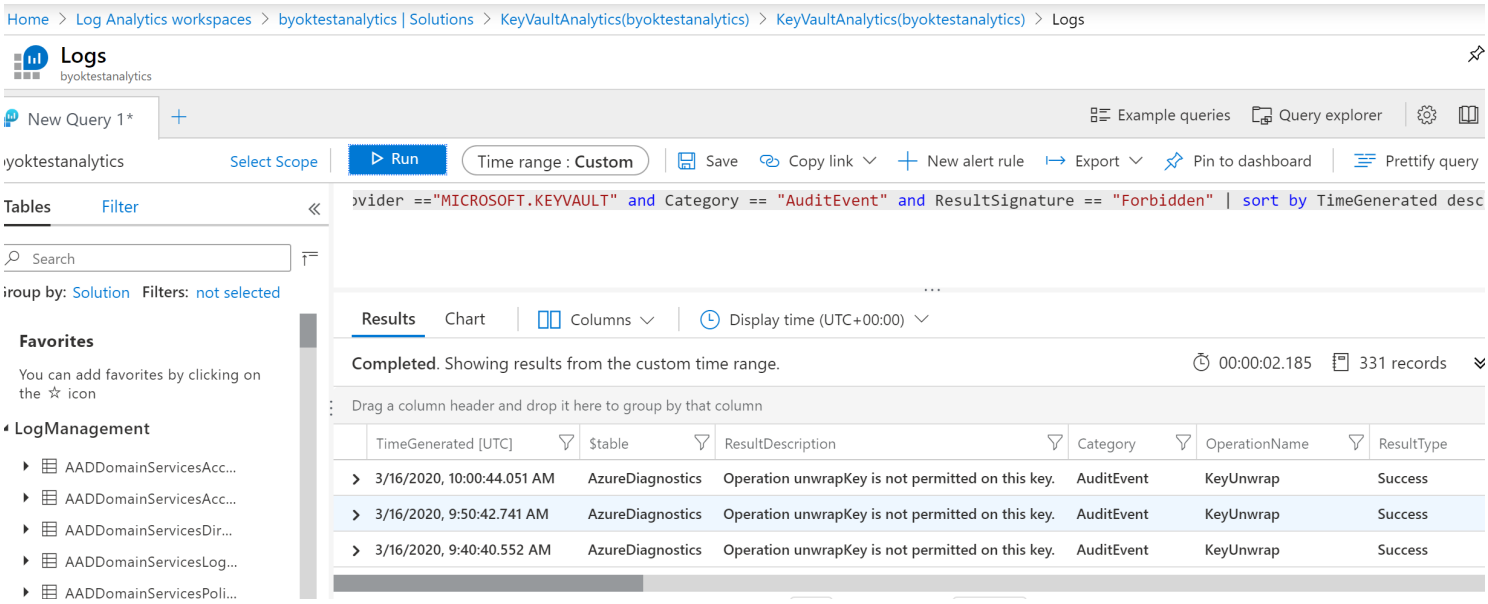
- Azure Resource Health: An inaccessible database that has lost access to the customer key shows as "Inaccessible" after the first connection to the database has been denied.
- Activity log: When access to the customer key in the customer-managed Key Vault fails, entries are added to the activity log. You can reinstate access as soon as possible, if you create alerts for these events.
- Action groups: Define these groups to send you notifications and alerts based on your preferences.

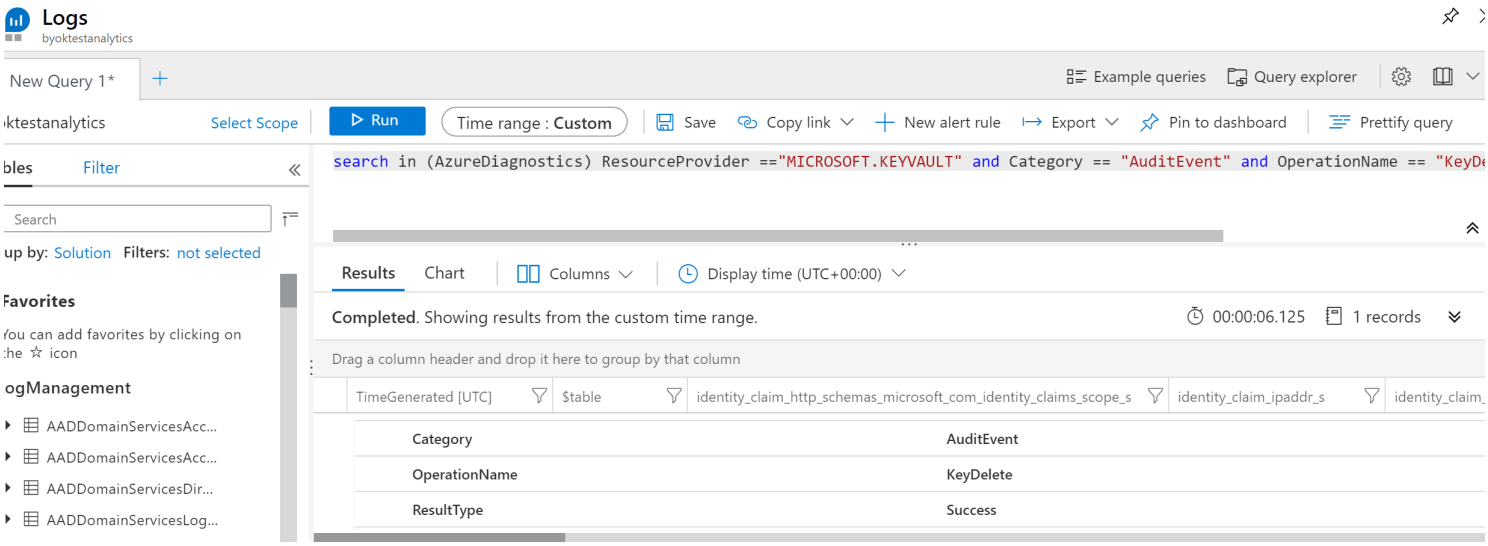
Note: The Activity Log here refers to the Activity log of the Azure Key Vault and not the Database The Azure Resource Health is being integrated + ASC improvements are upcoming shortly

Auditing

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





Internal Notes

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

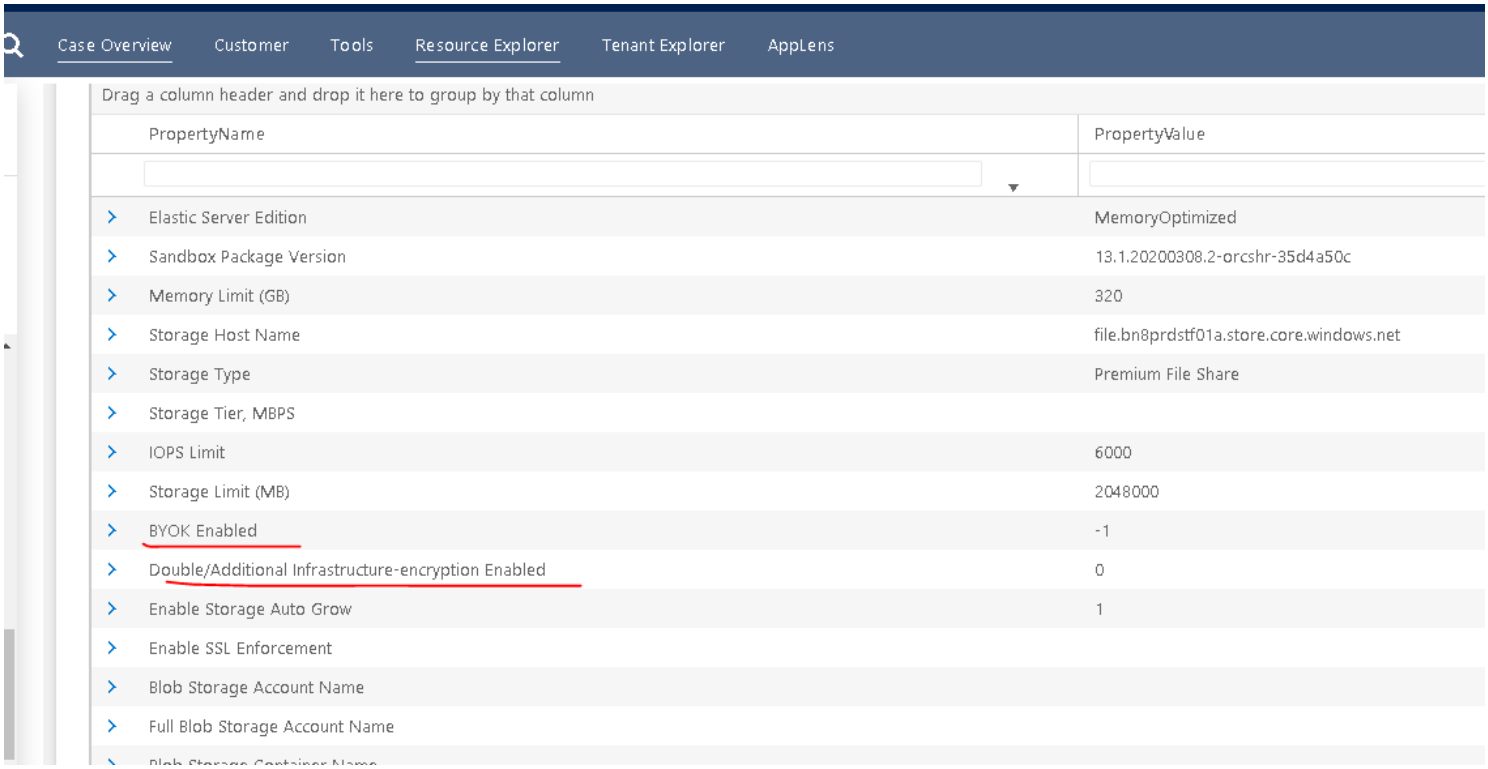
```
MonAnalyticsElasticServersSnapshot
| where name == "{REPLACE_HERE}"
| summarize min(TIMESTAMP), max(TIMESTAMP) by ['state'], bin(TIMESTAMP, 1h)
```

XTS View

XTS View

ASC

From the ASC we can currently see if the BYOK is turned on for the customer or not



Root cause Classification

Azure Open Source DB V2\Security\User Issue/Error\Data Encryption\How-to questions

How good have you found this content?