**Cyber Security data & Analytics**

**Azure Data Explorer**

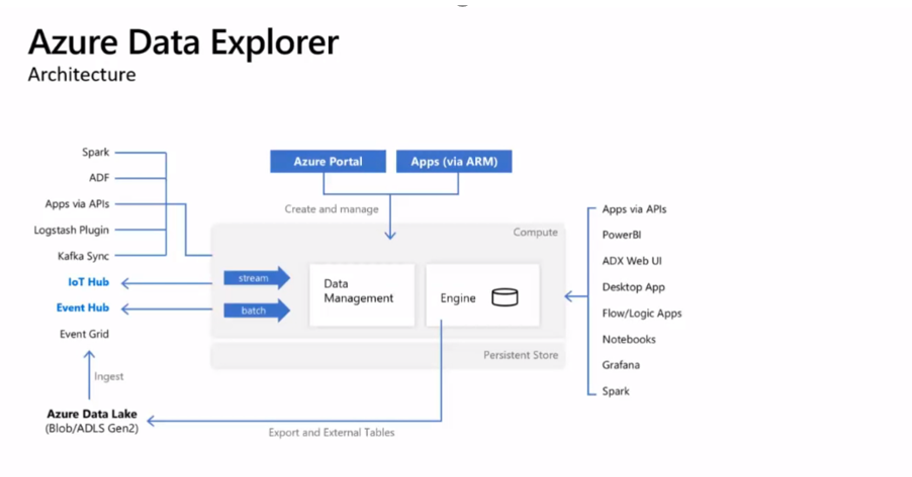
|  |  |
| --- | --- |
| Revision | 01 |
| Issued | April-14-2020 |
| Functional team | Cyber Security Data & Analytics |
| Document classification | GE Internal |

### Contents

1. What is Azure Data Explore 2
2. Why Azure Data Explorer 2
3. Features 3
4. Kusto Query Language 3
5. Integration 4
6. What is Event Grid 5
7. Uses Cases 6
8. SaaS solutions 7
9. Pricing 7
10. Document History 7
11. Location 7

# **What is Azure Data Explorer?**

* Azure data Explorer is a fully managed, fast flowing interactive data analytics service for real-time analysis on large volume of data coming from IoT Hub, EventHub and more.



**Figure 1**

1. **Why Azure Data Explorer?**

* Azure data explorer not only have the capability of the analytics but can also provide search engine capabilities.
* Azure data explorer is optimized for providing low latency ingestion.
* It also provides the ability to build and deploy other services of your need.
* Azure data explorer also supports the analysis of high volume of structured (code format), semi structured data (JSON, XML) and unstructured data (free text).

1. **Features:**

* It is PaaS (Platform as a service) so, no need to managed indexes. Microsoft Azure fully managed and provisioned Azure data Explorer but, we do have to create schema for our data.
* Main advantage of indexing is every column is indexed by default and compressed by default.
* It is designed for data exploration from streaming data.

1. **Kusto Query Language:**

* Azure data explorer is based on Kusto Query Language. It is used to query azure databases, i.e. log databases, monitor logs, insights and others.
* It is a very easy languages to pick especially if your familiar with SQL.

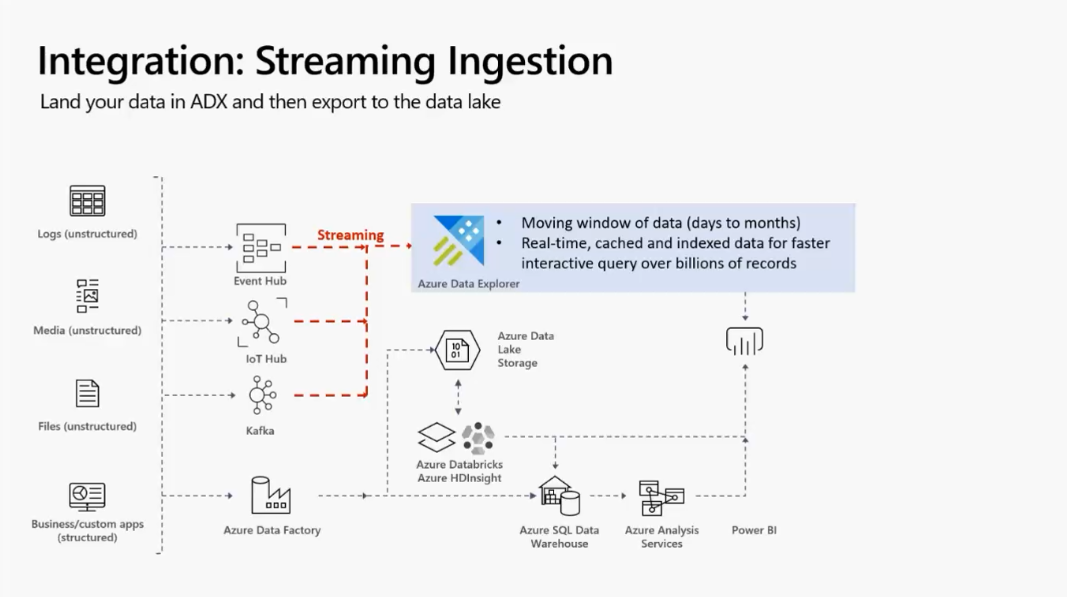


1. **Integration:**

* Azure provide two types of integration with data ingestion.

1. **Streaming Ingestion:**

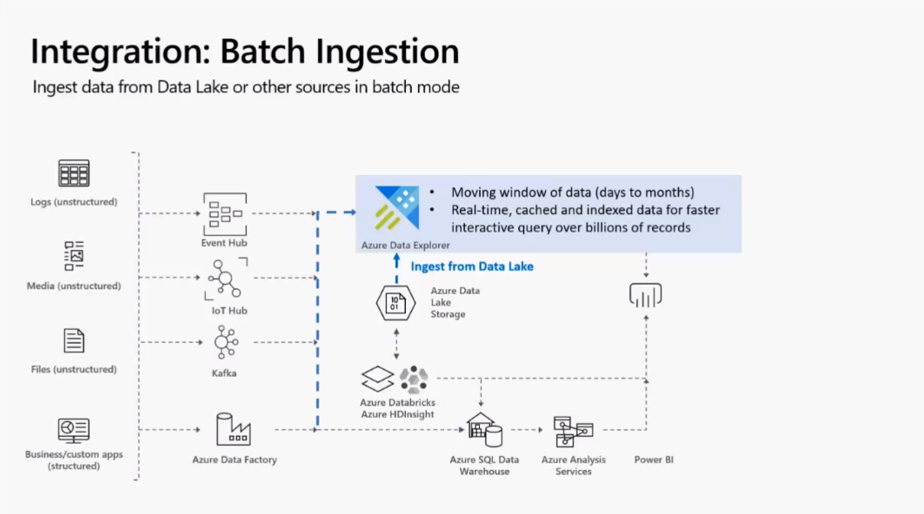
For EventHub, IoT Hub, and Kafka we use streaming mode and the latency is just 10 sec. we use this when we require low latency.



**Figure 2**

1. **Batching Ingestion:**

For high volume data we use batching ingestion mode and the latency is 10 sec to up-to 5 min however, it is configurable.



**Figure 3**

**In Azure data factory we have:**

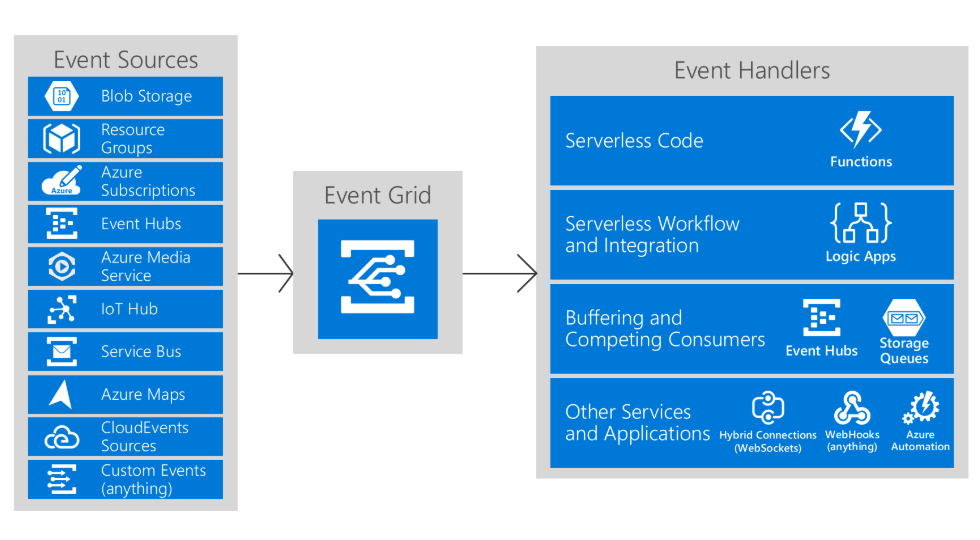
* \*Read data from azure data explorer.
* \*Send data from azure data explorer.
* \*Runs Job on azure data explorer.

***NOTE:***

Azure data explorer can also ingest data from data lake and blob storage through either code or Event grid.

1. **What is Event grid?**

Event grid is based on event as soon as the data arrives, Azure data explorer cache it in and the process is called event grid integration.



**Figure 4**

1. **Uses Cases:**

* IoT devices
* Time Series analysis
* Events analysis
* Log analysis
* Transaction data analysis
* It consolidates and corelate logs and events data
* Replace legacy logs search solutions which save costs, infrastructure and index management overhead.
* Azure data explorer can accelerate AI ops (pattern recognition, anomaly detection, forecasting etc.)
* IoT analysis on time series and Telemetry data.

1. **SaaS Solutions**

* Azure data explorer can build multi-tenants or single tenant SaaS analytics solutions for time series, logs, events, transaction and security data.

1. **Azure Data Explorer Pricing**

* You pay for what you use
* Per-hour billing

**2. Document History**

* 1. Review history table

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Reviewer** | **Review Date** | **Comments** |
| 01 | Hekmatullah  Attayee | 4/14/2020 |  |
|  |  |  |  |

1. **Location**

The current version of this document is stored at: