Kusto - Azure Monitor Log Queries

Taiob Ali

CincyPass
@CincyPASS

August 19th, 2020

Data Solutions Manager, GMO LLC

http://sqlworldwide.com/

/sqlworldwide

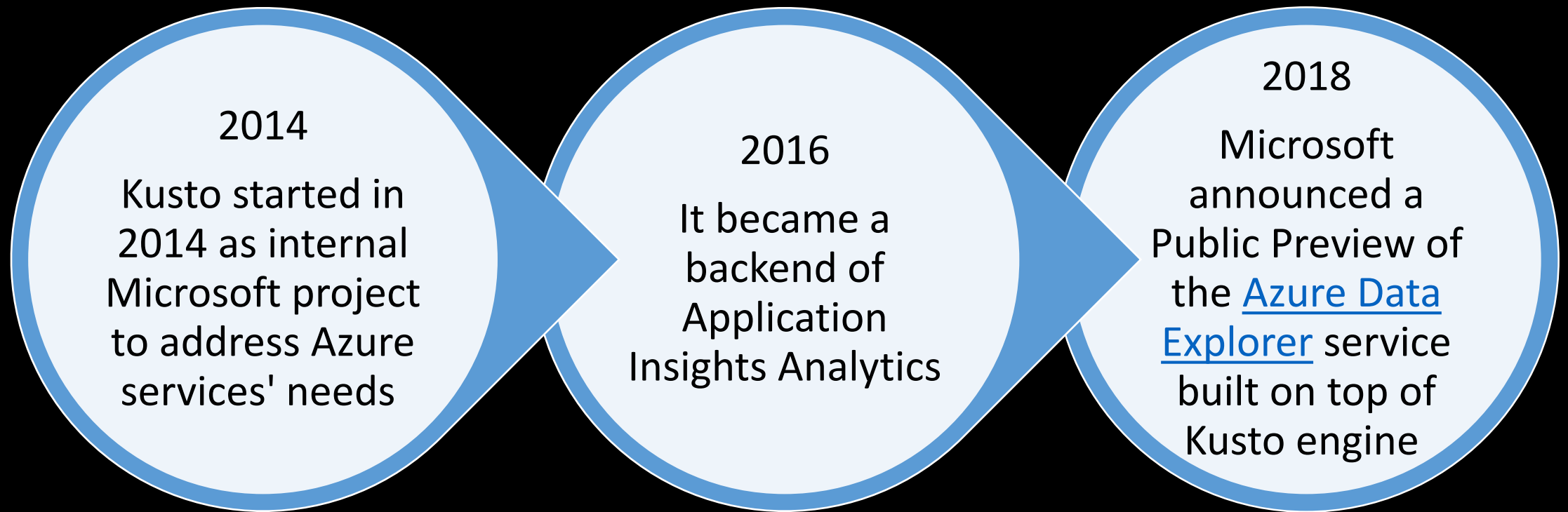@sqlworldwide

Taiob@sqlwroldwide.com

Data Professional

Microsoft Data Platform MVP. 14 Years working with Microsoft Data Platform. Microsoft and MongoDB certified. Worked in ecommerce, healthcare and finance industry.
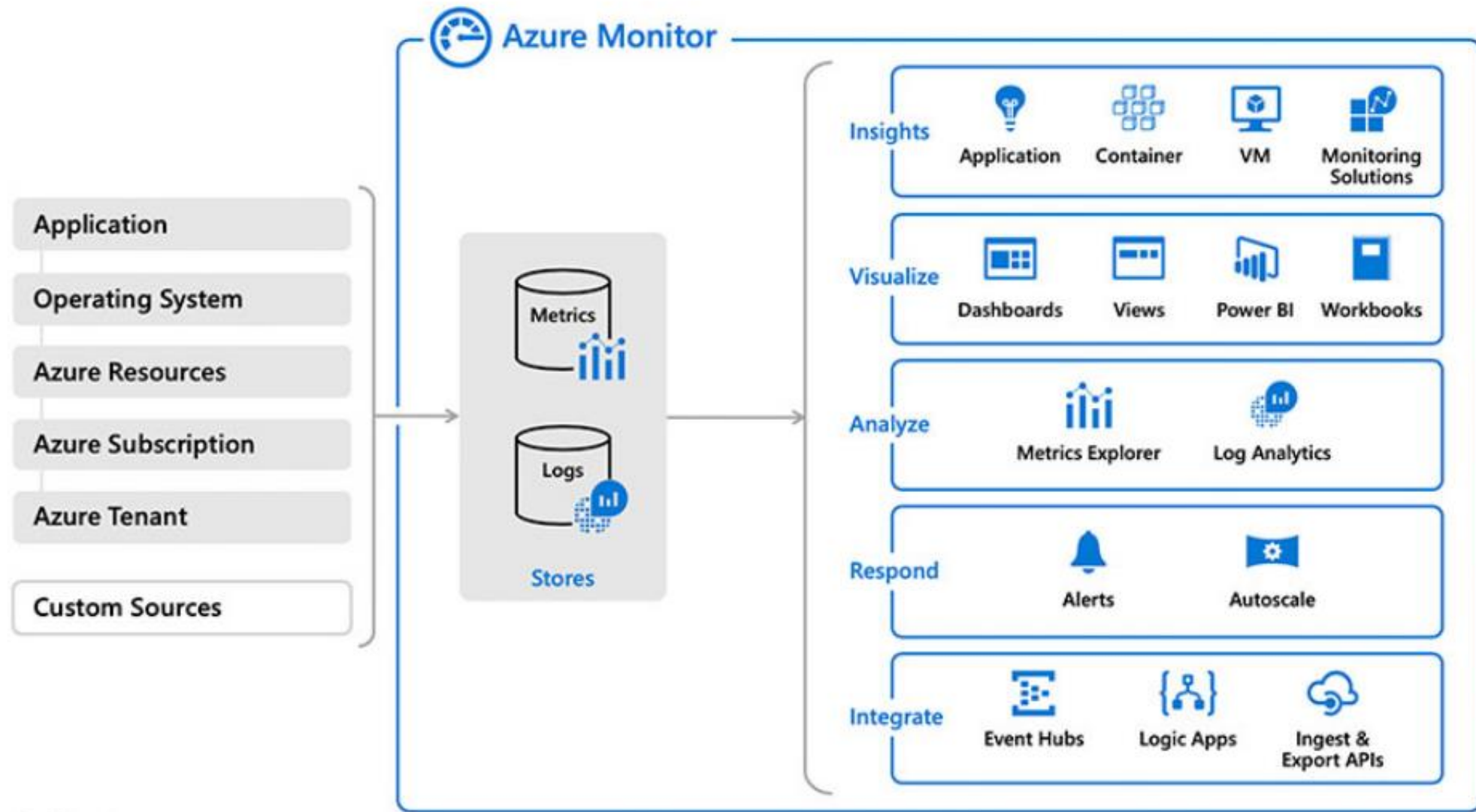
Giving Back

Board member NESQL user group and PASS DBA virtual group. Organizer of Boston SQL Saturday. Frequent speaker at local and virtual user groups, SQL Saturdays, and azure events.

When Not Working

Running – One 26.2 and many 13.1 miles. Learning US history. Shuttling 3 kids.
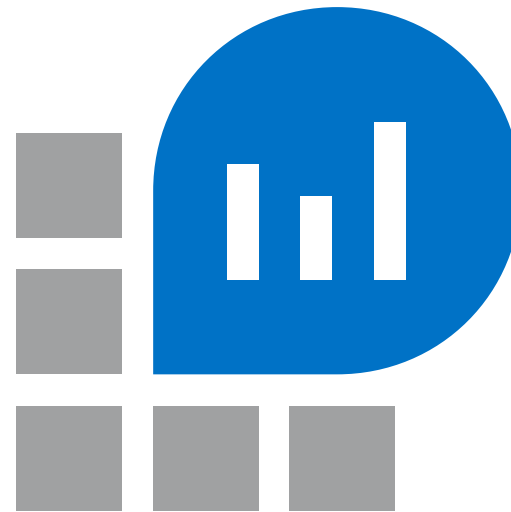
2014

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

https://docs.microsoft.com/en-us/azure/azure-monitor/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 through the use of the Kusto query language
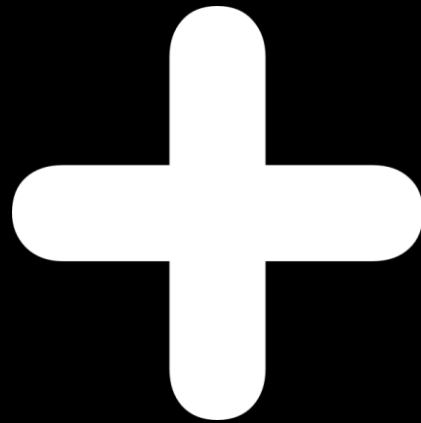
How can I learn?

Check the reference slide

Demo environment

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

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](#)

SQL2019 CU6

SSMS 18.6

ADS 1.21.0

VS Code 1.48.0

@SqlWorldWide

linkedin.com/in/sqlworldwide

sqlworldwide.com

taiob@sqlworldwide.com