The Sixth Sense:
Using Log Analytics To Efficiently Manage Your Azure Environment

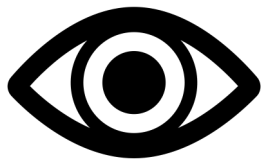
quorum

quorum

quorum

quorum

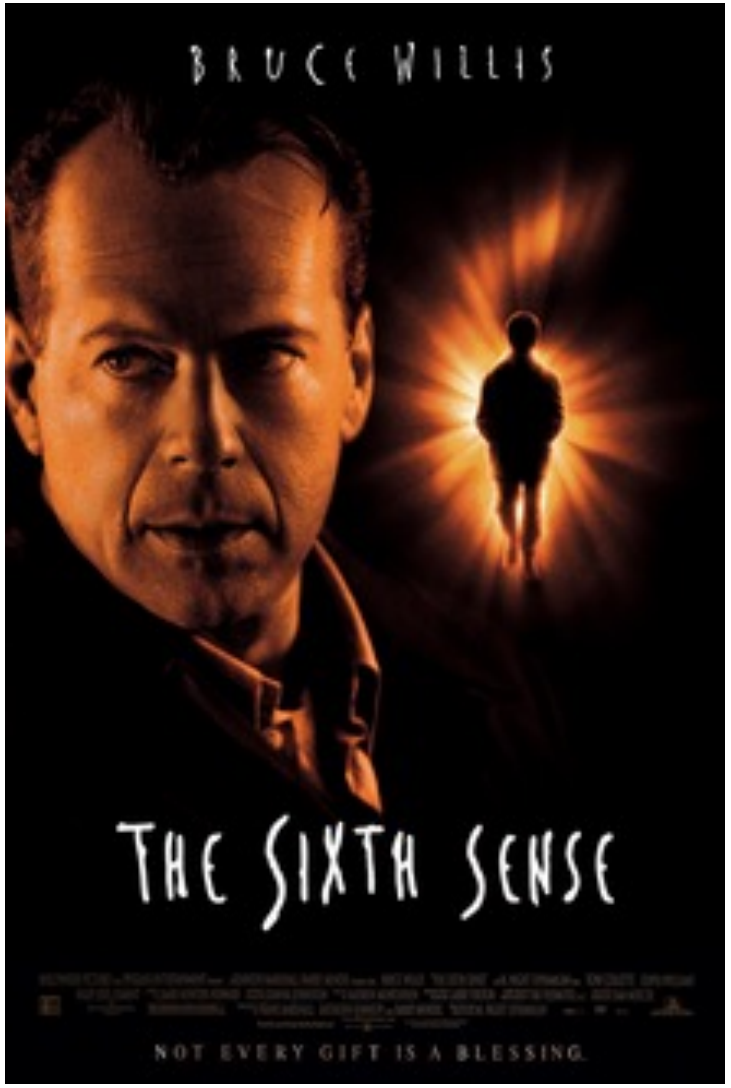
Make Sense?





quorum

Make Sense?



Abhi Jayanty

Data Engineer

E-Mail:
abhi.jayanty@quorum.co.uk

Twitter:
@data_abhinavj

LinkedIn:
Abhinav Jayanty

quorum

The terminology

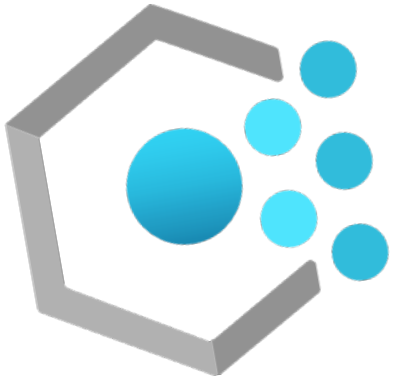
What are we actually talking about?

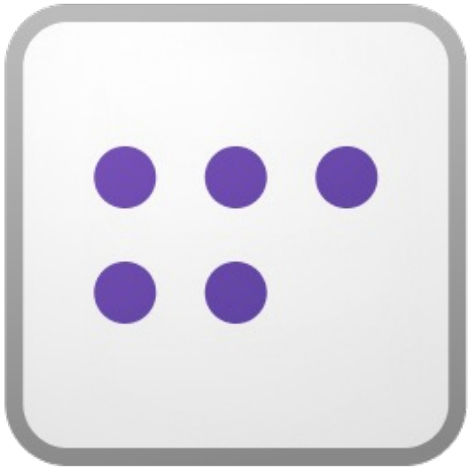
quorum

What are Azure's monitoring offerings?

- *What can be monitored?*
- *What should I use, and why?*

quorum





quorum

Azure Monitor

quorum

Azure Monitor

Azure Monitor can monitor resources in Azure, other clouds, or on-premises:

- Applications
- Virtual machines
- Databases
- Security events in combination with Azure Sentinel
- Networking events and health
- Guest OS, containers, custom sources using API

quorum

Monitor | Overview

Microsoft

Search

Overview
Activity log
Alerts
Metrics
Logs
Change Analysis
Service Health
Workbooks

Insights

Applications
Virtual Machines
Storage accounts
Containers
Networks
SQL (preview)
Azure Cosmos DB
Key Vaults
Azure Cache for Redis
Azure Data Explorer Clusters

Overview | Tutorials | What's new

Insights

Use curated monitoring views for specific Azure resources. View all insights

Application insights

Monitor your app's availability, performance, errors, and usage.

View ··· More

Container Insights

Gain visibility into the performance and health of your controllers, nodes, and containers.

View ··· More

VM Insights

Monitor the health, performance, and dependencies of your VMs and VM scale sets.

View ··· More

Network Insights

View the health and metrics for all deployed network resources.

View ··· More

Detection, triage, and diagnosis

Visualize, analyze, and respond to monitoring data and events. Learn more about monitoring

Metrics

Create charts to monitor and investigate the usage and performance of your Azure resources.

View ··· More

Alerts

Get notified and respond using alerts and actions.

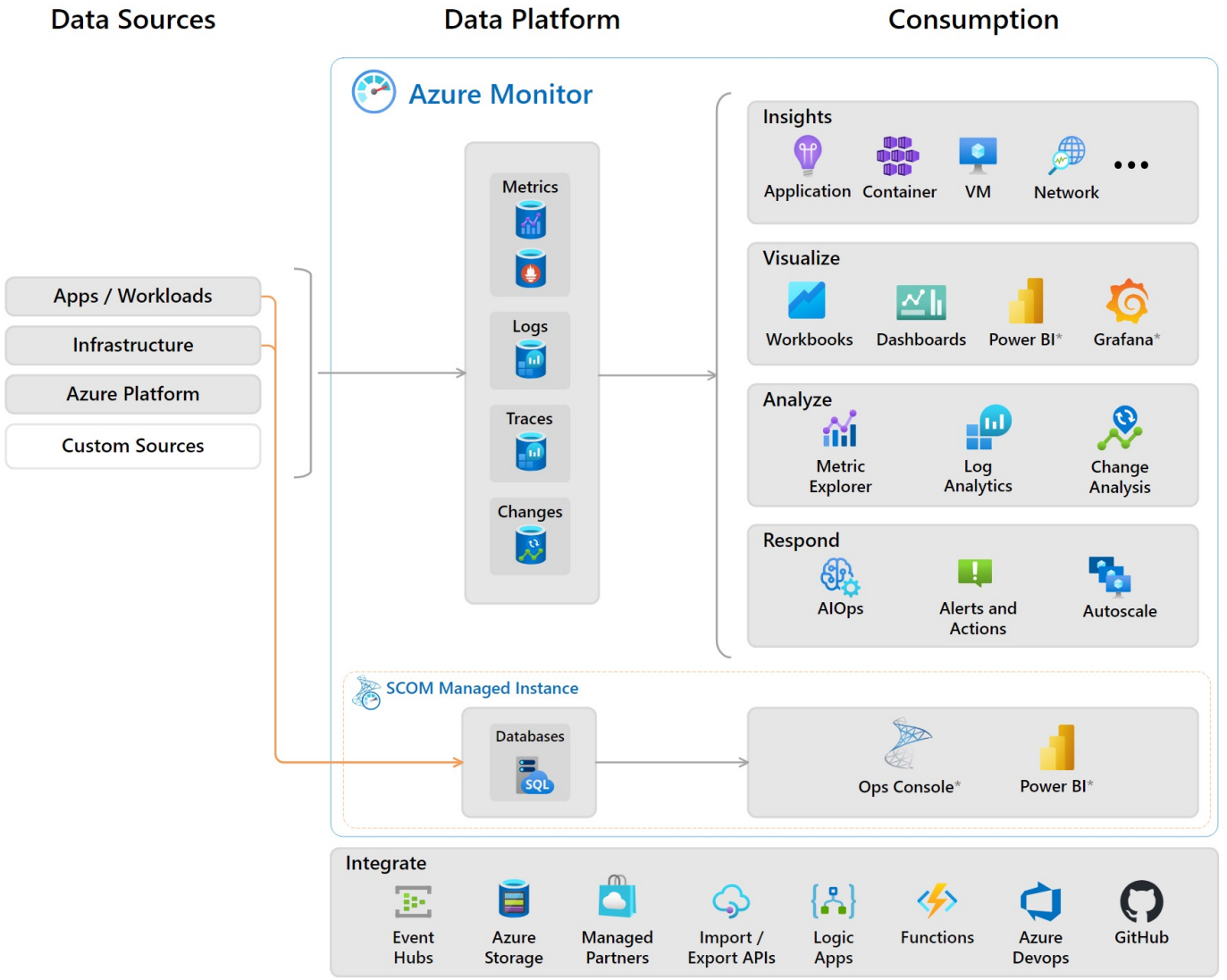
View ··· More

Logs

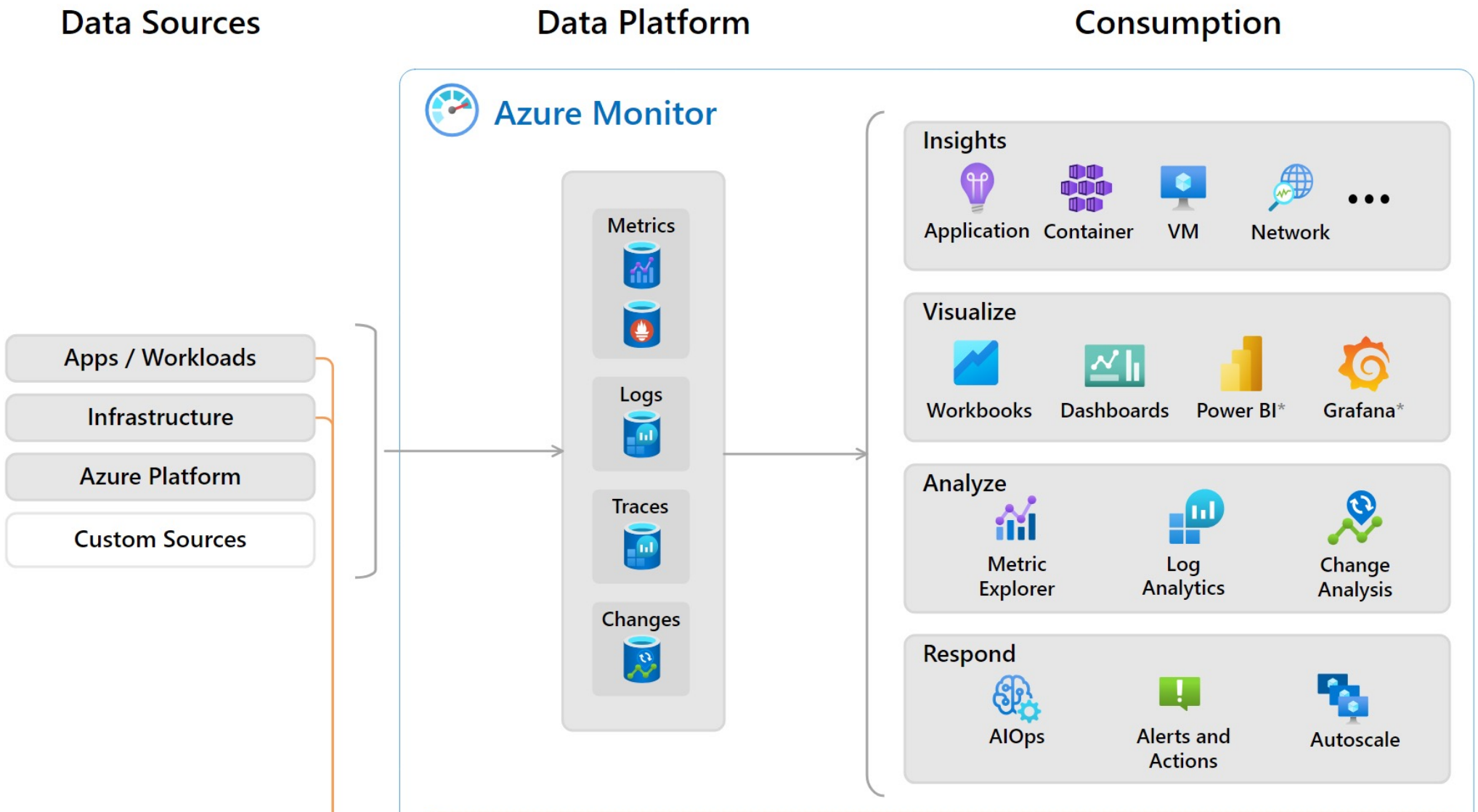
Analyze and diagnose issues with log queries.

View ··· More

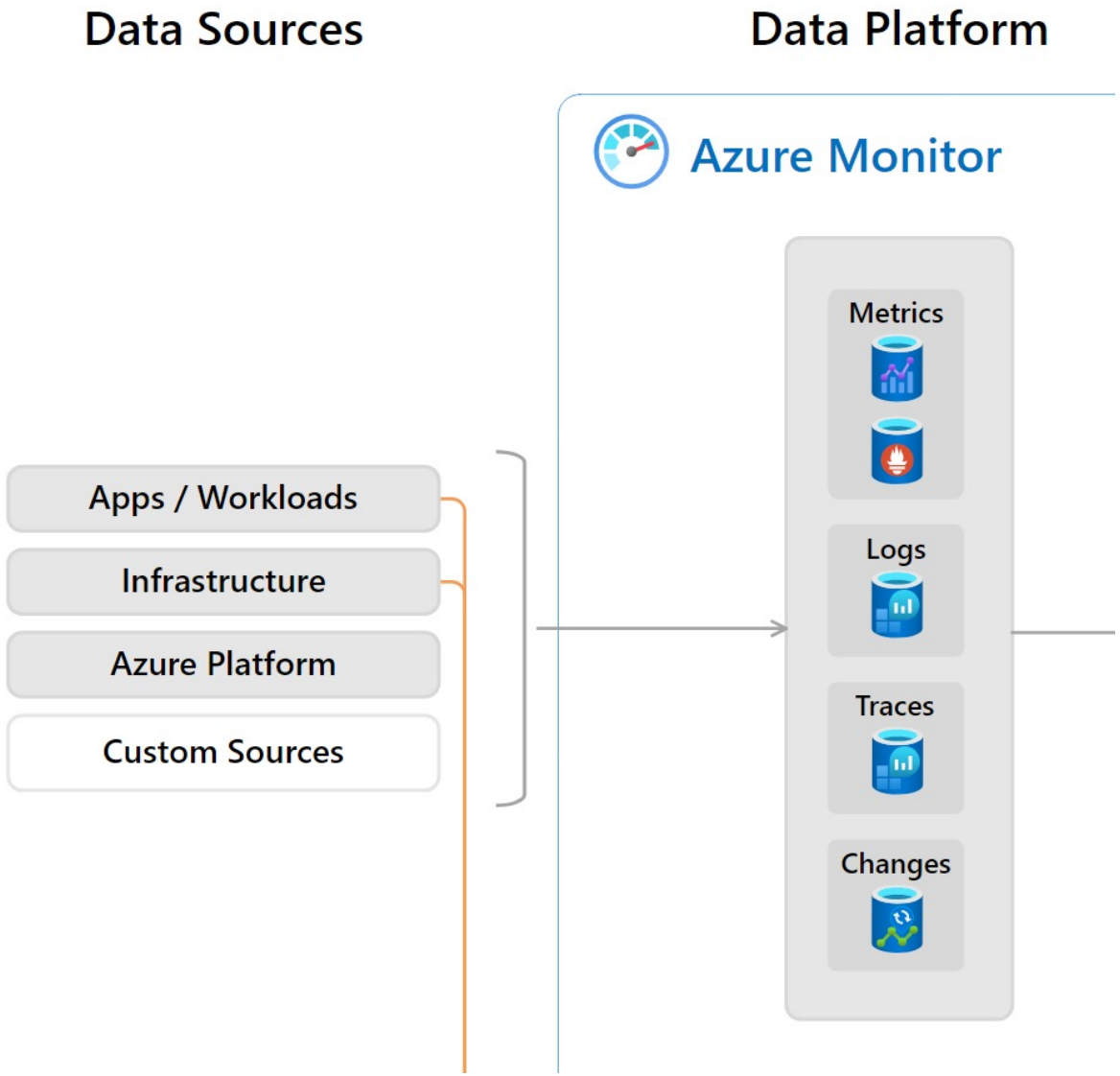
quorum


Data Sources
Data Platform
Consumption
Azure Monitor
Apps / Workloads
Infrastructure
Azure Platform
Custom Sources
Metrics
Logs
Traces
Changes
Insights
Application
Container
VM
Network
Visualize
Workbooks
Dashboards
Power BI*
Grafana*
Analyze
Metric Explorer
Log Analytics
Change Analysis
Respond
AIOps
Alerts and Actions
Autoscale
SCOM Managed Instance
Databases
SQL
Ops Console*
Power BI*
Integrate
Event Hubs
Azure Storage
Managed Partners
Import / Export APIs
Logic Apps
Functions
Azure Devops
GitHub

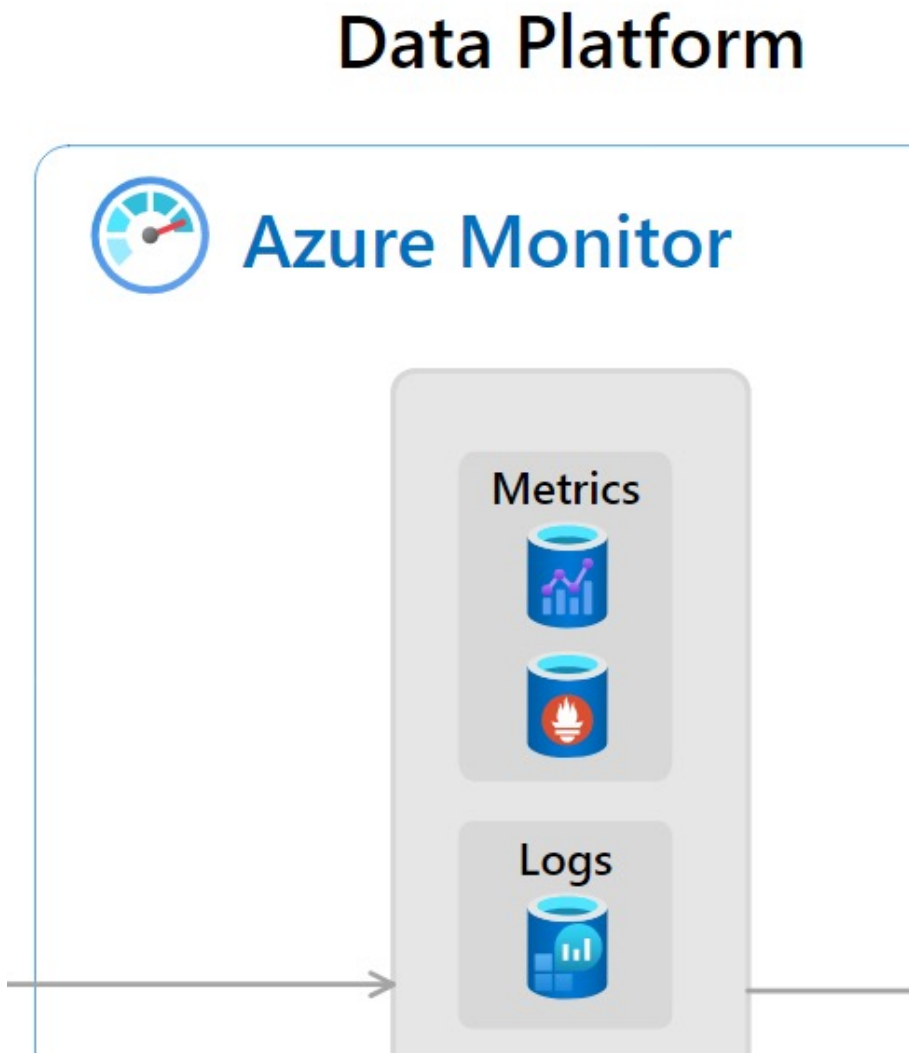
quorum


Data Sources
Data Platform
Consumption
Azure Monitor
Apps / Workloads
Infrastructure
Azure Platform
Custom Sources
Metrics
Logs
Traces
Changes
Insights
Application
Container
VM
Network
Visualize
Workbooks
Dashboards
Power BI*
Grafana*
Analyze
Metric Explorer
Log Analytics
Change Analysis
Respond
AIOps
Alerts and Actions
Autoscale

quorum


Data Sources
Data Platform
Azure Monitor
Apps / Workloads
Infrastructure
Azure Platform
Custom Sources
Metrics
Logs
Traces
Changes

quorum



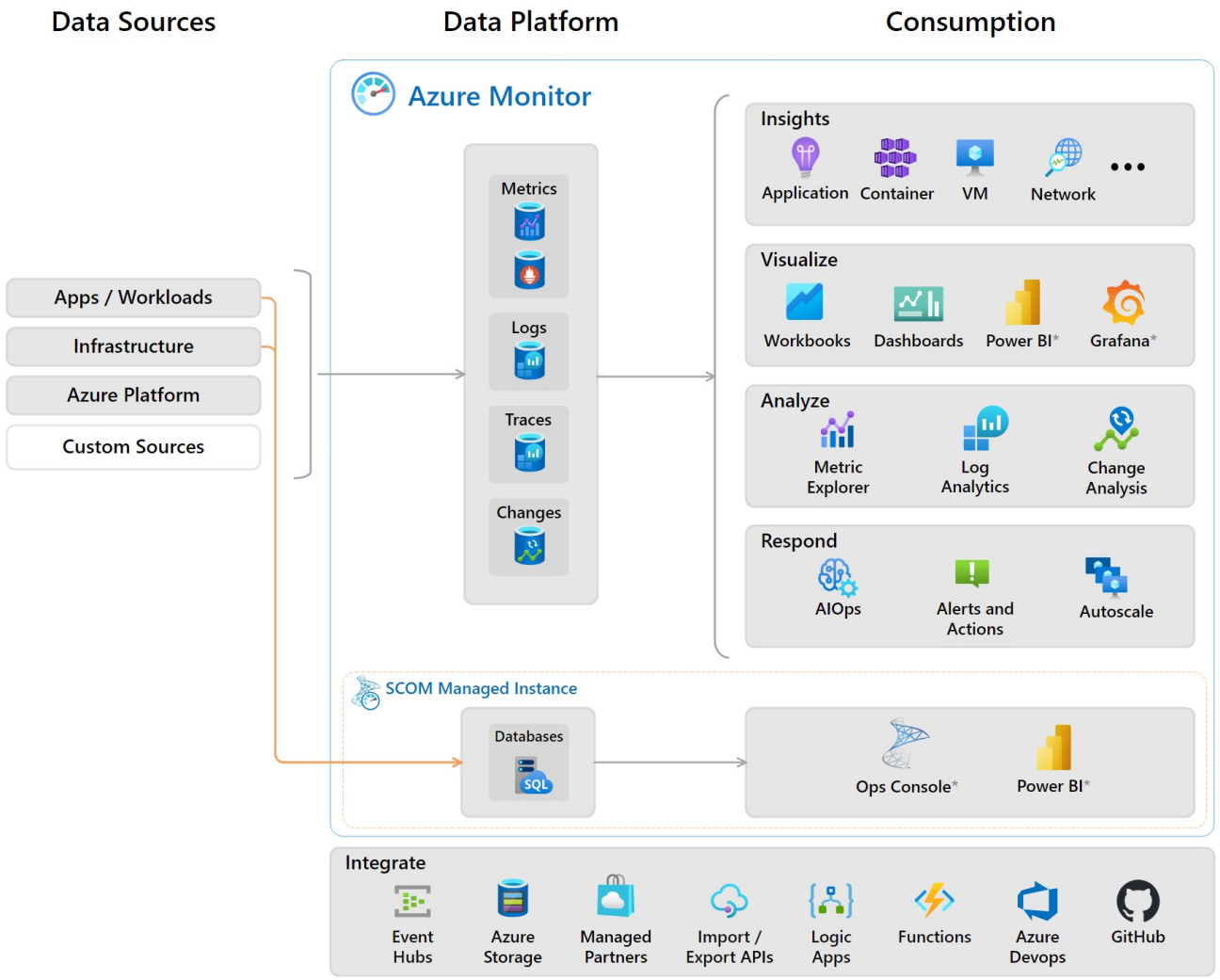
Metrics

- Numerical values that describe an aspect of a system at a particular point in time
- Stored in Azure Monitor Metrics, a time-series database

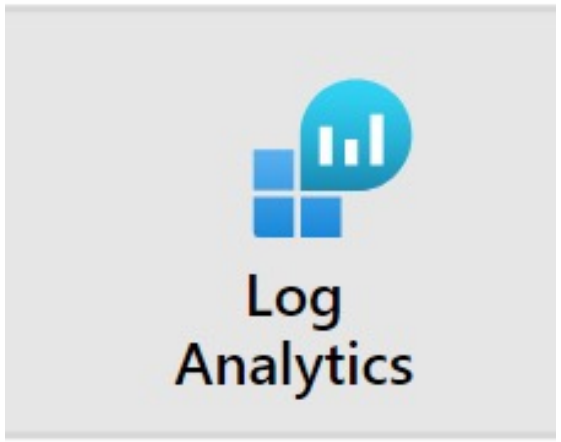
Logs

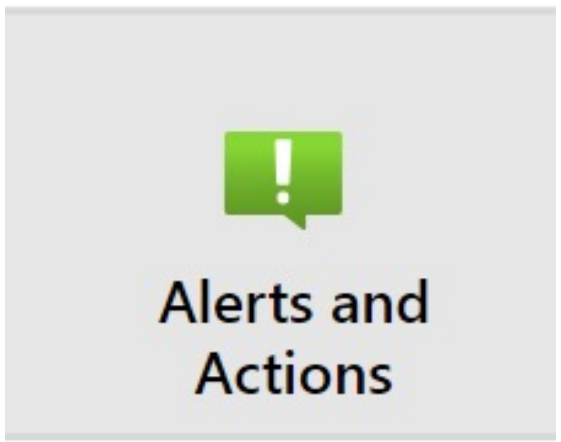
- Recorded system events, containing different types of data and activity.
- Logs can structured or free-form text, with a timestamp.

quorum


Data Sources
Data Platform
Consumption
Azure Monitor
Apps / Workloads
Infrastructure
Azure Platform
Custom Sources
Metrics
Logs
Traces
Changes
Insights
Application
Container
VM
Network
Visualize
Workbooks
Dashboards
Power BI*
Grafana*
Analyze
Metric Explorer
Log Analytics
Change Analysis
Respond
AIOps
Alerts and Actions
Autoscale
SCOM Managed Instance
Databases
SQL
Ops Console*
Power BI*
Integrate
Event Hubs
Azure Storage
Managed Partners
Import / Export APIs
Logic Apps
Functions
Azure Devops
GitHub

quorum





quorum

Agenda

Getting started with Log Analytics

- *Setup*
- *Kusto Query Language (KQL) basics*
- *Custom alerts*
- *Use-cases and business scenarios*

Demo Time

Ride into the danger zone…

quorum

Setting up & using Log Analytics

Workspace

Diagnostic Settings

Activity Log

quorum

Setting up & using Log Analytics

Workspace

- Out-of-the-box queries and insights
- Default data retention at workspace-level is 30 days
  - This can be increased to 730
- Pricing is per-GB/per-day of retention
- Data export to event hubs and storage accounts

Diagnostic Settings

Activity Log

quorum

Setting up & using Log Analytics

Workspace

- Out-of-the-box queries and insights
- Default data retention at workspace-level is 30 days
  - This can be increased to 730
- Pricing is per-GB/per-day of retention
- Data export to event hubs and storage accounts

Diagnostic Settings

- Resource logs are not collected by default.
- The setting defines the collection of the logs!
- Resource logs can be sent to LA as the AzureDiagnostics table, or resource-specific
  - All Azure services will eventually migrate to the resource-specific mode

Activity Log

quorum

Setting up & using Log Analytics

Workspace

- Out-of-the-box queries and insights
- Default data retention at workspace-level is 30 days
  - This can be increased to 730
- Pricing is per-GB/per-day of retention
- Data export to event hubs and storage accounts

Diagnostic Settings

- Resource logs are not collected by default.
- The setting defines the collection of the logs!
- Resource logs can be sent to LA as the AzureDiagnostics table, or resource-specific
  - All Azure services will eventually migrate to the resource-specific mode

Activity Log

- Lists changes and 'events' in resources
- Appears in *almost* every Azure resource
- No code or queries required for basic filtering of resource activity over a set time range

Kusto Query Language

"An ocean of data"

quorum

Kusto Query Language

Jacques Cousteau

French naval officer, oceanographer

Co-invented the first successful open-circuit self-contained underwater breathing apparatus

quorum

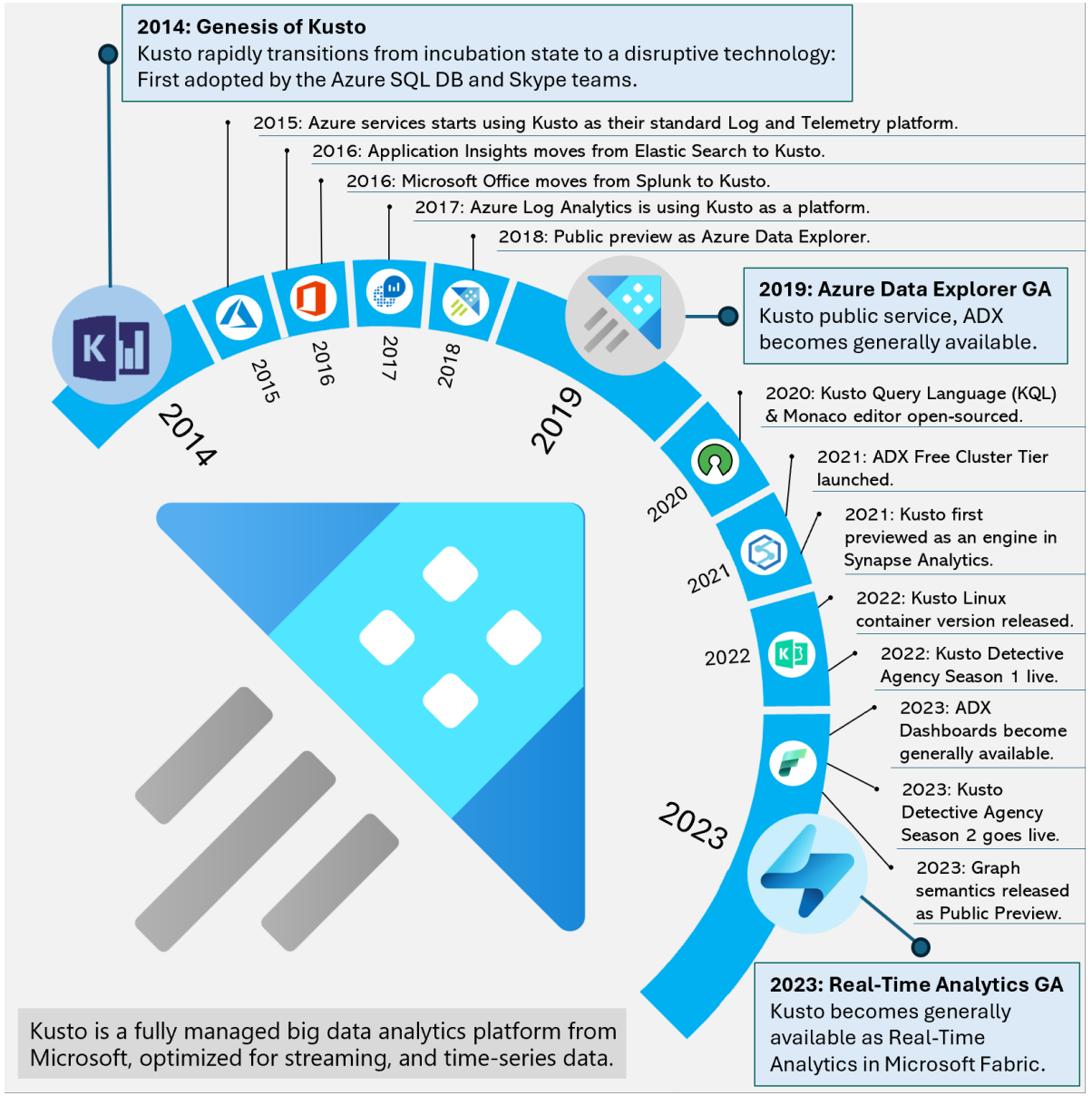
Kusto




Kusto is a fully-managed big data analytics platform, optimised for streaming and time-series data

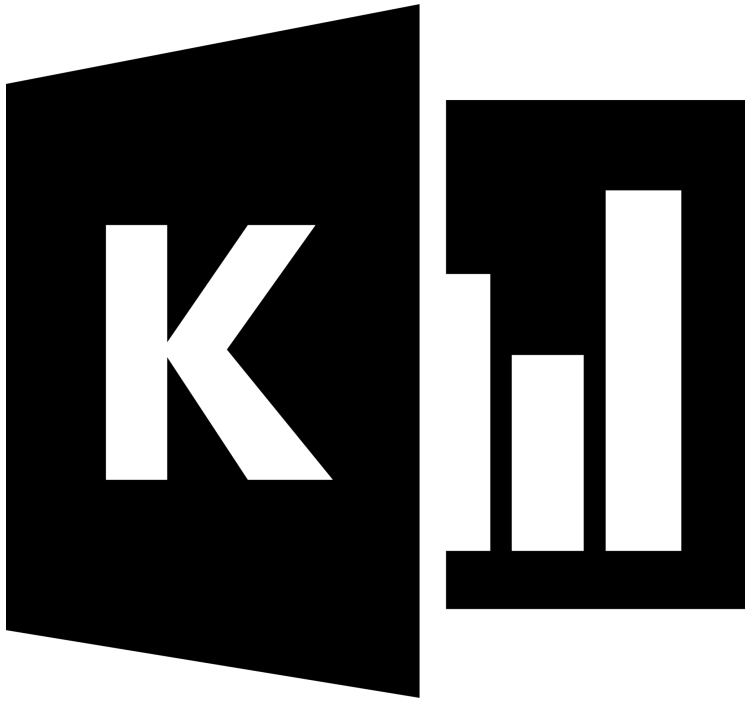
quorum

Kusto



quorum

Kusto Query Language



Kusto supports:

- Structured, semi-structured and unstructured data
- Text search and parsing
- Machine learning functions (anomaly detection)
- Rendered visuals for queries – charts, heatmaps etc.
- Geospatial, vector similarity, graph operators and more…

quorum

Comparisons to SQL

Writing SQL

SELECT

FROM

WHERE

GROUP BY

ORDER BY

LIMIT

Executing SQL

FROM

WHERE

GROUP BY

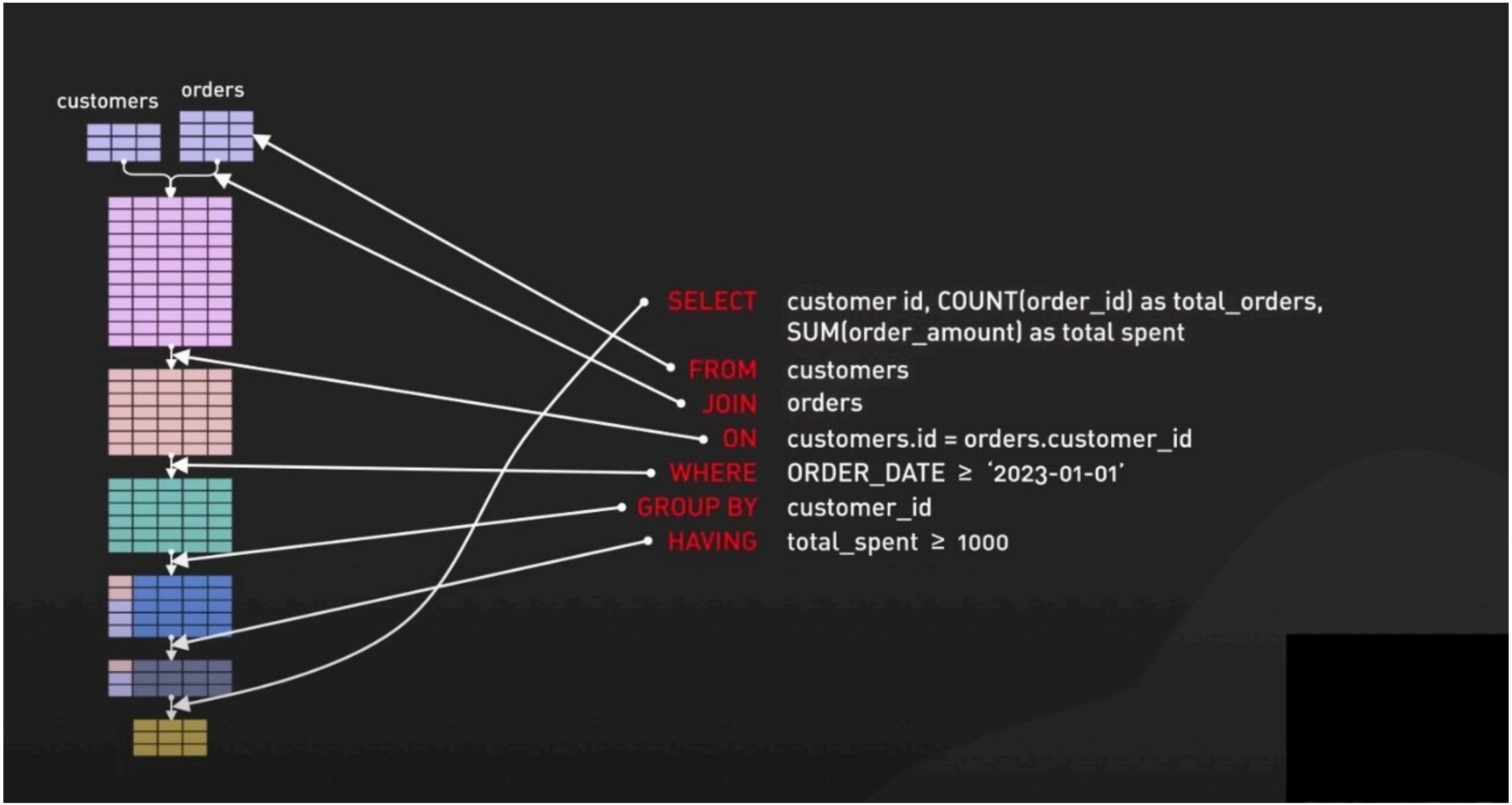
SELECT

ORDER BY

LIMIT

quorum

Comparisons to SQL



quorum

Comparisons to SQL

Writing SQL

SELECT

FROM

WHERE

GROUP BY

ORDER BY

LIMIT

Executing SQL

FROM

WHERE

GROUP BY

SELECT

ORDER BY

LIMIT

quorum

Comparisons to SQL

Executing SQL

FROM

WHERE

GROUP BY

SELECT

ORDER BY

LIMIT

quorum

Comparisons to SQL

Writing *and* Executing KQL

FROM

WHERE

GROUP BY

SELECT

ORDER BY

LIMIT

quorum

Query Examples

SQL

```
SELECT
      [column1],
      count(*)
  FROM [table]
WHERE [column1] = x
GROUP BY [column1]
ORDER BY [column1] desc
LIMIT 10
```

KQL

```
[table]
| where column1 == x
| summarize count() by column1
| project column1
| order by column1 desc
| limit 10
```

Alerts

“Mayday Mayday”

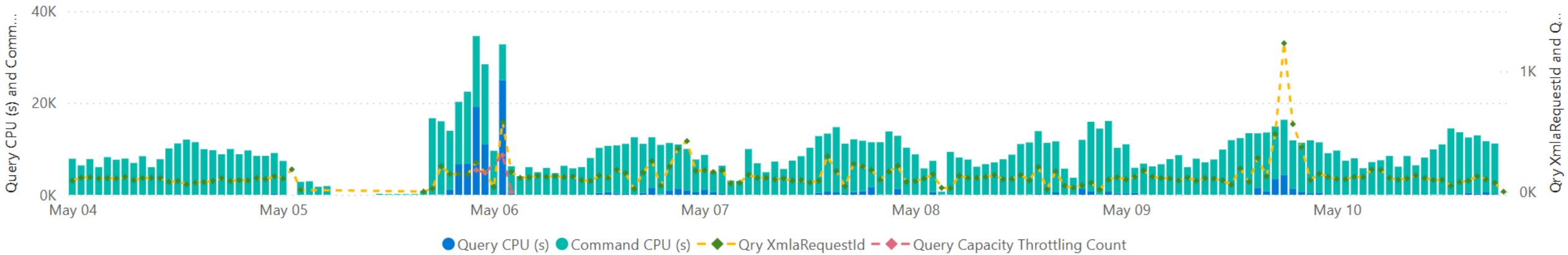
Other Cool Things

Fabric Analysis Services Engine

Last Event: 2024-05-10 14:05

33	22	5.1	6.6	405	204	44,698,081
Users	Semantic Models	Avg Query CPU (s)	Avg Query Duration (s)	Avg Cmd/Refresh CPU (s)	Avg Cmd/Refresh Duration (s)	Event Count
Capacities 2	Dataset Count 17	Qry XmlaRequestId 20,837	Max Qry Duration (s) 255	Cmd XmlaRequestId 3,388	Max Cmd Duration (s) 1,683	XmlaRequestId Cnt 93,016
Workspaces 2	Report Count 17	Failed Query 765 3.7%	Qry Peak Mem (MB) 10,240	Failed Command 330 9.7%	Cmd Peak Mem (MB) 29,647	Failed Requests 1,225 1.3%

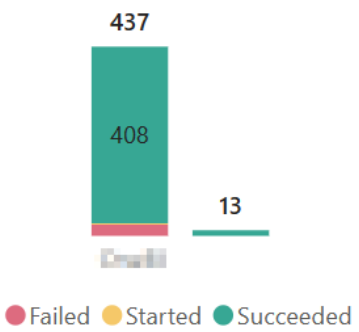
Query CPU (s), Command CPU (s), Qry XmlaRequestId and Query Capacity Throttling Count by DateTime(Hour)



Semantic Model Id	Semantic Model Name	Total CPU (s)	Execution From	Query CPU (s)	Query Count	Failed Qry %	Capacity Thrl Cnt	User Count	Report Count	Max Qry CPU (s)	Avg Qry Dur (s)	Max Qry Dur (s)	Direct Qry Cnt	Command CPU (s)	Command Count	Failed Cmd %	Avg Cmd Dur (s)
[redacted]	[redacted]	74,377	2024-05-05 13:16	70,831	1,249	10.4%	583	1	1	214	77.9	226		3,509	12		505
[redacted]	[redacted]	307,496	2024-05-03 14:01	10,124	3,636	8.4%		21	3	210	2.4	110		285,458	385	14.0%	365
[redacted]	[redacted]	341,460	2024-05-03 14:17	9,756	3,295	1.7%		8	1	368	1.4	184		318,039	439	3.9%	292
[redacted]	[redacted]	400,826	2024-05-03 14:03	3,856	2,392	2.0%		7	1	335	1.1	226		377,688	458	7.6%	340
[redacted]	[redacted]	3,205	2024-05-03 15:47	2,700	497	6.0%		16	2	190	4.6	135		323	1		379
[redacted]	[redacted]	10,243	2024-05-03 15:52	2,602	170	12.4%		6	1	188	17.1	98		607	11	90.9%	60
[redacted]	[redacted]	65,175	2024-05-03 14:12	1,884	3,036	1.1%		11	1	88	0.9	162		60,356	348	3.2%	131
[redacted]	[redacted]	2,087	2024-05-04 23:34	1,843	261	4.2%		5	1	94	4.5	65		167	1		204
[redacted]	[redacted]	72,940	2024-05-03 14:15	1,843	1,603	0.7%		4	1	225	1.0	55		67,713	348	5.5%	148
[redacted]	[redacted]	37,465	2024-05-03 14:13	865	1,705	1.6%		2	1	129	0.5	124		34,985	429	2.1%	51
Total		**1,546,343**	**2024-05-03 14:01**	**107,047**	**20,837**	**3.7%**	**643**	**33**	**17**	**368**	**6.6**	**255**	**341**	**1,368,601**	**3,388**	**9.7%**	**204**

Commands / Refreshes / Write Operations

Commands and Requests by RequestApp and Status



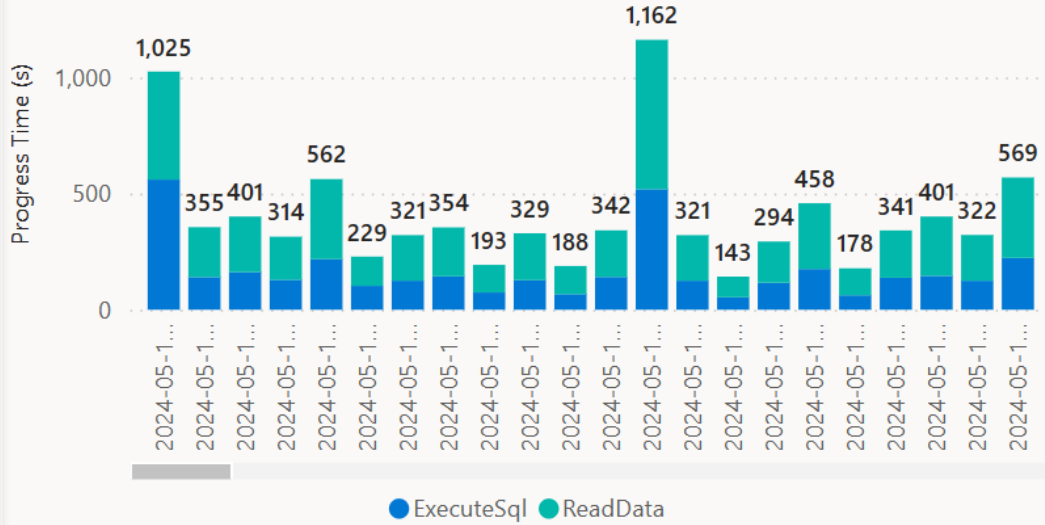
StatusCode	Count
-1056899034	10
-1055784932	8
-1056899032	3
Total	26

RequestID	XmlaRequest Id	intended Usage	Status	Request App	Operation DetailName	timeStart	Duration (s)	Command CPU (s)	Row Processed	timeEnd	Peak Mem(MB)	StatusCode
		Interactive	Succeeded		Batch	2024-05-13 01:38:36	647	466	4,951,657	2024-05-13 01:49:22	6,471	0
		Interactive	Succeeded		Batch	2024-05-13 01:06:53	261	635	5,927,107	2024-05-13 01:11:14	8,042	0
		Interactive	Succeeded		Batch	2024-05-13 00:43:56	283	683	6,253,398	2024-05-13 00:48:40	8,156	0
		Interactive	Succeeded		Batch	2024-05-13 00:19:07	227	574	5,488,798	2024-05-13 00:22:54	7,543	0
		Interactive	Succeeded		Batch	2024-05-12 23:55:49	385	791	7,308,990	2024-05-13 00:02:14	8,878	0
		Interactive	Succeeded		Batch	2024-05-12 23:30:17	180	425	4,680,569	2024-05-12 23:33:17	7,090	0
		Interactive	Succeeded		Batch	2024-05-12 23:07:18	234	551	5,426,211	2024-05-12 23:11:12	7,116	0
		Interactive	Succeeded		Batch	2024-05-12 22:42:03	247	606	5,659,885	2024-05-12 22:46:09	7,104	0
		Interactive	Succeeded		Batch	2024-05-12 22:19:15	151	451	5,270,471	2024-05-12 22:21:46	7,879	0
		Interactive	Succeeded		Batch	2024-05-12 21:54:22	233	545	6,121,918	2024-05-12 21:58:15	7,032	0
		Interactive	Succeeded		Batch	2024-05-12 21:31:35	144	472	4,771,790	2024-05-12 21:33:59	7,968	0
		Interactive	Succeeded		Batch	2024-05-12 21:06:50	240	587	5,648,787	2024-05-12 21:10:51	7,191	0
			Started		ReadData	2024-05-12 20:55:36			5,962,864	2024-05-12 21:08:51		

Semantic Model, Tables, Partitions and Tabular Objects

Semantic Model Id	Row Processed	Max Row Processed	Progress Start	Count	Progress End	Table Count	Partition Count	Column Count
		68,528,232	2024-05-06 07:07:05	445	2024-05-13 02:08:51	13	90	276
		33,926,826	2024-05-06 07:07:05	420	2024-05-13 02:08:51	1	8	30
		11,599,867	2024-05-06 07:31:34	423	2024-05-13 02:01:05	1	8	10
		6,636,325	2024-05-06 07:32:11	418	2024-05-13 02:01:54	1	8	18
		5,678,189	2024-05-06 07:31:36	423	2024-05-13 02:00:04	1	8	7
		4,981,912	2024-05-06 07:31:37	420	2024-05-13 02:01:15	1	8	50
		2,826,654	2024-05-06 07:32:36	415	2024-05-13 02:02:44	1	1	6
		1,275,492	2024-05-06 07:31:33	423	2024-05-13 01:59:30	1	8	13
		869,085	2024-05-06 07:31:51	418	2024-05-13 02:01:50	1	8	62
Total		68,528,232	2024-05-06 07:07:05	445	2024-05-13 02:08:51	13	90	276

Progress Time (s), Progress Start, Row Processed and Progress End by timeStart, XmlaRequestId and OperationDetailName



Questions?