Kusto - Azure Monitor Log Queries

Taiob Ali

Taiob Ali

Database Solutions Manager, GMO LLC

http://sqlworldwide.com/

/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.

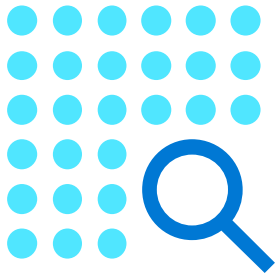
Giving Back

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



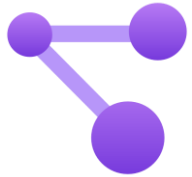
- Optimized **query language** with **visualization** options
- For **fast read-only** data retrieval
- **Troubleshooting** & deep diagnostics
- Real-time stream / big data **analytics**

Use KQL to connect and query these Azure Services:

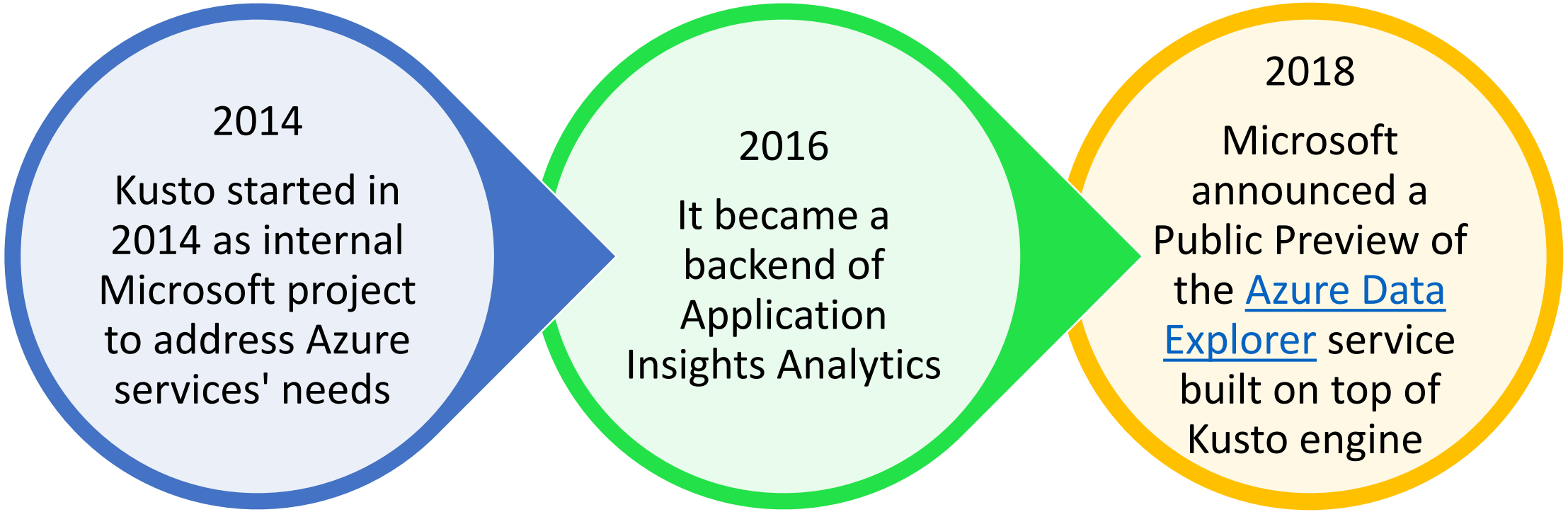
Azure Data Explorer

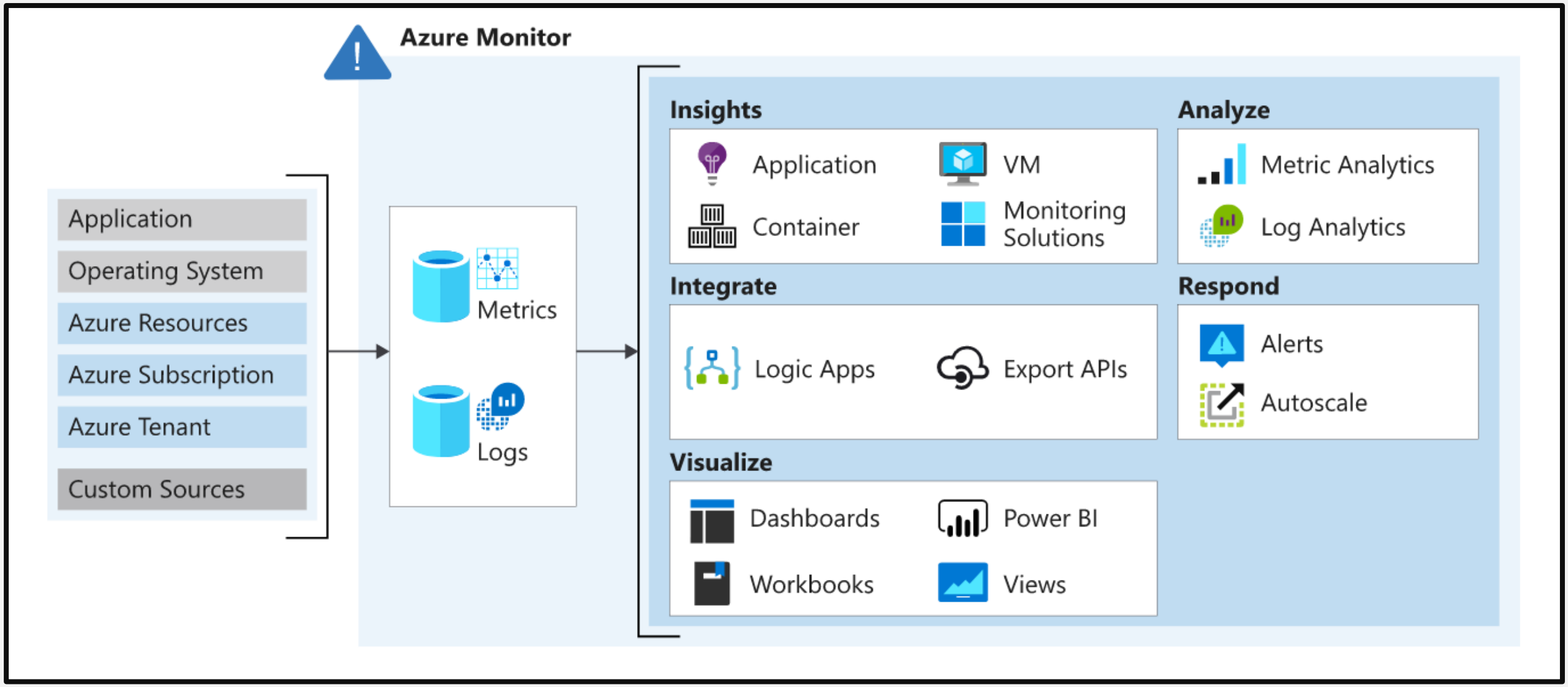
Log Analytics

App Insights



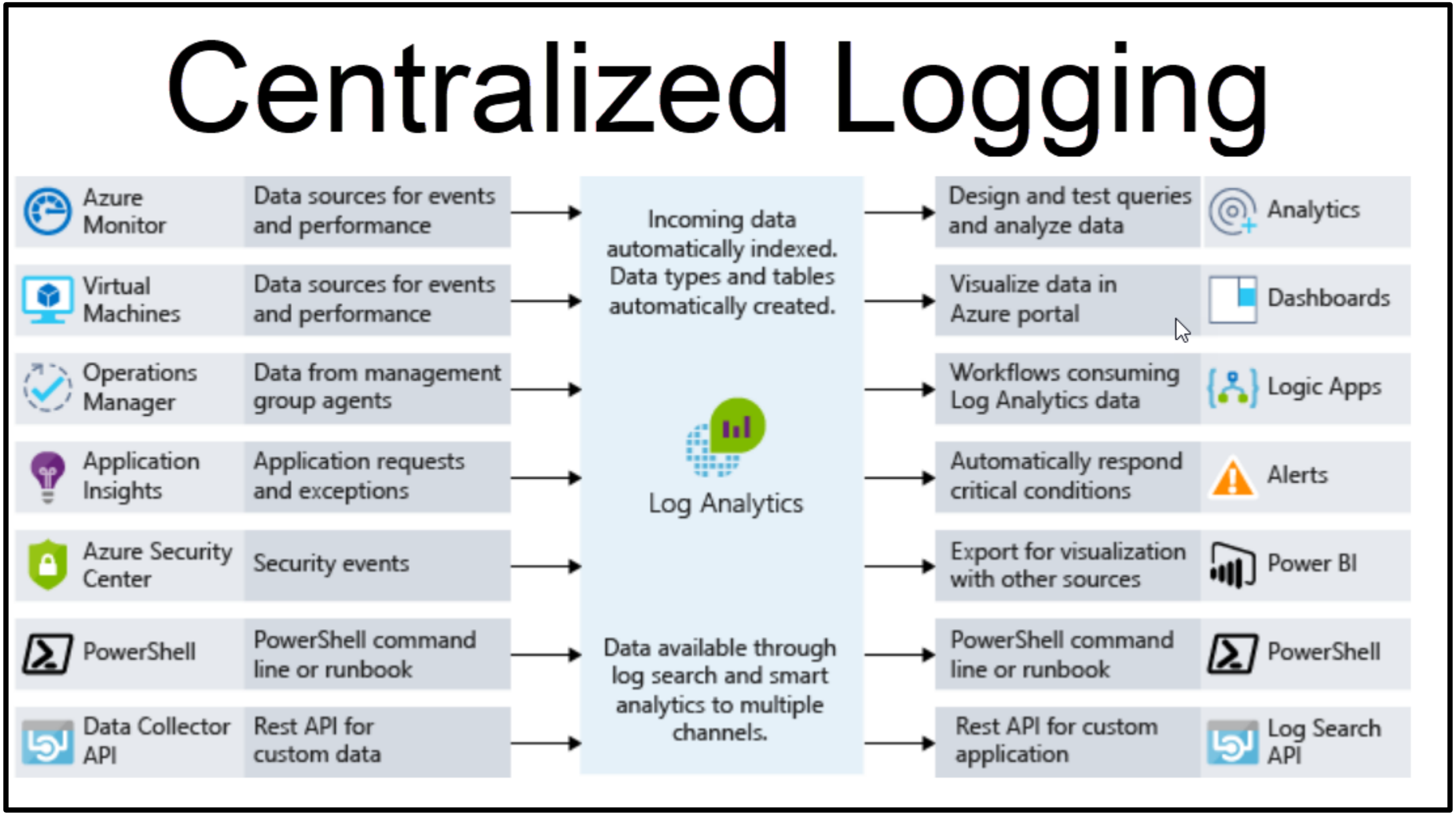
Resource Graph


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

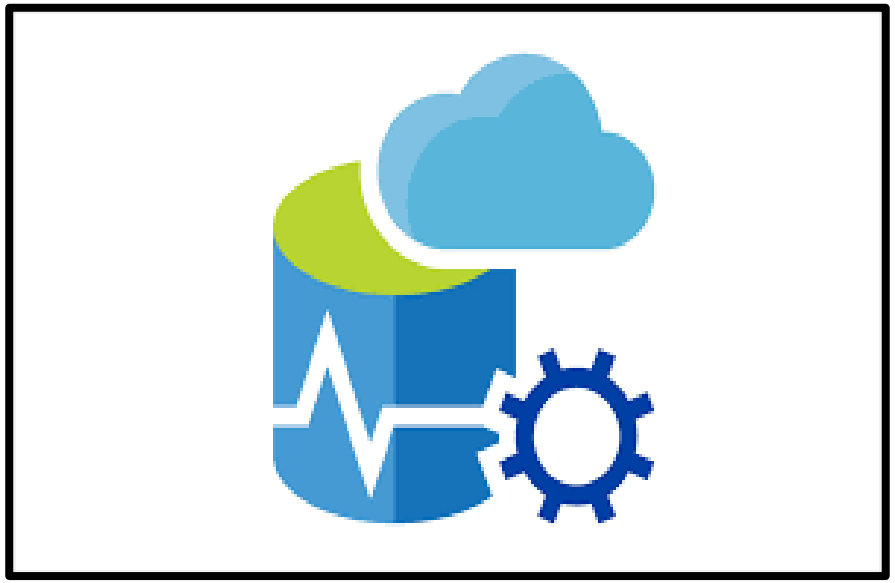


https://docs.microsoft.com/en-us/learn/modules/analyze-infrastructure-with-azure-monitor-logs/2-features-azure-monitor-log

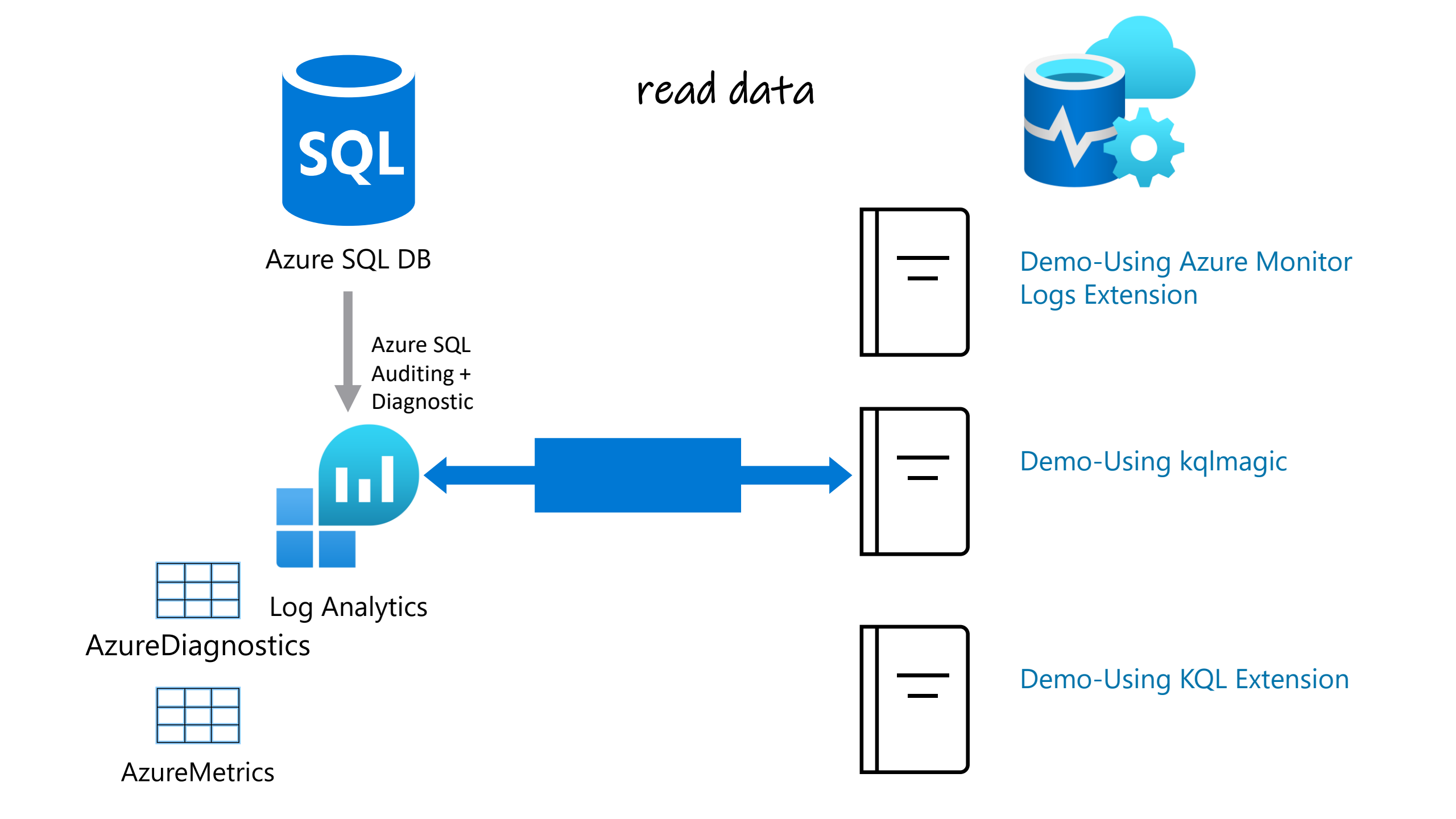
Centralized Logging



https://docs.microsoft.com/en-us/learn/modules/azure-well-architected-performance-efficiency/5-identify-performance-bottlenecks-in-your-application



kql


read data
Azure SQL DB
Azure SQL
Auditing +
Diagnostic
Log Analytics
AzureDiagnostics
AzureMetrics
Demo-Using Azure Monitor
Logs Extension
Demo-Using kqlmagic
Demo-Using KQL Extension

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

ADS 1.32.0
Azure Portal
Azure SQL Database

https://www.invotide.com/demo

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

THANK
YOU