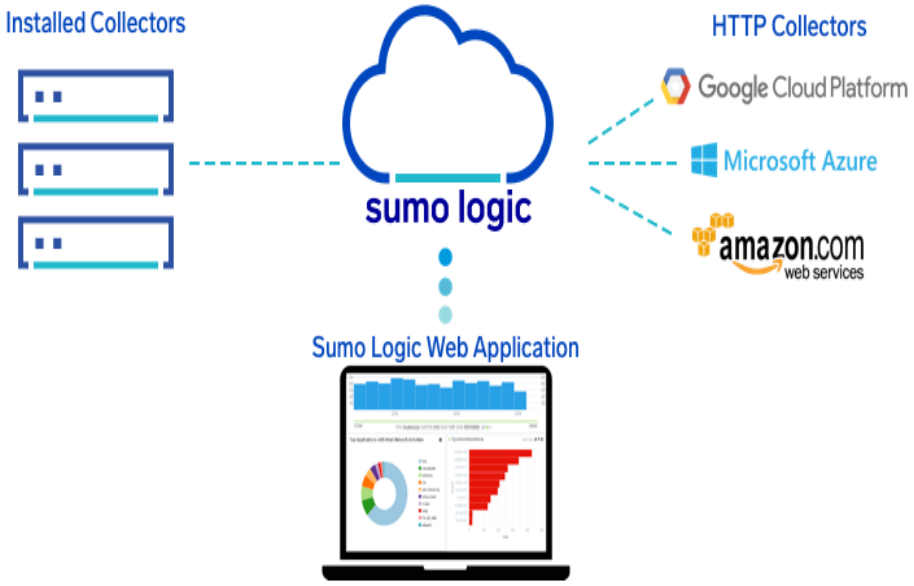
SUMO Logic is cloud-native, Multi-tenant platform helps in making data-driven decisions and reduces the to investigate security and operational issues

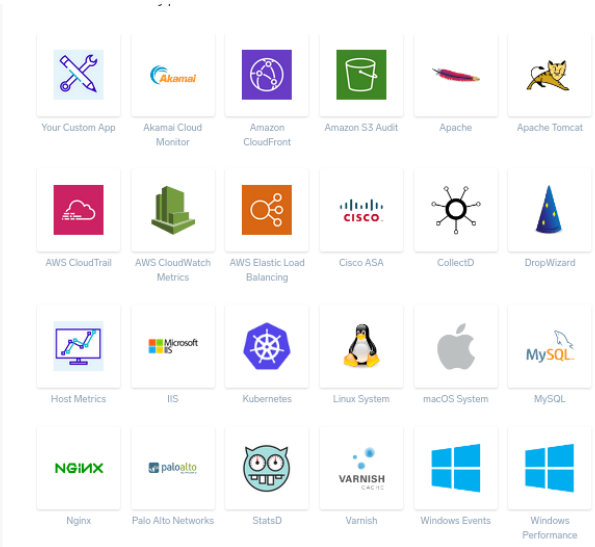
Sumo logic can collect logs from almost any system in nearly any format

Sumo logic Provides real time altering and notifications

Sumo logic can collect terabytes of logs Data and can perform analytics on that

Sumo Logic Installed Collectors receive data from one or more Sources.Collectors collect raw log data, compress it, encrypt it, and send it to the Sumo Cloud, in real time. A single Sumo Logic Collector can collect up to 15,000 events per second or more and has fault tolerance during network or service outages. If you'd like to collect non-traditional machine data, a Script Source or Script Action provide a great deal of flexibility to collect files.



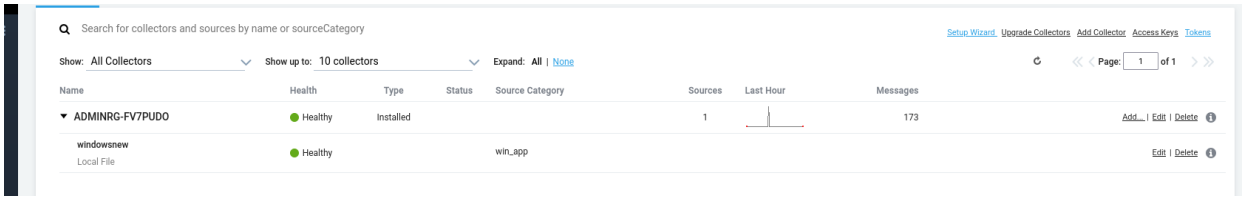


Collectors is a Java agent that receives logs and metrics from its Sources and then encrypts, compresses, and sends the data to the Sumo service. Apps help you get started gaining insights from your data source by providing example searches and dashboards for common use cases. They are customized with your source configurations and populated in a folder

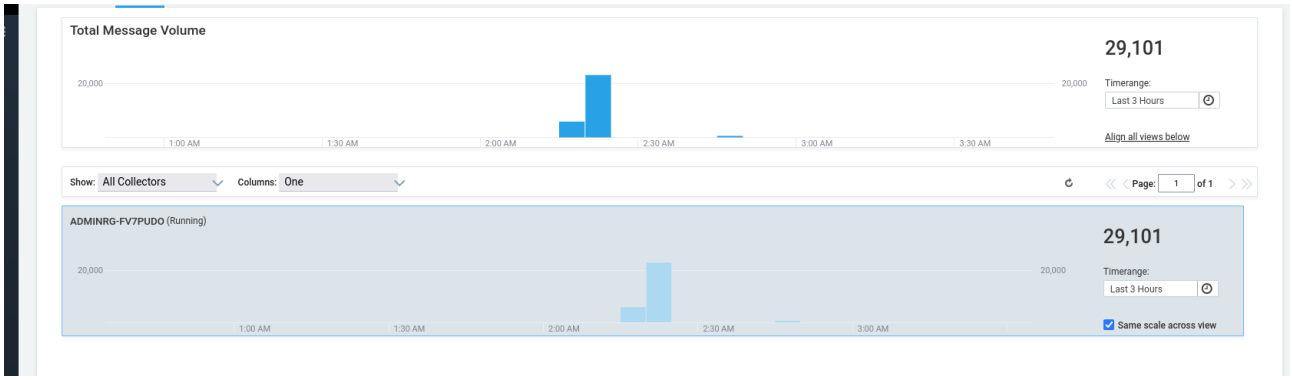
Installing collectors onWindows

- Locate and install the app you need from the **App Catalog**.

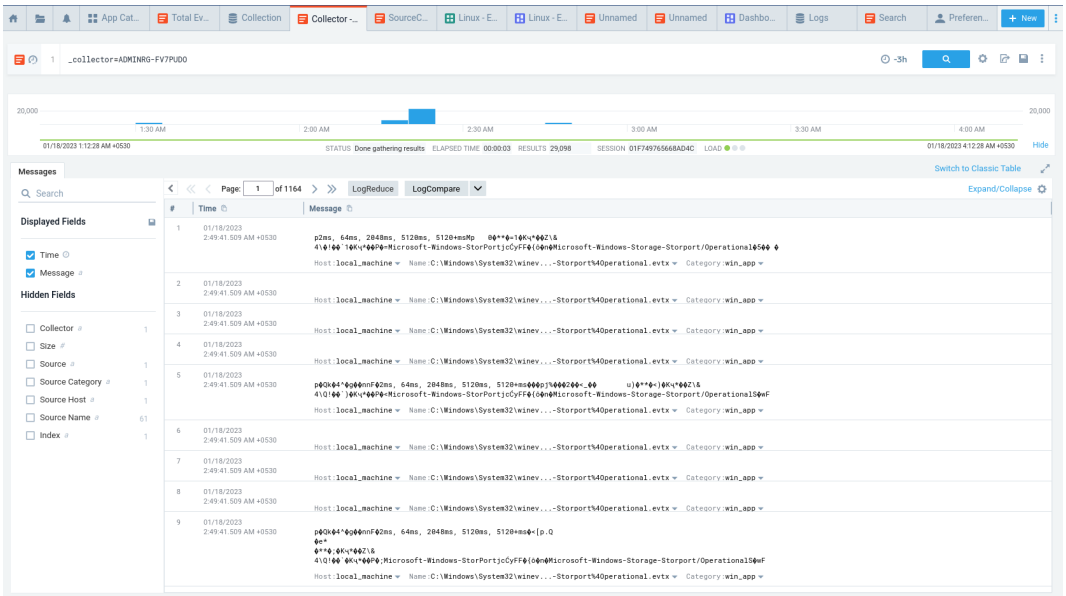
- From the **App Catalog**, search for and select the app**.**
- Select application of Windows .exe and install in windows system
- In Sumo Logic select **Manage Data > Collection > Collection**.
- Find the name of the installed collector to which you'd like to add a Source. Click **Add** and then choose **Add Source** from the pop-up menu.



- Click **Windows Event Log**.
- Choose **Local** for **Type of Windows Source**.
- Path of the log files to fetch (ex : C:windows\system32\winevt\Logs*.evtx(* represents select all))



- check status of fetching Logs



Log Search

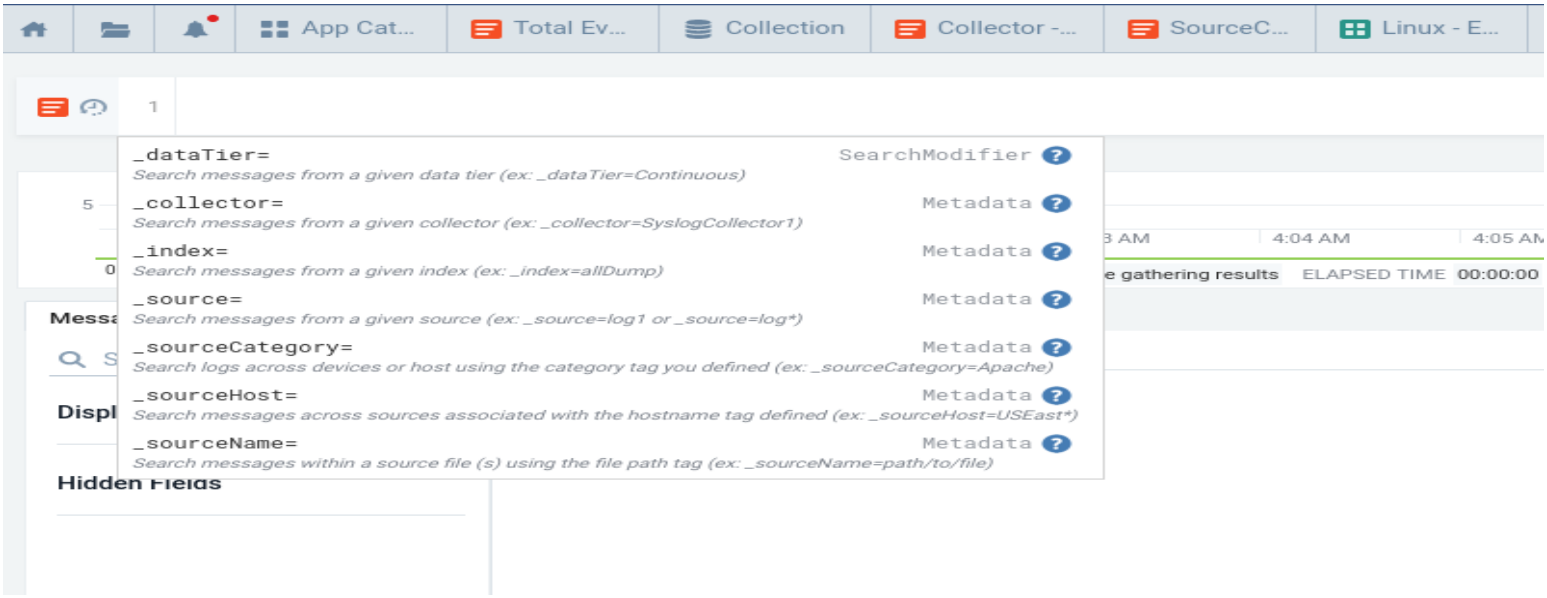
Search Syntax is based on a funnel or "pipeline" concept. The wide mouth of the funnel begins with all your current Sumo Logic data, and you narrow the funnel by entering keywords and operators separated by pipes

a search query is typically formatted something like this:

```
keyword search | parse | where | group-by | sort | limit
```

At a minimum, all searches should use one or more metadata tags in the scope, for example: _sourceCategory, _source, _sourceName, _sourceHost, or _collector.

Search allows to query and analyze log data sent to Sumo Logic. There are many features to help you use our robust Search Query Language, such as LogCompare, LogReduce, LogExplain, Lookup Tables, Subqueries, and Time Compare.



`_collector` = The name of the Collector (set when the Collector was installed) that received the log Message
`_messageCount` = sequence number (per Source) added by the Collector when the message was received

`_messageTime` = The parsed timestamp by the Collector from the log message in milliseconds. If the message does not have a timestamp, messageTime uses the receiptTime.

`_raw` = The raw log message.

`_receiptTime` = The time the Collector received the message in milliseconds

`_size` = The size of the log message in bytes.

`_source` = The name of the Source, determined by the name you entered when you configured the Source.

`_sourceCategory` = The category of the Source that collected the log message. This can be a maximum of 1,024 characters.

`_sourceHost` = The host name of the Source. For local Sources the name of the Source is set when you configure the Source. For remote Collectors, this field uses the remote host's name. The `_sourceHost` = metadata field is populated using a reverse DNS lookup. If the name can't be resolved, `_sourceHost` is displayed as `localhost`. This can be a maximum of 128 characters.

`_sourceName` = The name of the log file, determined by the path you entered when you configured the Source.

`_format` = The pattern used for parsing the timestamp.

`_view =` The name of the index, view, or partition.