Mastering Kusto Query Language (KQL):
Your Gateway to Azure Monitoring and Insights

Taiob Ali

Taiob Ali

Database Solutions Manager @ GMO | Microsoft MVP | Global Data Solutions Leader | Cloud & AI Advocate

Let's connect and collaborate:

🌐 linkedin.com/in/sqlworldwide

📊 sqlworldwide.com

📧 taiob@sqlworldwide.com

🔷 @sqlworldwide.bsky.social

https://learn.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-overview?tabs=simple#introduction-video

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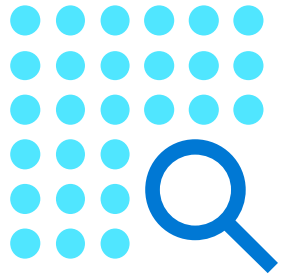
- Optimized **query language** with **visualization** options
- For **fast read-only** data retrieval
- **Troubleshooting** & deep diagnostics
- Real-time stream / big data **analytics**

Use KQL to connect and query these Azure Services:

Azure Data Explorer

Log Analytics

App Insights

Time Series Insights

Azure Monitor Logs

2014

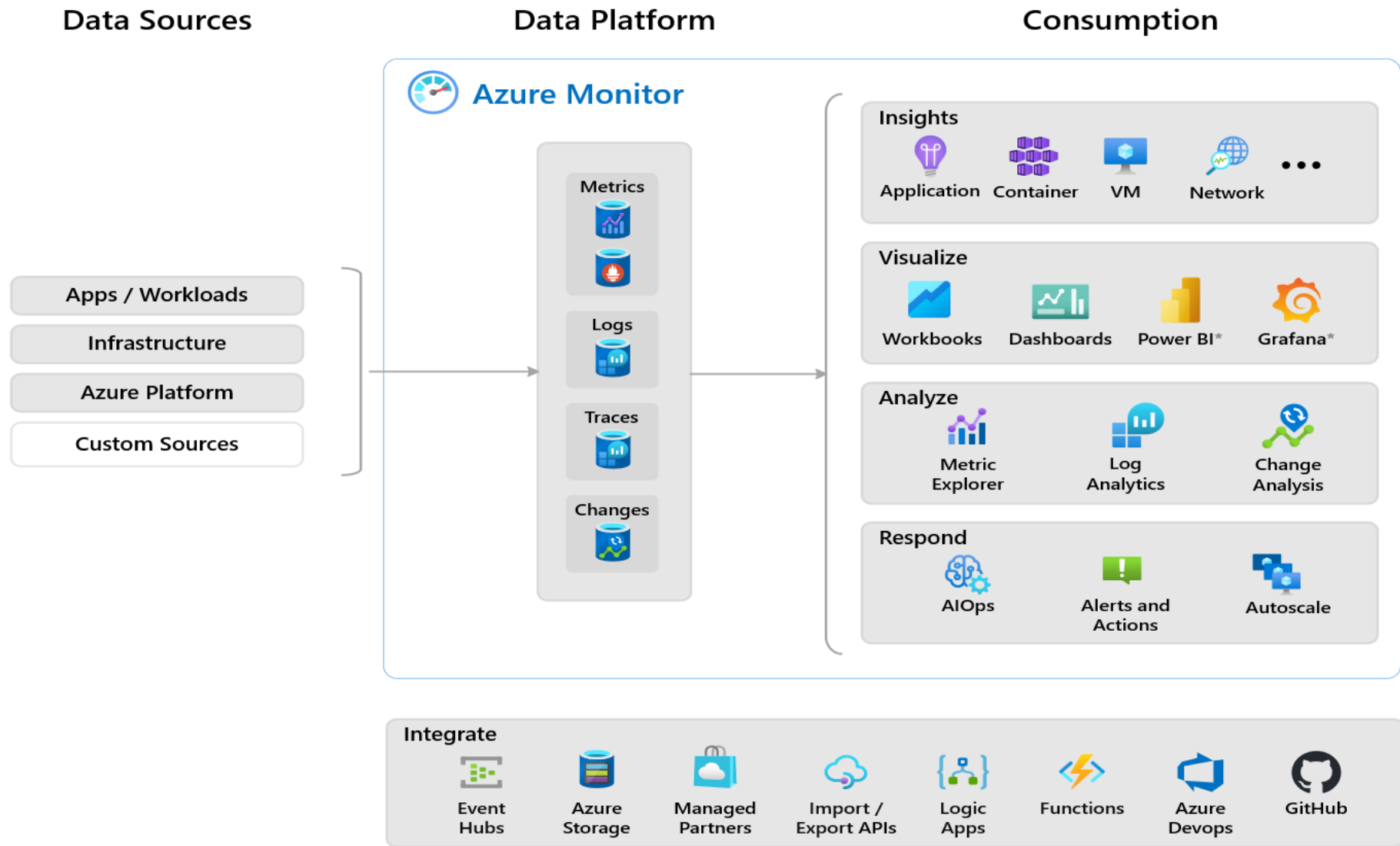Kusto started in 2014 as internal Microsoft project to address Azure services' needs

2016

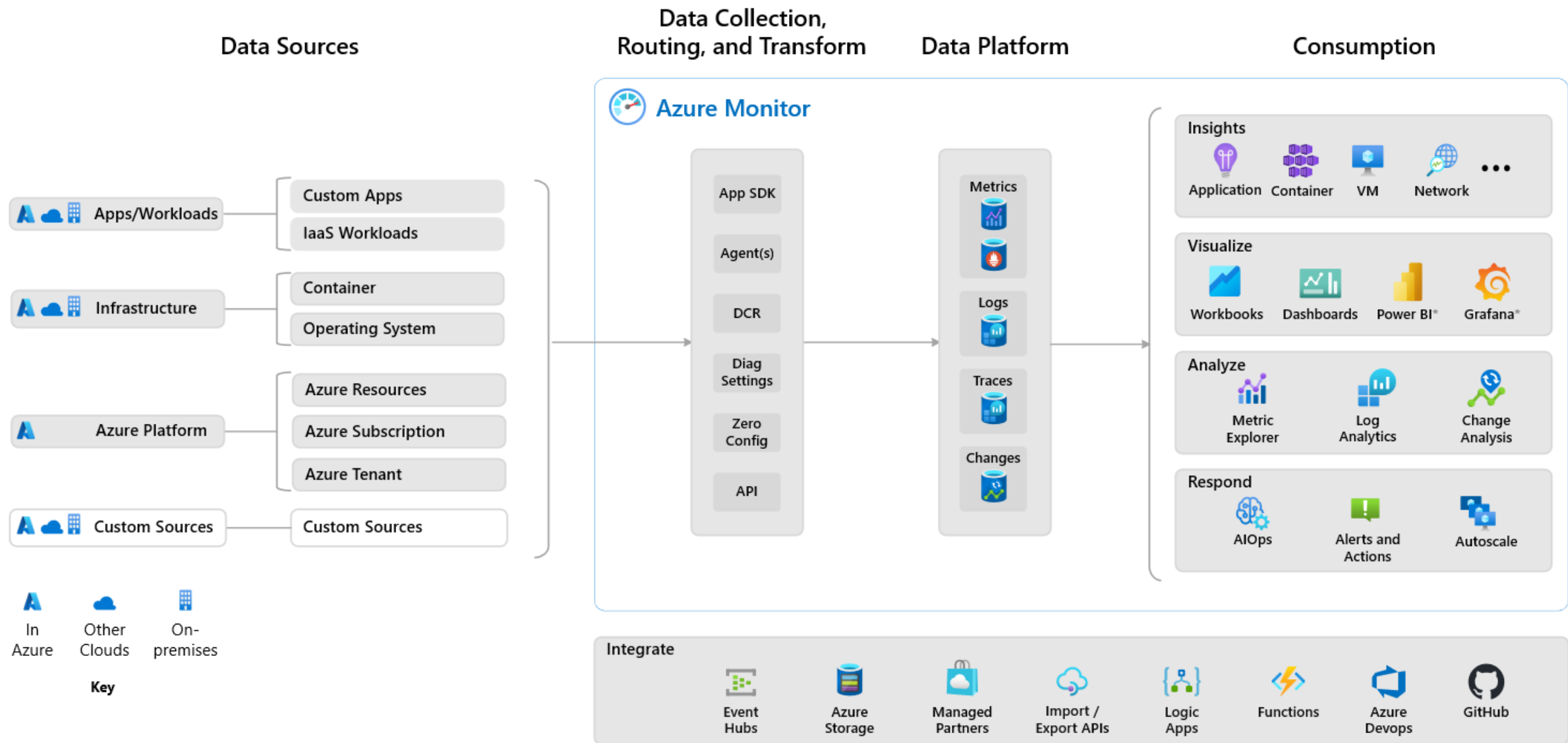It became a backend of Application Insights Analytics

2018

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

2020

General Availability announced, marking full production readiness and enterprise adoption

Data Sources · Data Platform · Consumption

Azure Monitor

Data Sources: Apps / Workloads, Infrastructure, Azure Platform, Custom Sources

Data Platform: Metrics, Logs, Traces, Changes

Consumption:
- Insights: Application, Container, VM, Network
- Visualize: Workbooks, Dashboards, Power BI*, Grafana*
- Analyze: Metric Explorer, Log Analytics, Change Analysis
- Respond: AIOps, Alerts and Actions, Autoscale

Integrate: Event Hubs, Azure Storage, Managed Partners, Import / Export APIs, Logic Apps, Functions, Azure Devops, GitHub

https://learn.microsoft.com/en-us/azure/azure-monitor/fundamentals/overview?

Azure Monitor architecture overview diagram

Data Sources

- Apps/Workloads
  - Custom Apps
  - IaaS Workloads
- Infrastructure
  - Container
  - Operating System
- Azure Platform
  - Azure Resources
  - Azure Subscription
  - Azure Tenant
- Custom Sources
  - Custom Sources

Key:
- In Azure
- Other Clouds
- On-premises

Data Collection, Routing, and Transform

Azure Monitor

- App SDK
- Agent(s)
- DCR
- Diag Settings
- Zero Config
- API

Data Platform

- Metrics
- Logs
- Traces
- Changes

Consumption

Insights
- Application
- Container
- VM
- Network
- ...

Visualize
- Workbooks
- Dashboards
- Power BI*
- Grafana*

Analyze
- Metric Explorer
- Log Analytics
- Change Analysis

Respond
- AIOps
- Alerts and Actions
- Autoscale

Integrate
- Event Hubs
- Azure Storage
- Managed Partners
- Import / Export APIs
- Logic Apps
- Functions
- Azure DevOps
- GitHub

https://learn.microsoft.com/en-us/azure/azure-monitor/fundamentals/overview?

Not another one, can I use TSQL?

➢Azure Monitor – NO
➢Azure Data Explorer - YES

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

Primary means of interaction with Kusto is using the Kusto Query Language

How can I learn?

Check the reference slide

Demo environment

- https://dataexplorer.azure.com/clusters/help/databases

Azure Portal

Azure Data Explorer

Azure SQL Database

https://www.invotide.com/demo

Reference

- [Azure Monitor overview](#)
- [Get started with log queries in Azure Monitor](#)
- [Tutorial: Learn common operators](#)
- [Tutorial: Use aggregation functions](#)
- [Tutorial: join data from multiple tables](#)
- [Tutorial: Create geospatial visualizations](#)
- [Tutorial: Create your first graphs in Kusto Query Language](#)
- [SQL to Kusto Query Language cheat sheet](#)
- [Azure Data Explorer documentation](#)
- [Kusto.Explorer installation and user interface](#)
- [Log Analytics Advanced Queries](#)by Marc Kean

Contact Information

LinkedIn

linkedin.com/in/sqlworldwide

Email

taiob@sqlworldwide.com

GitHub

github.com/sqlworldwide

Website

sqlworldwide.com

Bluesky

@sqlworldwide.bsky.social