

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

Home > Log Analytics workspaces > byoktestanalytics | Solutions > KeyVaultAnalytics(byoktestanalytics) > KeyVaultAnalytics(byoktestanalytics) > Logs

Logs
byoktestanalytics

New Query 1* +

Example queries Query explorer Settings

byoktestanalytics Select Scope **Run** Time range: Custom Save Copy link New alert rule Export Pin to dashboard Prettify query

Tables Filter

Search

Group by: Solution Filters: not selected

Favorites
You can add favorites by clicking on the ☆ icon

LogManagement

- AADDomainServicesAcc...
- AADDomainServicesAcc...
- AADDomainServicesDir...
- AADDomainServicesLog...
- AADDomainServicesPoli...

Provider == "MICROSOFT.KEYVAULT" and Category == "AuditEvent" and ResultSignature == "Forbidden" | sort by TimeGenerated desc

Results Chart Columns Display time (UTC+00:00)

Completed. Showing results from the custom time range. 00:00:02.185 331 records

Drag a column header and drop it here to group by that column

TimeGenerated [UTC]	Stable	ResultDescription	Category	OperationName	ResultType
> 3/16/2020, 10:00:44.051 AM	AzureDiagnostics	Operation unwrapKey is not permitted on this key.	AuditEvent	KeyUnwrap	Success
> 3/16/2020, 9:50:42.741 AM	AzureDiagnostics	Operation unwrapKey is not permitted on this key.	AuditEvent	KeyUnwrap	Success
> 3/16/2020, 9:40:40.552 AM	AzureDiagnostics	Operation unwrapKey is not permitted on this key.	AuditEvent	KeyUnwrap	Success

4/5/23, 3:58 PM

Monitoring_CMK_KeyVault - Overview

Logs

byoktestanalytics

New Query 1*

+

Example queries

Query explorer

⚙️

📖

▼

byoktestanalytics

Select Scope

▶ Run

Time range: Custom

💾 Save

🔗 Copy link

+

New alert rule

➡ Export

📌 Pin to dashboard

🔧 Prettify query

bles

Filter

Search

up by: Solution

Filters: not selected

Favorites

You can add favorites by clicking on the ☆ icon

ogManagement

▶ AADDomainServicesAcc...

▶ AADDomainServicesAcc...

▶ AADDomainServicesDir...

▶ AADDomainServicesLog...

search in (AzureDiagnostics) ResourceProvider == "MICROSOFT.KEYVAULT" and Category == "AuditEvent" and OperationName == "KeyDelete"

Results

Chart

Columns

Display time (UTC+00:00)

Completed. Showing results from the custom time range.

00:00:06.125

1 records

Drag a column header and drop it here to group by that column

TimeGenerated [UTC]	\$table	identity_claim_http_schemas_microsoft_com_identity_claims_scope_s	identity_claim_ipaddr_s	identity_claim...
Category	AuditEvent			
OperationName	KeyDelete			
ResultType	Success			

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

Q

Case OverviewCustomerToolsResource ExplorerTenant ExplorerAppLens

Drag a column header and drop it here to group by that column	
PropertyName	PropertyValue
> Elastic Server Edition	MemoryOptimized
> Sandbox Package Version	13.1.20200308.2-orcshr-35d4a50c
> Memory Limit (GB)	320
> Storage Host Name	file.bn8prdstf01a.store.core.windows.net
> Storage Type	Premium File Share
> Storage Tier, MBPS	
> IOPS Limit	6000
> Storage Limit (MB)	2048000
> <u>BYOK Enabled</u>	-1
> <u>Double/Additional Infrastructure-encryption Enabled</u>	0
> Enable Storage Auto Grow	1
> Enable SSL Enforcement	
> Blob Storage Account Name	
> Full Blob Storage Account Name	
> Blob Storage Container Name	

Root cause Classification

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

How good have you found this content?

