Kusto - Azure Monitor Log Queries

Taiob Ali





Taiob Ali

Database Solutions Manager, GMO LLC

- http://sqlworldwide.com/
- in /sqlworldwide
- @sqlworldwide
- taiob@sqlworldwide.com

Data Professional

Microsoft Data Platform MVP. 15 Years working with Microsoft Data Platform. Microsoft and MongoDB certified. Worked in ecommerce, healthcare and finance industry.

Giving Back

Board member NESQL user group and Founder of DBA virtual group. Organizer of Boston SQL Saturday. Frequent speaker at local and virtual user groups, Data Saturdays and Azure conferences.

When Not Working

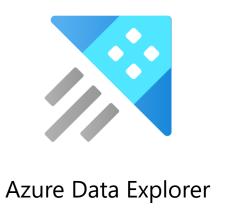
Running – 1x26.2 and 30+x 13.1, Learning US history. Shuttling 3 kids.

Kusto Query Language



- Optimized query language with visualization options
- For fast read-only data retrieval
- Troubleshooting & deep diagnostics
- Real-time stream / big data analytics

Use KQL to connect and query these Azure Services:











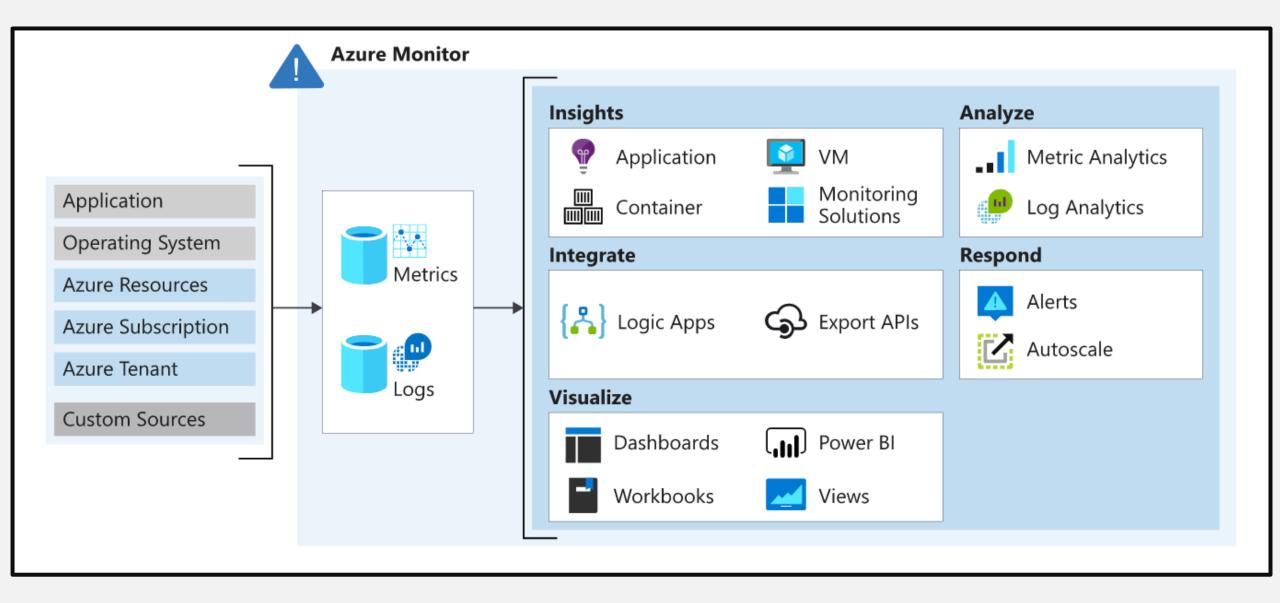
2014

Kusto started in 2014 as internal Microsoft project to address Azure services' needs 2016

It became a backend of Application Insights Analytics

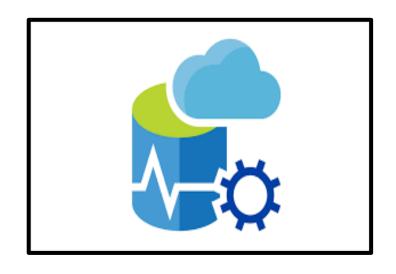
2018

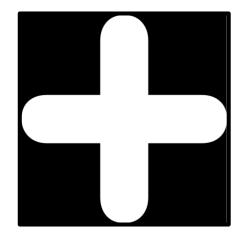
Microsoft
announced a
Public Preview of
the <u>Azure Data</u>
<u>Explorer</u> service
built on top of
Kusto engine

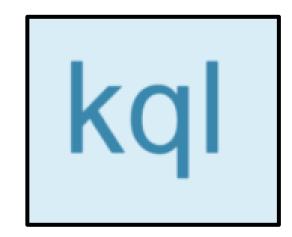


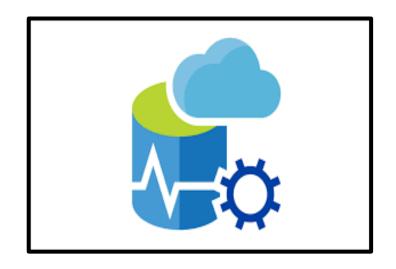
https://docs.microsoft.com/en-us/learn/modules/analyze-infrastructure-with-azure-monitor-logs/2-features-azure-monitor-log

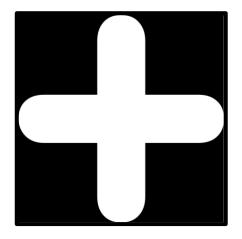
Centralized Logging Data sources for events Design and test queries Azure Analytics Incoming data Monitor and performance and analyze data automatically indexed. Data types and tables Data sources for events Visualize data in Virtual Dashboards automatically created. Machines and performance Azure portal Operations Data from management Workflows consuming 🔼 Logic Apps Log Analytics data group agents Manager Application Application requests Automatically respond Alerts and exceptions critical conditions Insights Log Analytics Azure Security Export for visualization Power BI Security events with other sources Center PowerShell command PowerShell command > PowerShell > PowerShell Data available through line or runbook line or runbook log search and smart analytics to multiple Data Collector Rest API for Rest API for custom Log Search channels. custom data application



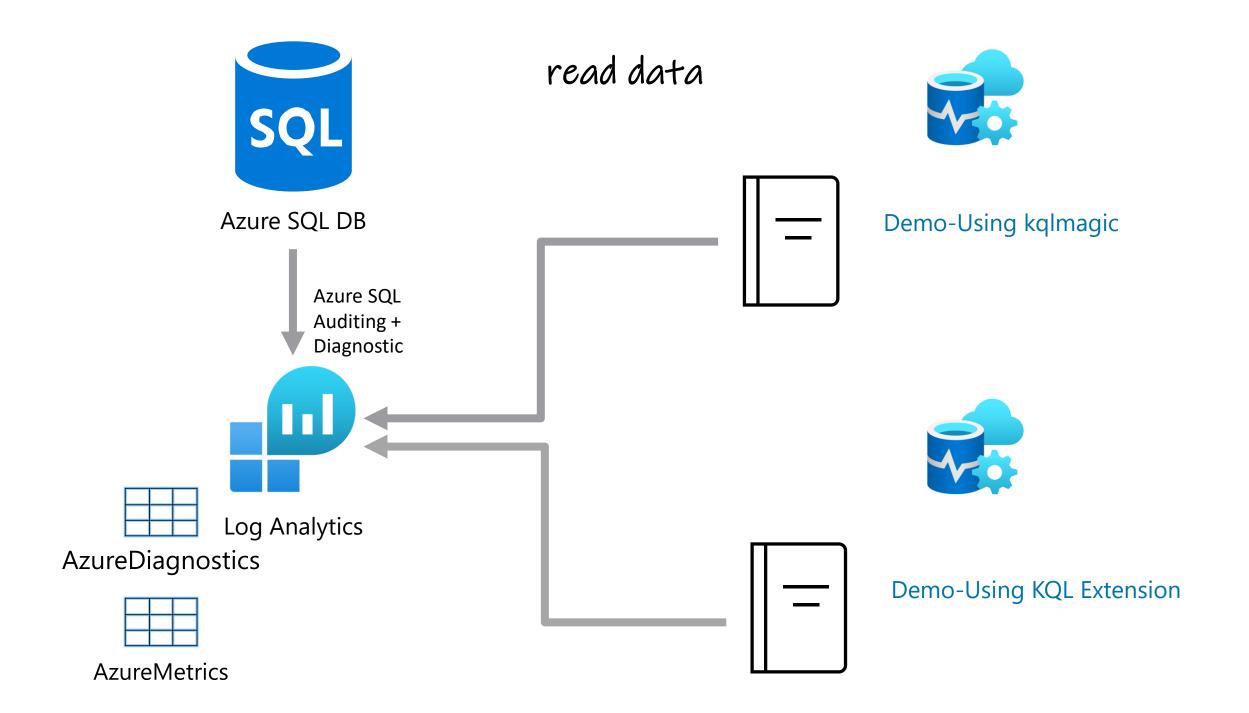












Not another one, can I use TSQL?

- ➤ Azure Monitor NO
- ➤ Azure Data Explorer YES

While <u>SQL Queries</u> to Kusto are supported, the primary means of interaction with Kusto is through the use of the <u>Kusto query</u> <u>language</u> to send data queries, and through the use of <u>control</u> <u>commands</u> to manage Kusto entities, discover metadata, etc.

Primary means of interaction with Kusto is through the use of the Kusto Query

Language

How can I learn?

Check the reference slide

Demo environment

- https://aka.ms/LADemo
- https://aka.ms/AlAnalyticsDemo
- https://aka.ms/WidDevATP



ADS 1.30.0 Azure Portal Azure SQL Database

Reference

- Azure Monitor overview
- Pluralsight course 'Kusto Query Language (KQL) from Scratch by Robert Cain
- Get started with log queries in Azure Monitor
- Common Query Samples
- Write queries for Azure Data Explorer
- SQL to Azure Monitor log query cheat sheet
- SQL to Analytics Language cheat sheet
- Azure AD Log Analytics KQL queries via API with PowerShell
- Operations Management Suite 101: Log Analytics Queries 101
- Log Analytics Advanced Queries by Marc Kean
- Kqlmagic extension in Azure Data Studio



@sqlworldwide



linkedin.com/in/sqlworldwide



sqlworldwide.com



taiob@sqlworldwide.com

