Set and setting

- presentation: 45 min
- Q&A: ~15 min
- Ask your questions on a chat, I'll try to answer ASAP
- Q&A time at the very end
- Have fun :-)

Applied Azure Data Explorer

Marek Gawryszewski

2022.02.15

Roadmap

- Azure Data Explorer - what it is?
- Kusto Query Language - hands-on intro
- Why, when, how?

What is ADX?

> A big data analytics cloud platform optimized for interactive, ad hoc-queries

What is ADX?

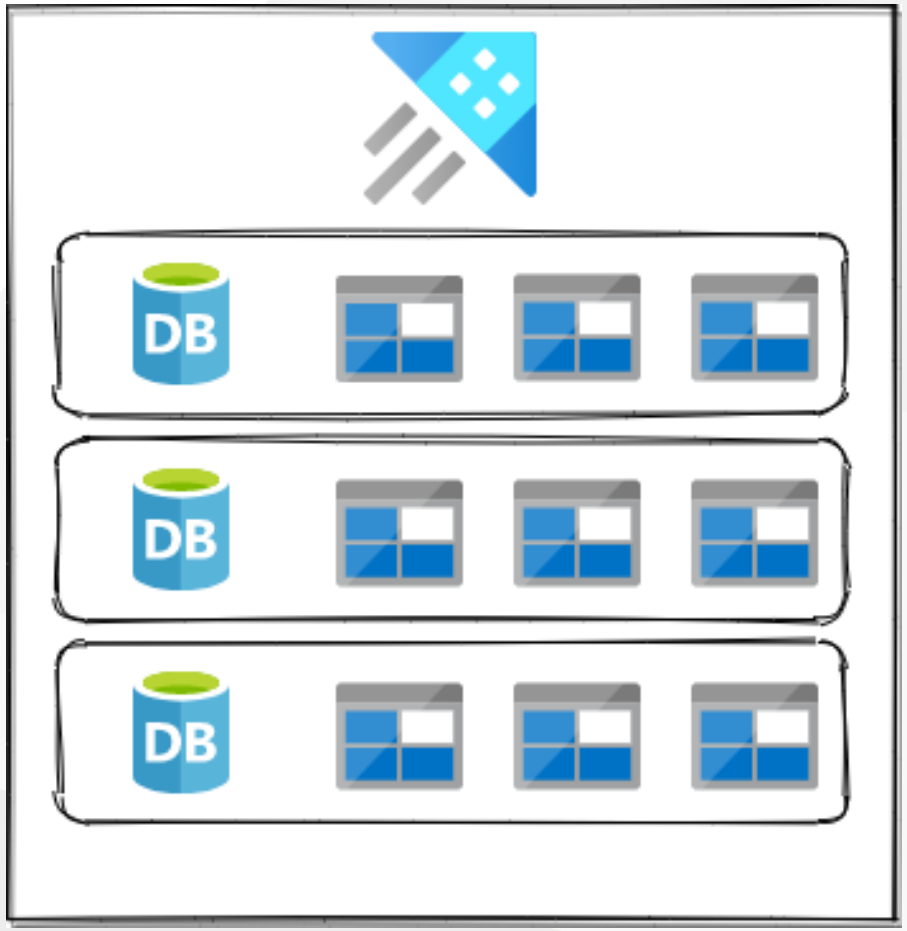
- PaaS
- append only
- 3V: volume, velocity, variance
- data: structured, semi-structured, unstructured
- query with Kusto Query Language (KQL)

ADX Architecture

Logical structure:

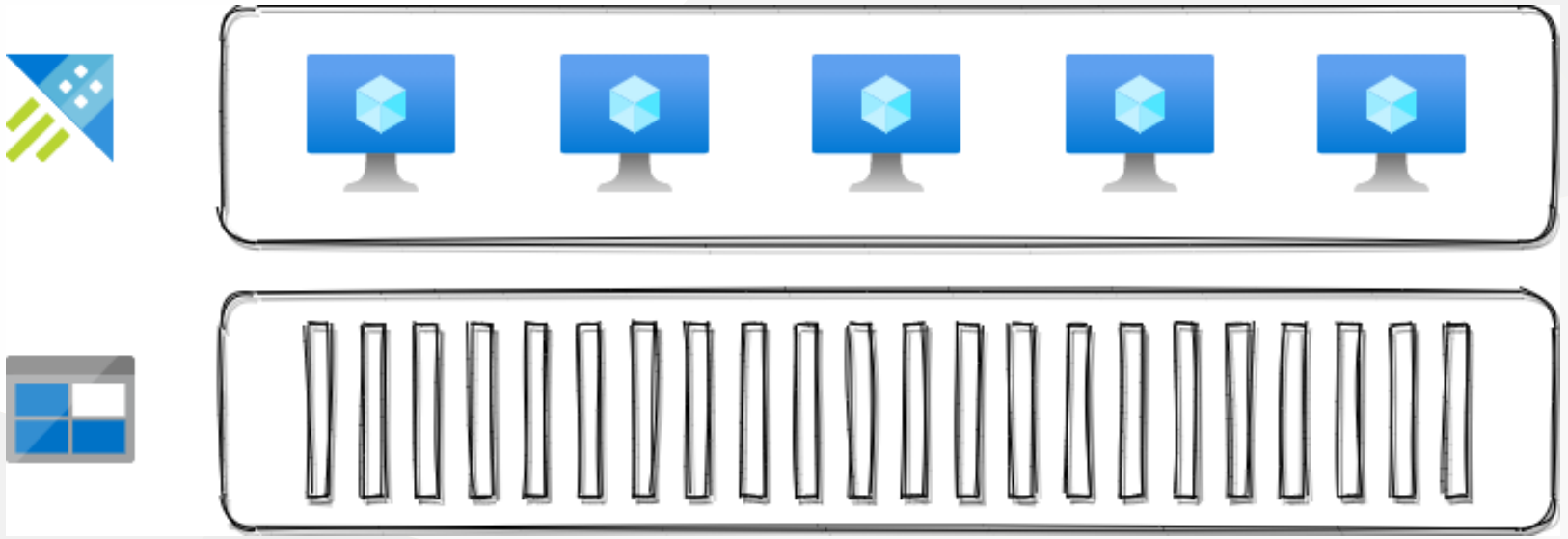
- cluster,
- database,
- table

source



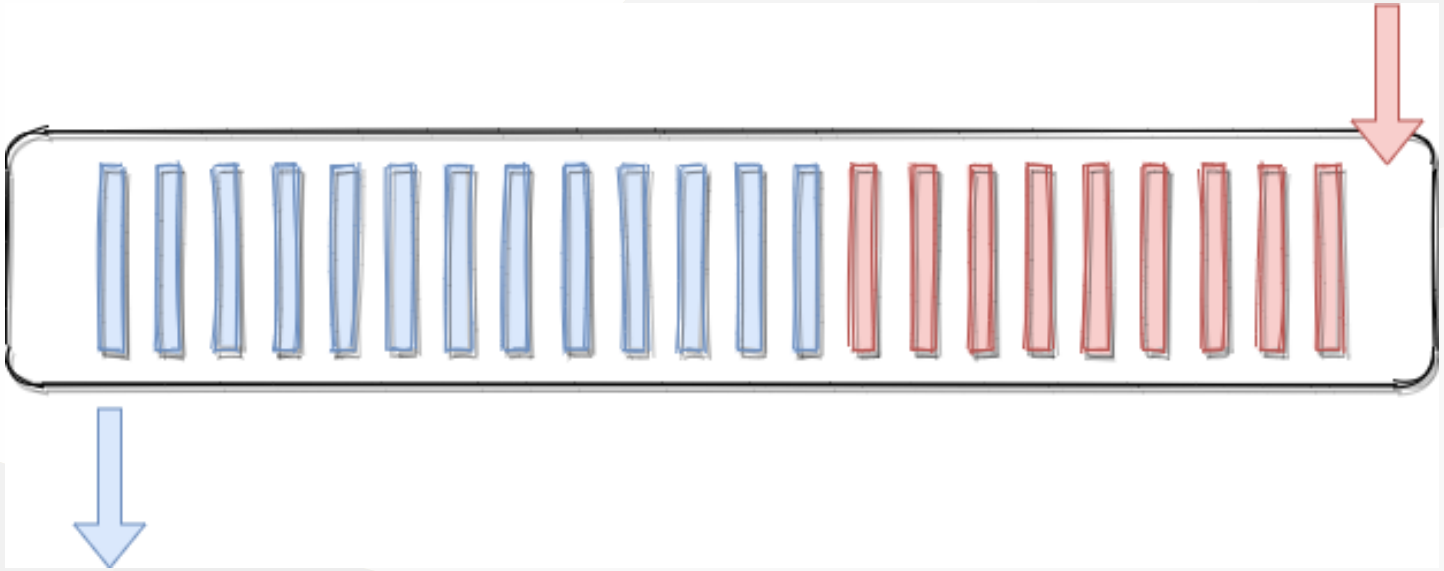
Physical structure

- nodes,
- extents



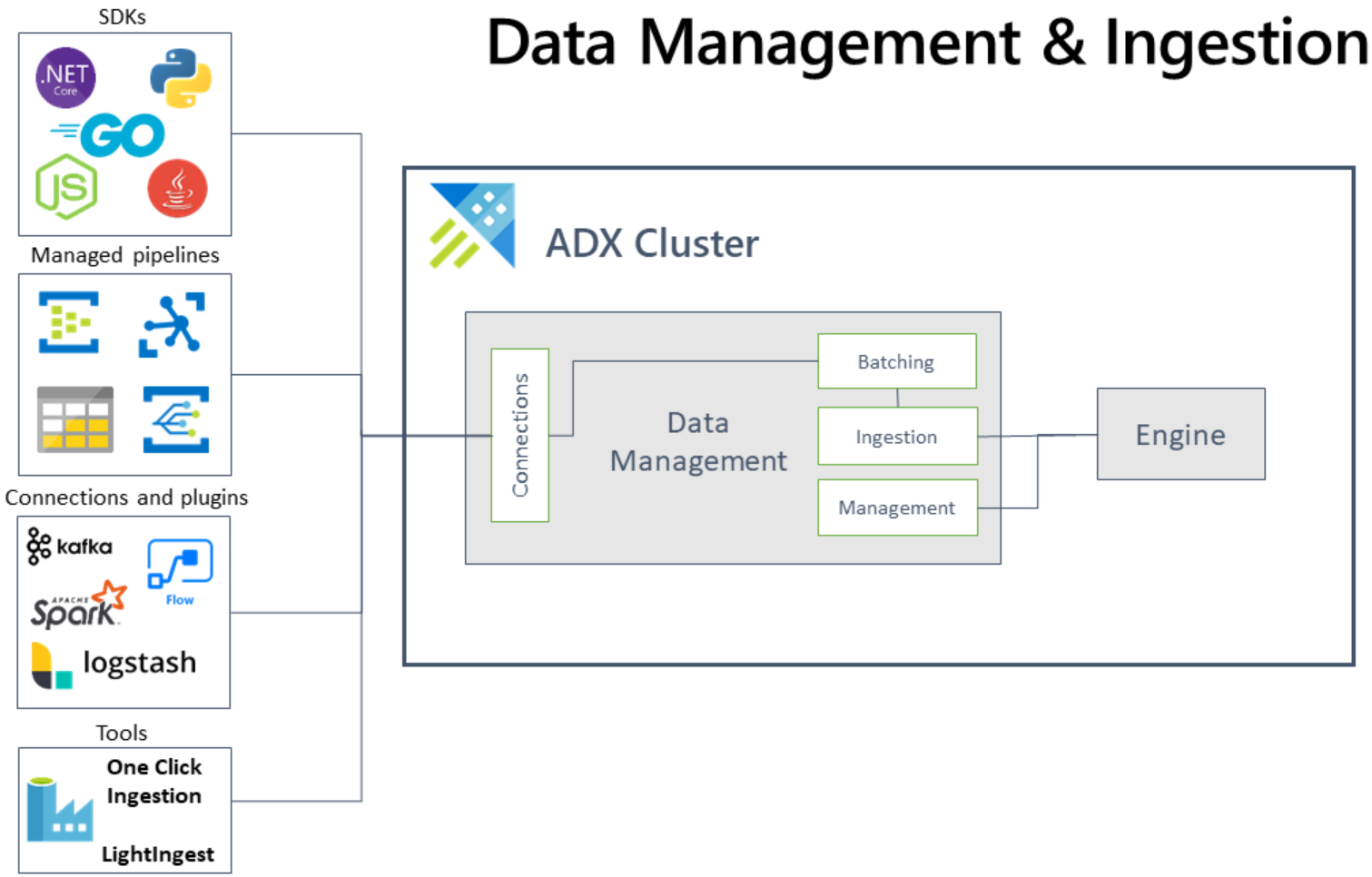
Data lifecycle

- hot cache,
- cold cache

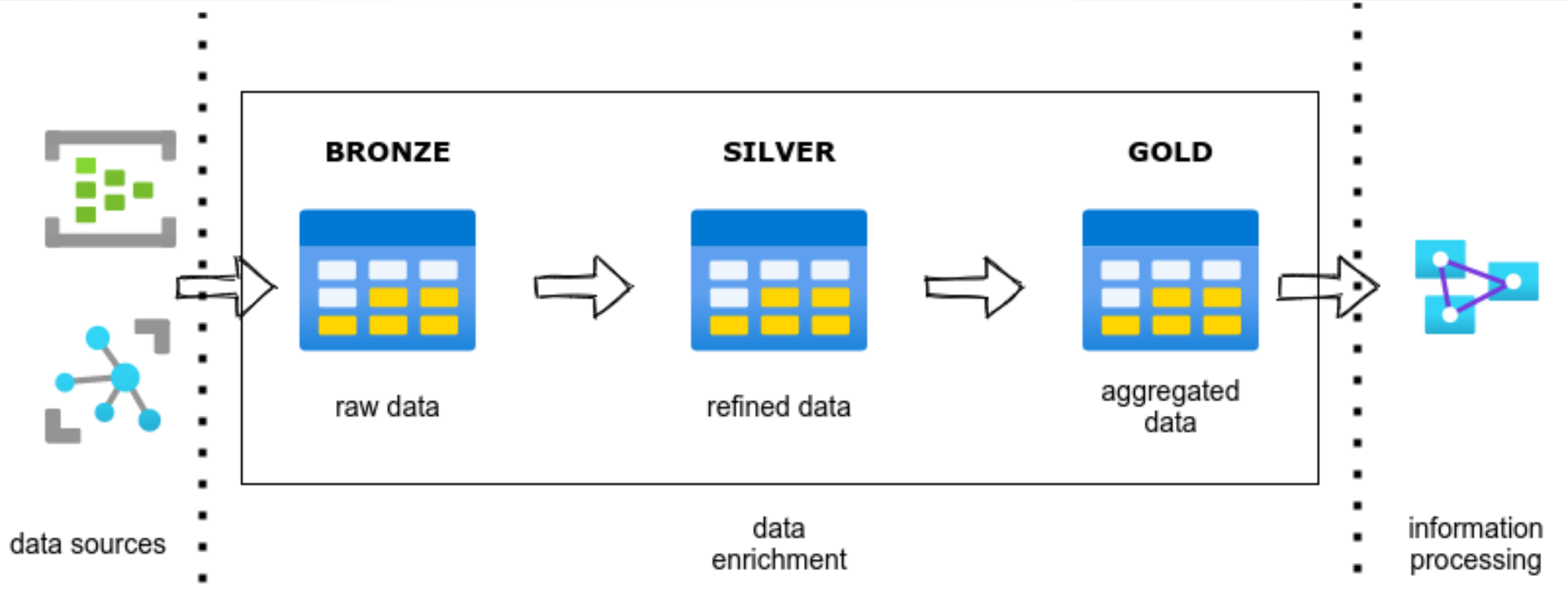


Ingress

[source]



How to organize data?



Too short intro to KQL

[KQL quick reference]

```
Perf
| where TimeGenerated > ago(1h)
| summarize count() by ObjectName
```

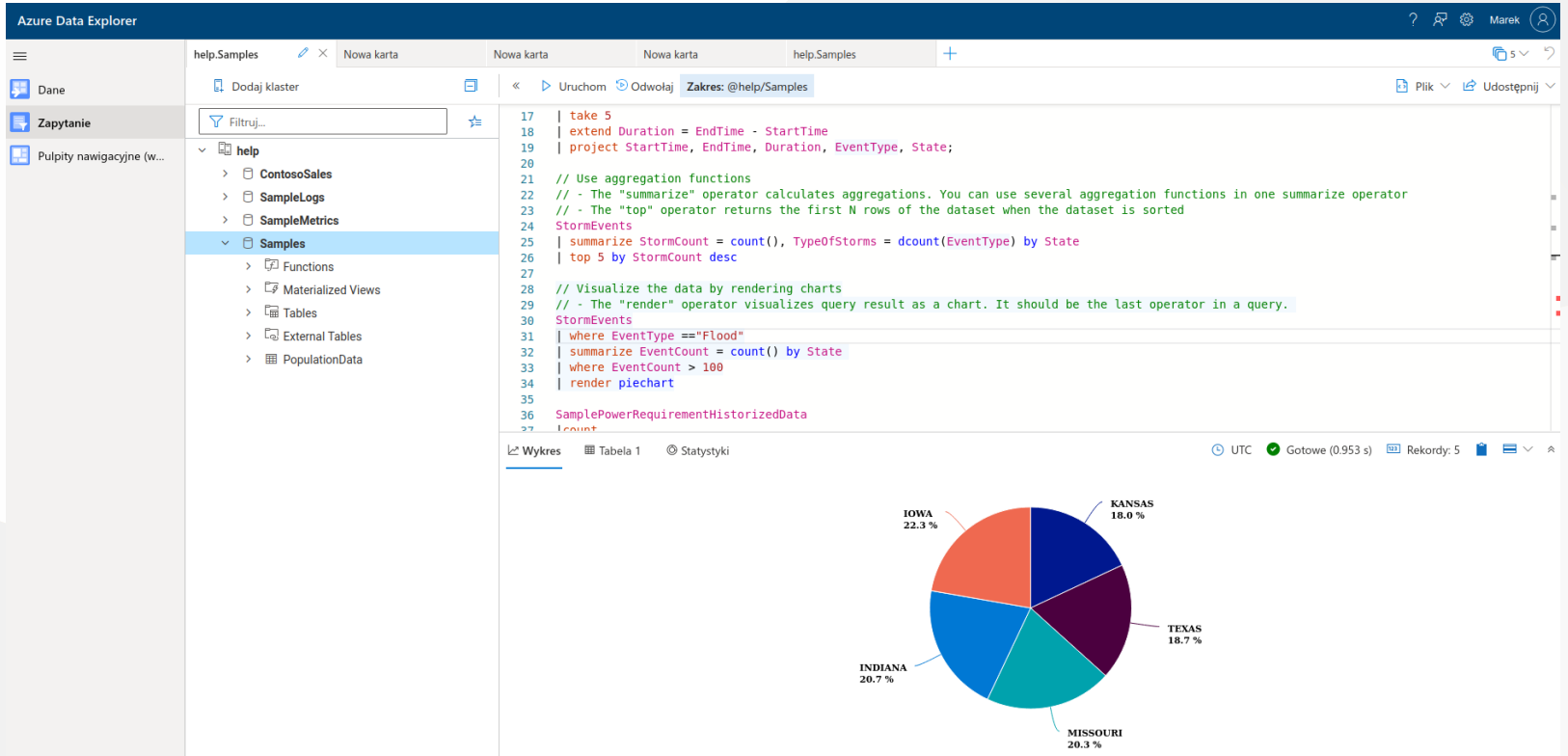
```
Perf
```

```
| where TimeGenerated > ago(1h)
```

```
| summarize count() by ObjectName
```

How to try for *free*?

- Free ADX cluster
- Free cluster for Log Analytics



80/20 rule for KQL

- `count` - return no. of records
- `take` - return no. of first records
- `where` - filter
- `summarize` - aggregates
- `extend` - create new(computed) column in the output
- `let` - define querable object
- `project-away` - delete column from the result
- `project` - include columns from the list

Query with SDK

C# example

```
var client = Kusto.Data.Net.Client.KustoClientFactory
        .CreateCslQueryProvider("https://help.kusto.windows.net/Samples;Fed=true");
var reader = client.ExecuteQuery("StormEvents | count");
```

reference

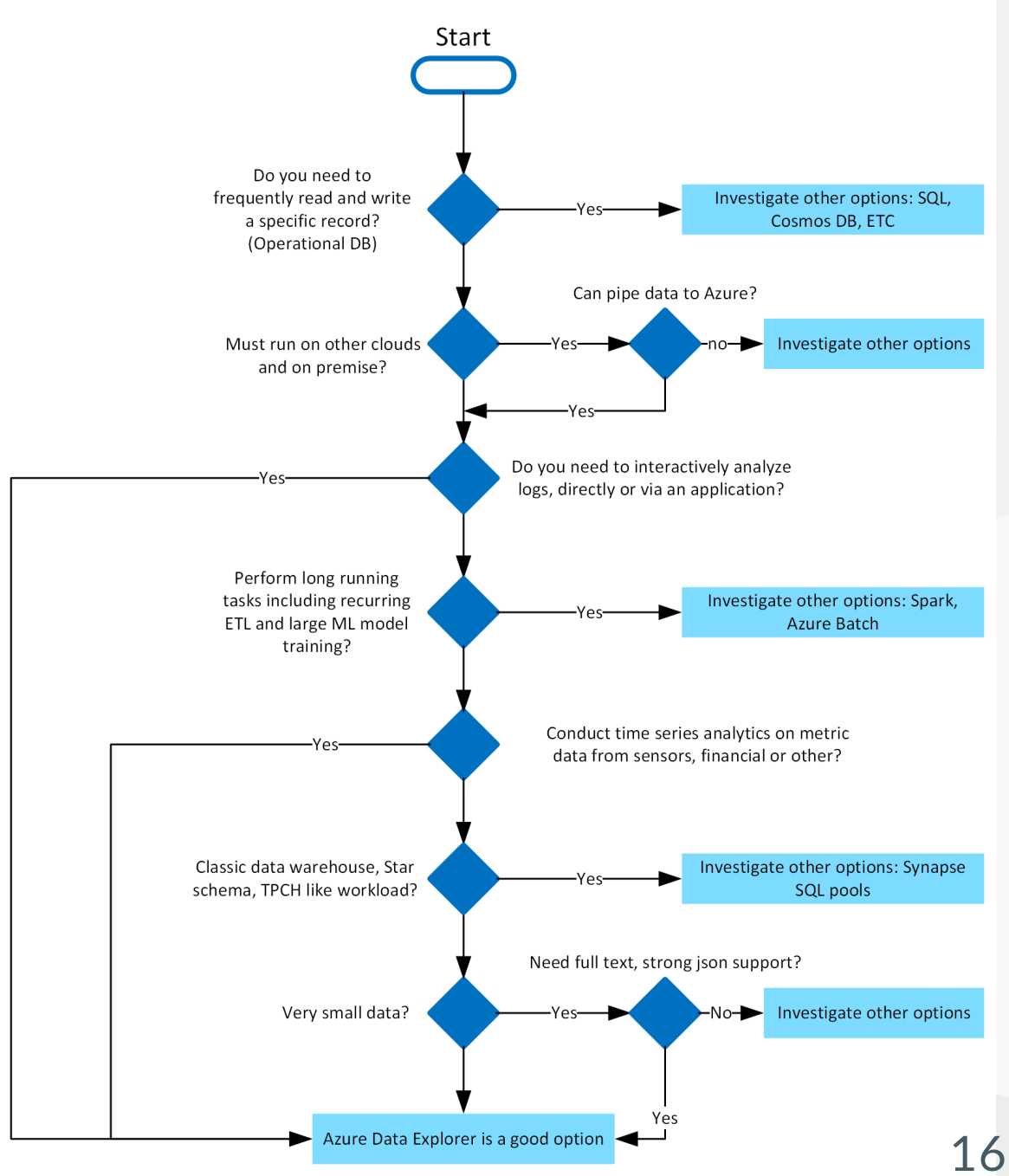
examples

Usage scenarios

1. Analysis of Azure Compute logs
2. Analysis of security threats
3. Data analysis on the spot
4. Data storage engine for IoT solution

When (not) to choose ADX?

[reference]



Azure Monitor

Demo Workspace

- Azure Monitor Logs uses ADX
- extra: Query data in Azure Monitor using Azure Data Explorer

Demo 1

```
SecurityEvent
| where TimeGenerated >= ago(30d)
| where EventID == 4625
| project TimeGenerated, Account, Computer, EventID, Activity, IpAddress
| summarize FailedLogons = count() by Computer
| order by FailedLogons
| render piechart
```

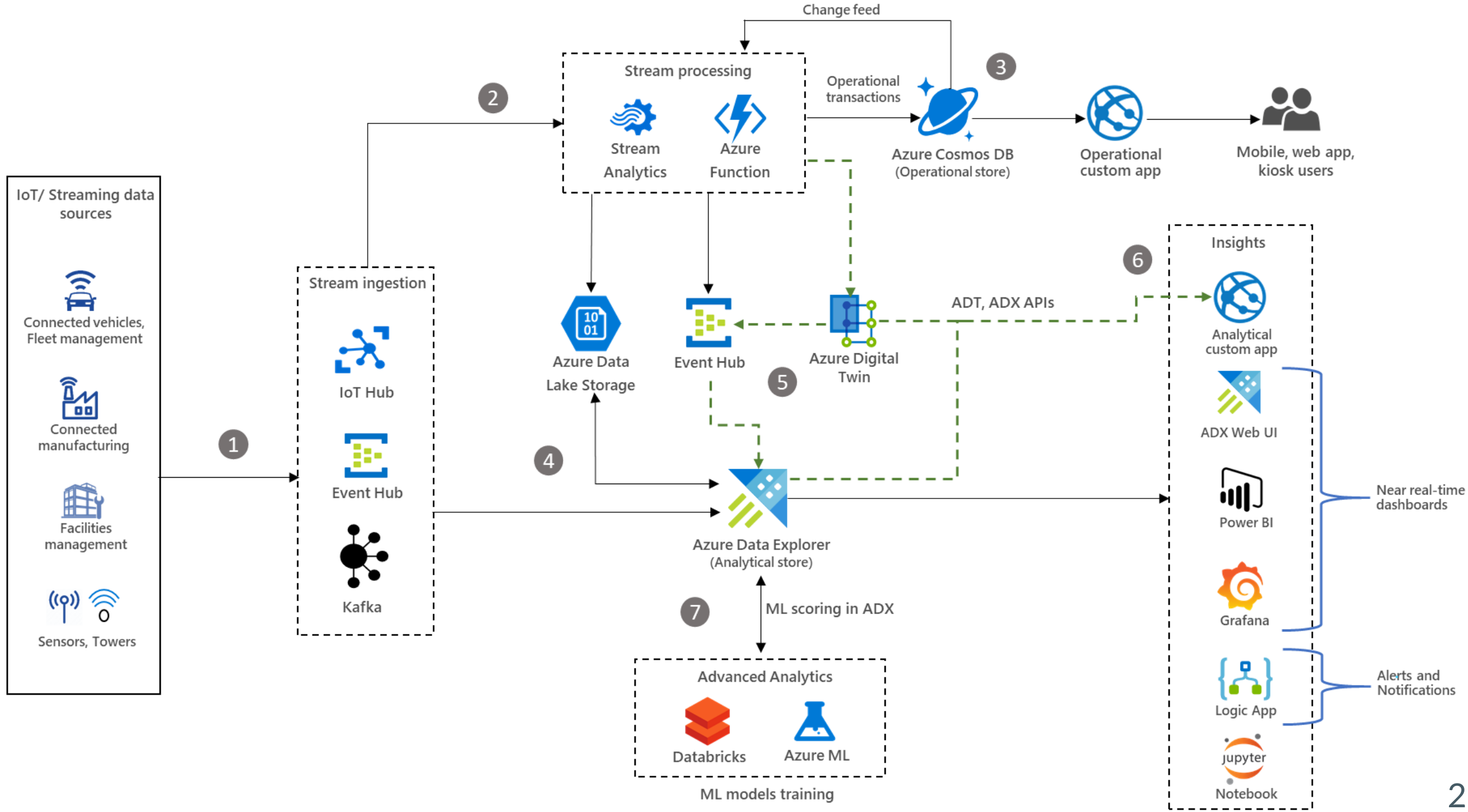
Demo 2

```
Perf
| where ObjectName == "Process"
| where CounterName == "% Processor Time"
| where CounterValue > 0
| extend CPUTime = strcat(tostring(round(CounterValue, 1)), "%")
| project TimeGenerated, Computer, InstanceName, CounterValue, CPUTime
| summarize arg_max(TimeGenerated, *) by Computer
| order by CounterValue desc
```

ADX for IoT

Reference architectures and solutions:

- Big data analytics with Azure Data Explorer
- Azure IoT reference architecture
- IoT analytics with Azure Data Explorer


Change feed
Stream processing
Stream Analytics
Azure Function
Operational transactions
Azure Cosmos DB
(Operational store)
Operational custom app
Mobile, web app, kiosk users
IoT/ Streaming data sources
Connected vehicles, Fleet management
Connected manufacturing
Facilities management
Sensors, Towers
Stream ingestion
IoT Hub
Event Hub
Kafka
Azure Data Lake Storage
Event Hub
Azure Digital Twin
ADT, ADX APIs
Insights
Analytical custom app
ADX Web UI
Power BI
Grafana
Near real-time dashboards
Logic App
Alerts and Notifications
jupyter
Notebook
Azure Data Explorer
(Analytical store)
ML scoring in ADX
Advanced Analytics
Databricks
Azure ML
ML models training
1
2
3
4
5
6
7

Key Takeaways

- ADX is used by many services for telemetry storage
- KQL is helpful for any DevOps working with Azure
- ADX is not a replacement for MSSQL or CosmosDB
- ADX requires crafted solution architecture

Q&A

Links

Documentation

- Azure Data Explorer
- Azure Data Explorer documentation
- IoT analytics with Azure Data Explorer

Links

Github

- rod-trent
- MustLearnKQL
- SentinelKQL
- AddictedtoKQL

Links

YouTube

- KQL Cafe | Session 1
- Azure Data Explorer channel

Links

- Azure Cloud & AI Domain Blog
- Stack Overflow tag
- Pluralsight: How to Start with Microsoft Azure Data Explorer