Dashboards and Apps in Sumo Logic

What are Apps in Sumo Logic?

In Sumo Logic, **Apps** are **pre-built collections of searches, dashboards, and visualizations** designed to help you **monitor, analyze, and secure** your environment.
Each app focuses on a specific **data source or technology**, such as AWS CloudTrail, Microsoft 365, Windows Firewall, or Palo Alto Networks.

Apps help users **quickly gain insights** without having to manually build complex queries or dashboards from scratch.
They are like **plug-and-play analytics packages** that automatically interpret and visualize incoming log data.

Why are Apps Used

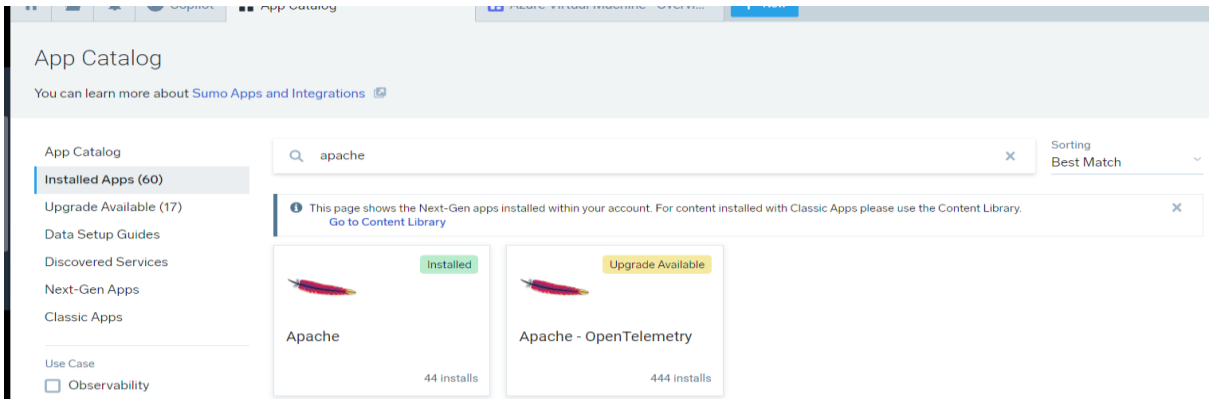
Apps are used to:

- **Simplify log analysis** – Instead of writing queries, you can use ready-made dashboards and visualizations.
- **Save time** – Pre-configured searches help identify key metrics and alerts instantly.
- **Provide visibility** – Apps organize data into meaningful charts and tables for security, performance, and operations teams.
- **Standardize monitoring** – Multiple teams can view the same dashboards for consistency and collaboration.
- **Speed up incident response** – Security apps (e.g., for firewalls or endpoint protection) highlight threats and anomalies in real time.

I navigated to the **App Catalog**, located on the left-hand panel of the Sumo Logic interface. From there, I could view a list of available applications, including several that were already pre-installed in the environment.

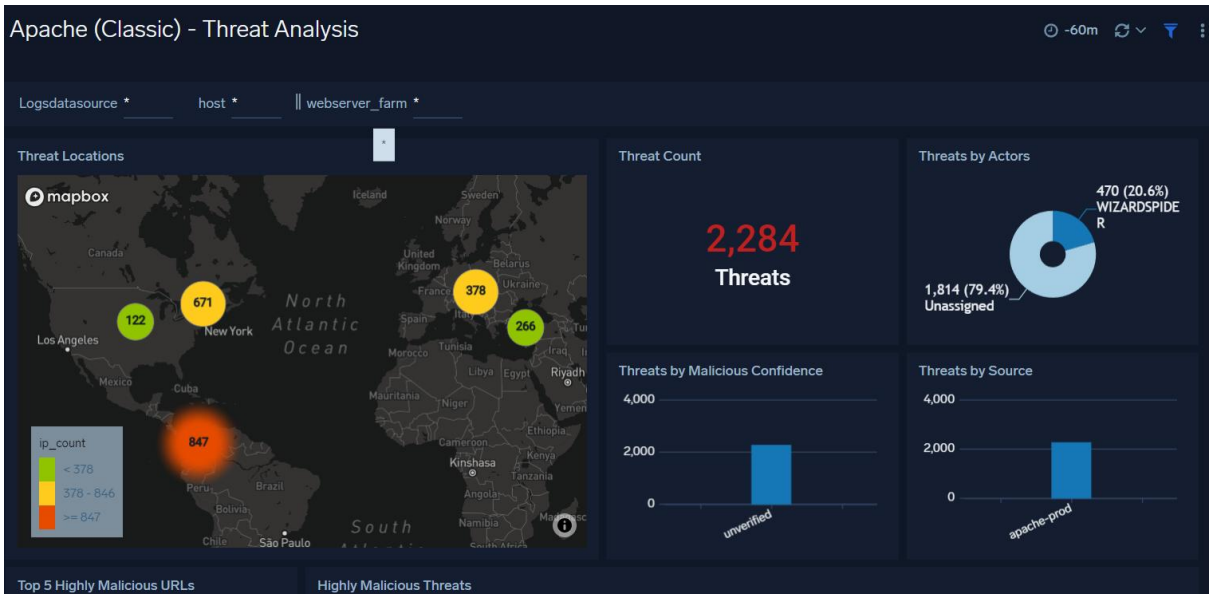
For practice, I searched for the **Apache App** and installed it.

Once I installed the **Apache App**, it appeared under the **App Catalog** section as *Installed* and was also added to the **Shared Library**, making it accessible to other users as well.

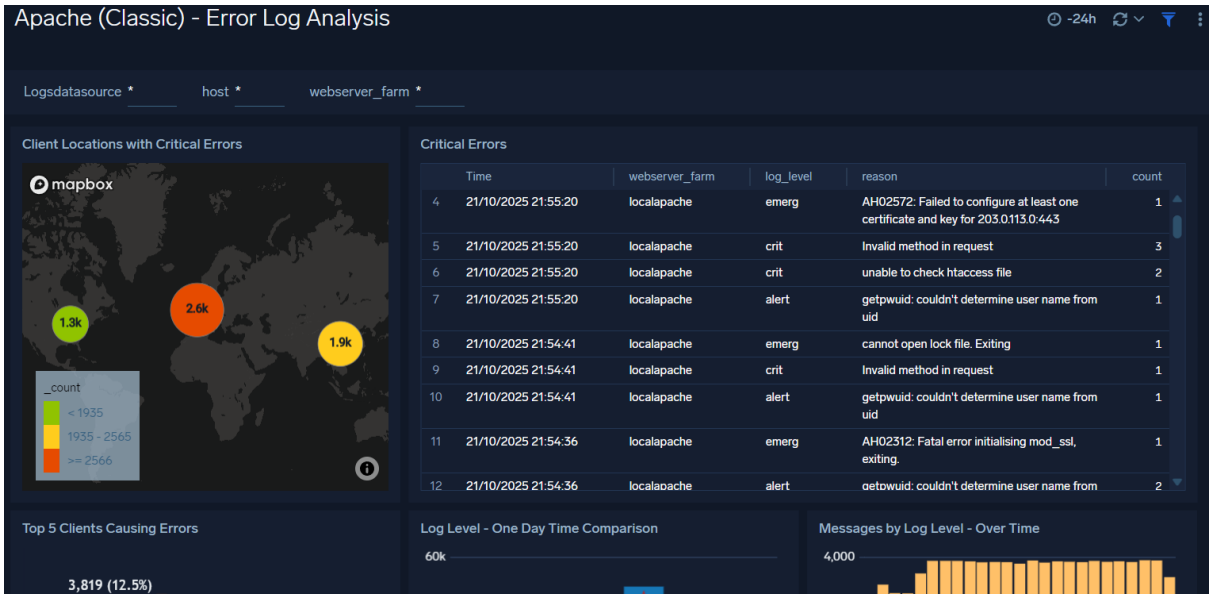


I then opened the App directly from the **App Catalog**, where a list of predefined dashboards was displayed.

First, I selected the **Thread Analysis Dashboard**. Within this dashboard, I had the option to choose **all log data sources** or select **specific ones** to focus the analysis. This feature allows analysts to narrow down the data view for more targeted investigation, such as isolating logs from particular servers or environments.



After reviewing the Thread Analysis Dashboard, I opened the **Error Dashboard**, which showed where and when errors occurred in the Apache logs, helping to quickly identify issues and patterns.



Next, I opened the **Trend Dashboard**, which displayed detailed insights such as **traffic distribution by server**, **traffic volume**, **bytes served**, and **response trends over time**, along with several other metrics that help analyze overall server performance and activity patterns.

Conclusion

In this lab, I learned how to explore and analyze data through **Sumo Logic Apps and Dashboards**. By installing and accessing the **Apache App**, I was able to view multiple dashboards that visualize key metrics such as thread activity, errors, and traffic trends. These dashboards demonstrated how raw log data is transformed into meaningful visual insights, making it easier to monitor system health, detect issues, and understand overall server performance. This exercise provided a clear understanding of how dashboards in a SIEM environment like Sumo Logic support both **security monitoring** and **operational analytics**.