Searching Data

Types of Data Tiers

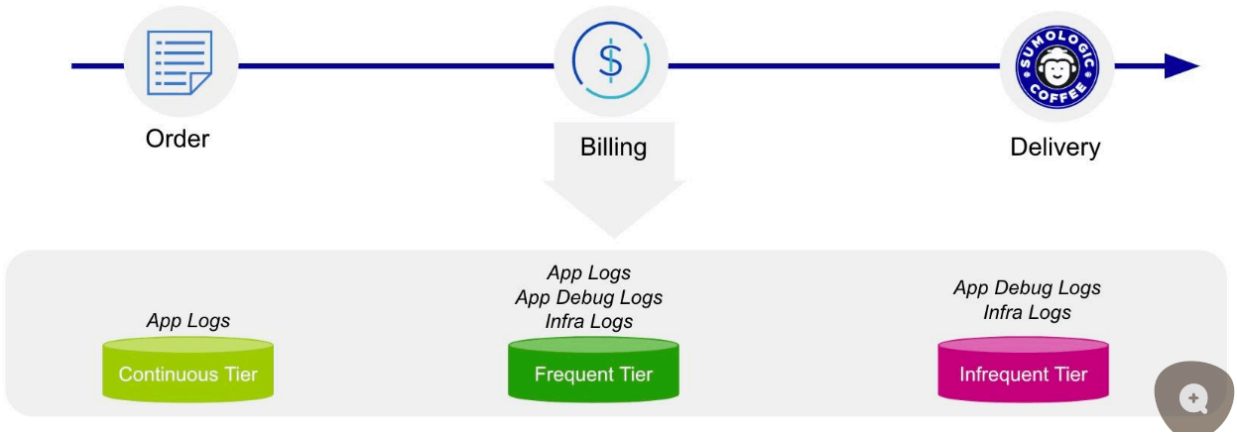
Continuous Tier

- Data you use to **monitor** and **troubleshoot** production applications and to **ensure the security** of your applications

Frequent Tier

- Data you need to **frequently access** to troubleshoot and investigate issues
  - ex) development and test data
- Searching the Frequent tier is **free**

Infrequent Tier



- Data that is used to troubleshoot **intermittent** or **hard-to-reproduce** issues
  - ex) debug logs, OS logs, thread dumps
- **Pay-per-search** pricing model, and **very low ingestion** cost

How the logs are stored?

- `Billing/infra` goes to the **Infrequent**
- `Billing/applog` is going to the **Continuous**
- Anything tagged with **Frequent**, would go to the **Frequent** Tier for our **Billing**

How to search logs data

Basic mode

- The Basic Mode provides a simple and intuitive workflow to select the data tier, indexes of interest, filter based on metadata and eventually zero in on the logs of interest through the specific keywords.
- Offers an easy-to-use, structured query builder
- **Recent Search** runs previously ran queries. (Auto saved)
- Can pick **Data Tier** to run the query against.
- Type in any **partitions** or **Views** that you want to run the query against
  - **Partition**: Shows up as **<Tier> Index**

- **Scheduled View:** Shows up as a **<Tier> View**.

Metadata

Tag	Description
`_collector`	Name of the collector (set when the Collector was installed) that received the log message.
`_sourceHost`	Hostname of the Source
`_sourceName`	The name of the log file, determined by the path you entered when you configured the Source
`_source`	Name of the source this data came through
`_sourceCategory`	**The category of the Source that collected the log message. Can be freely configured. Main metadata tag**

Tag	Description
`_messageCount`	A sequence number (per Source) added by the Collector when the message was received.
`_messageTime`	The timestamp of the message (in milliseconds)
`_receiptTime`	The time the Collector received the message (in milliseconds)
`_size`	The size of the log message in bytes
`_raw`	The raw log message
`_format`	The pattern used for parsing the timestamp