servicenow

Internship Project

HLA (Health Log Analytics)

servicenow

1. Purpose, Background and Scope

1.1 Purpose

The purpose of this document is to provide the procedure of implementation of use-case of ingesting Splunk logs into NOW Platform's Health Log Analytics (HLA) which is used for AI needs.

1.2 Background

Health Log Analytics: HLA helps prevent issues before the users are affected. It helps to identify the root cause of an issue by detecting anomalies, organizing meaningful log properties and providing searchable surrounding logs. It continuously gathers, comprehends, and correlates log data generated by machines in real-time. The application promptly identifies any deviations from normal behavior and notifies of potential problems.

Splunk environments:
Cloud - https://splunk.servicenow.net
Corp - https://splunk.corp.service-now.com
Fed - https://splunk.fed.servicenow.net
IFSDev - https://azlabsplunk.ifsdev.servicenowlab.com/
IL5 - https://il5splunk.servicenowcloud.com/

Alert Correlation: Grouping alerts together and remediating them as a group instead of individually to save time and reduce the noise.

Types of Correlation:

- Rule-Based/ Human-Defined
- Automated – Specific CI, General CI Class
- Manual/ Semi-Supervised
- CMDB/ Topological
- NLP/ Text-based
- Tag-based Correlation

Event Management: Alert management rules from OOB are used to create an incident to launch a sub-flow from flow designer where if the alert filter criteria are met, the sub-flow is triggered.

1.3 Scope

Use-case of ingesting Splunk logs will be evaluated to know the performance impact.

2. Architecture and Design

2.1 HLA Architecture

Health Log Analytics receives, analyzes and transmits logs to Event Management application through the MID Server. After the instance receives logs from MID Server connection instance

and HLA collects Splunk logs to find anomalies using unsupervised machine learning (ML) models. To identify the root source of the problem using additional algorithms, it combines these anomalies together.

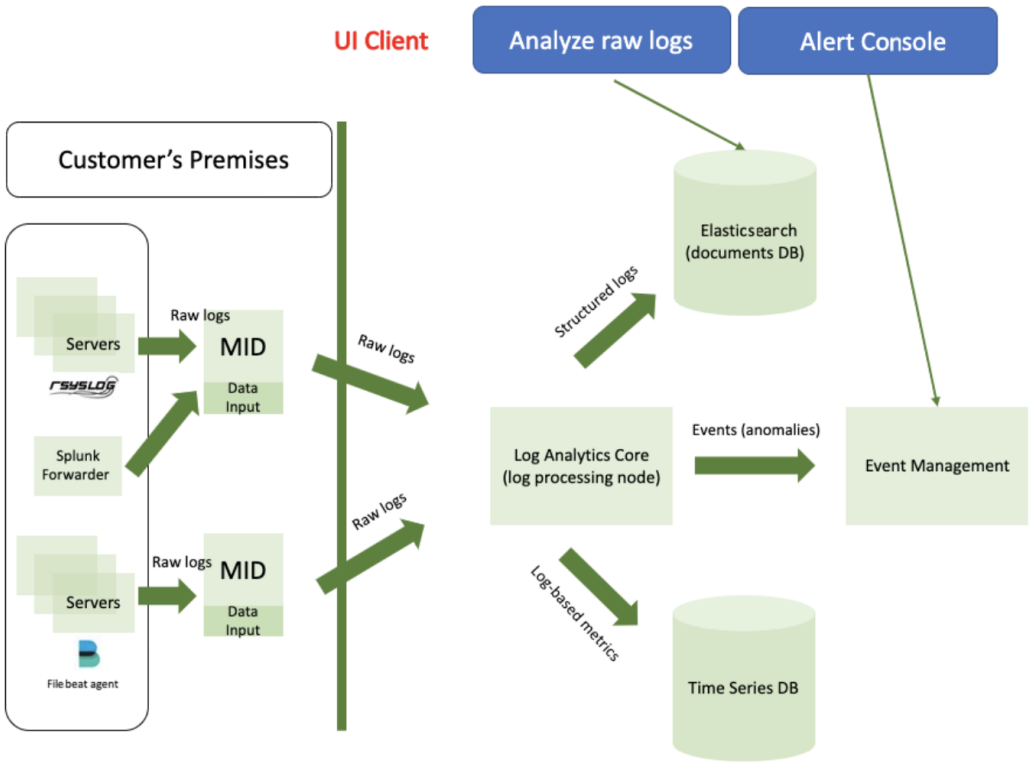

Figure 1: HLA Architecture

2.2 HLA Workflow

Figure 2: HLA Workflow

2.3 HLA Flow

⇒ Data Collection and Mapping: Log data streams pushed to Mid server via Agent Client Collector. Mapping is used to identify the structure of the log line for accurate automatic parsing.

⇒ Data Parsing and Normalization: Uses advanced unsupervised ML algorithm to identify patterns within logs & learn their unique data behavior creating a source type. Data normalization is done with message clustering.

⇒ Data Analysis: Anomaly detection, correlation & diagnose.

⇒ Now Platform: Workspace log viewer enables operators to view raw logs within a certain timeframe.

3. Use Cases

3.1 Zoom

Problem Statement: It is hard to find the root cause of Zoom quality issues. Incidents where quality of zoom calls are reported leads to downgraded performance and quality of the zoom.

Solution: Log viewer to provide detailed analysis in preventive action to be taken by reviewing anomalies provided by HLA, thus reducing incidents. Predict the performance of Zoom Quality of Experience.

Steps:

1. Prepare the MID Server with property name as mid public_ip with the public IP address as the value and enable log ingestion.
2. Request for Splunk Corp Access (https://splunk.corp.service-now.com) using catalog item.
3. Create a new Splunk token using the “New Token” button. Fill the form and copy the token after creating.

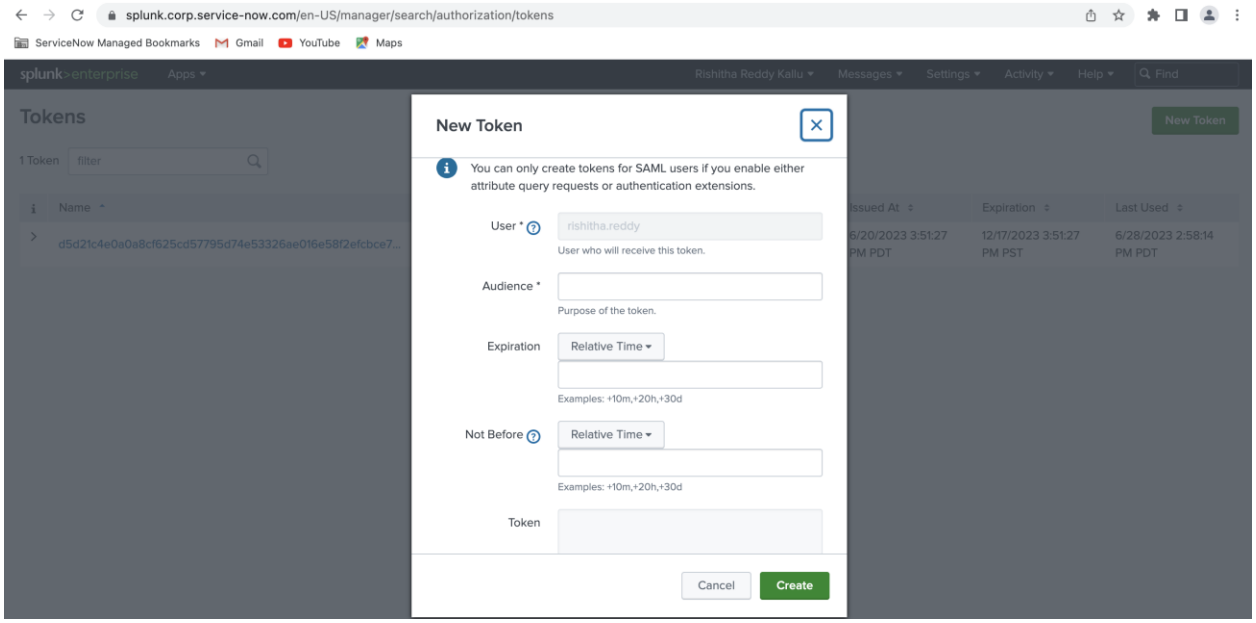

Figure 3: Splunk Token

4. Write a python script to retrieve all zoom logs data recorded within last 5 minutes from Splunk using the search query "search index=zoom earliest=-5m" into a text file.
5. Create a TCP Data Input Configuration on the instance.

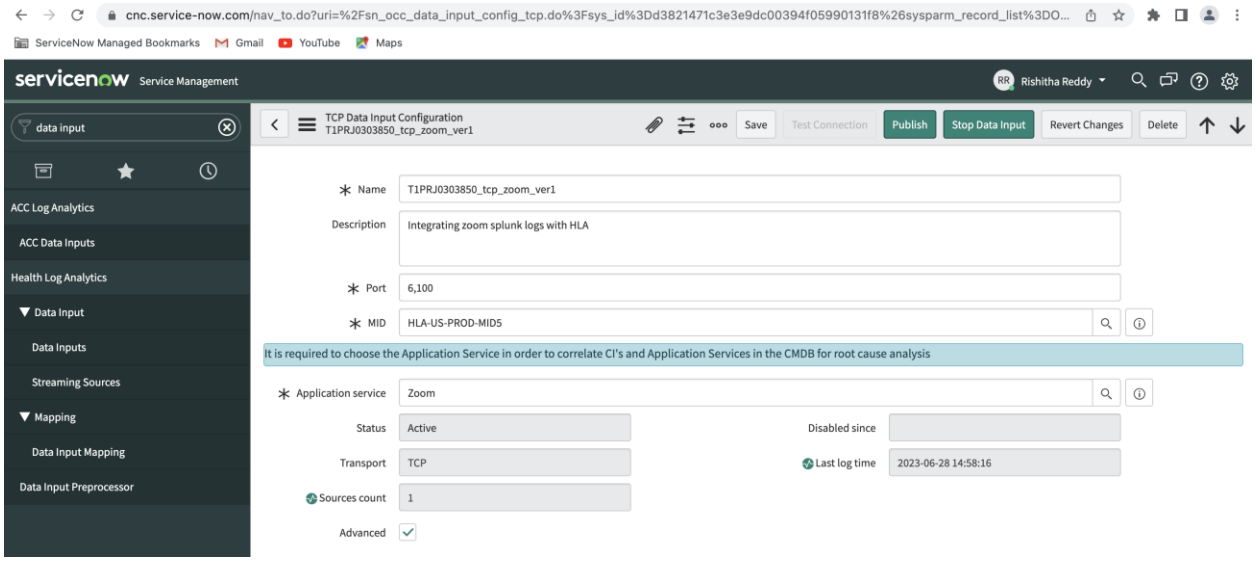

Figure 4: TCP Data Input Configuration

6. Configure the Data Input Preprocessor using the custom JavaScript function. Manipulate the raw log data by filtering, editing or splitting the log data.

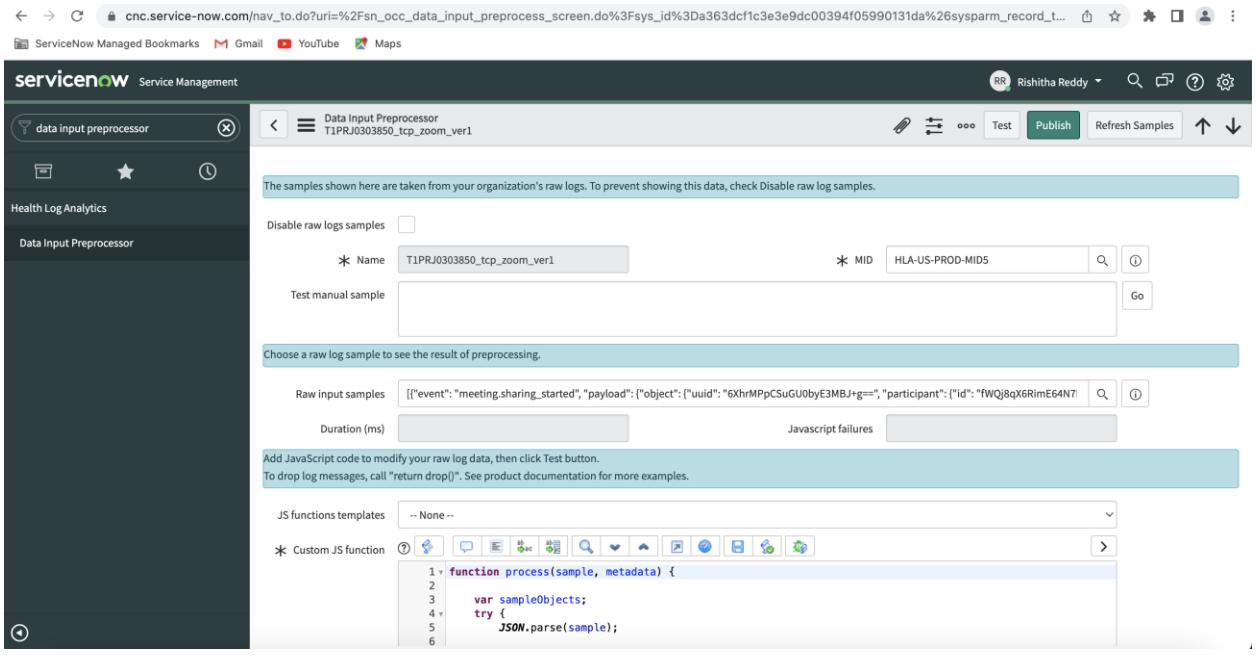

Figure 5: Data Input Preprocessor

7. Write a shell script to send logged data from text file to server with the above specified port for HLA.
8. Write a shell script where mid server can automatically execute the scripts.

9. Login to a jump server using Microsoft Remote Desktop.
10. Upload the scripts to the mid server from local host using WinSCP with ADM account credentials.

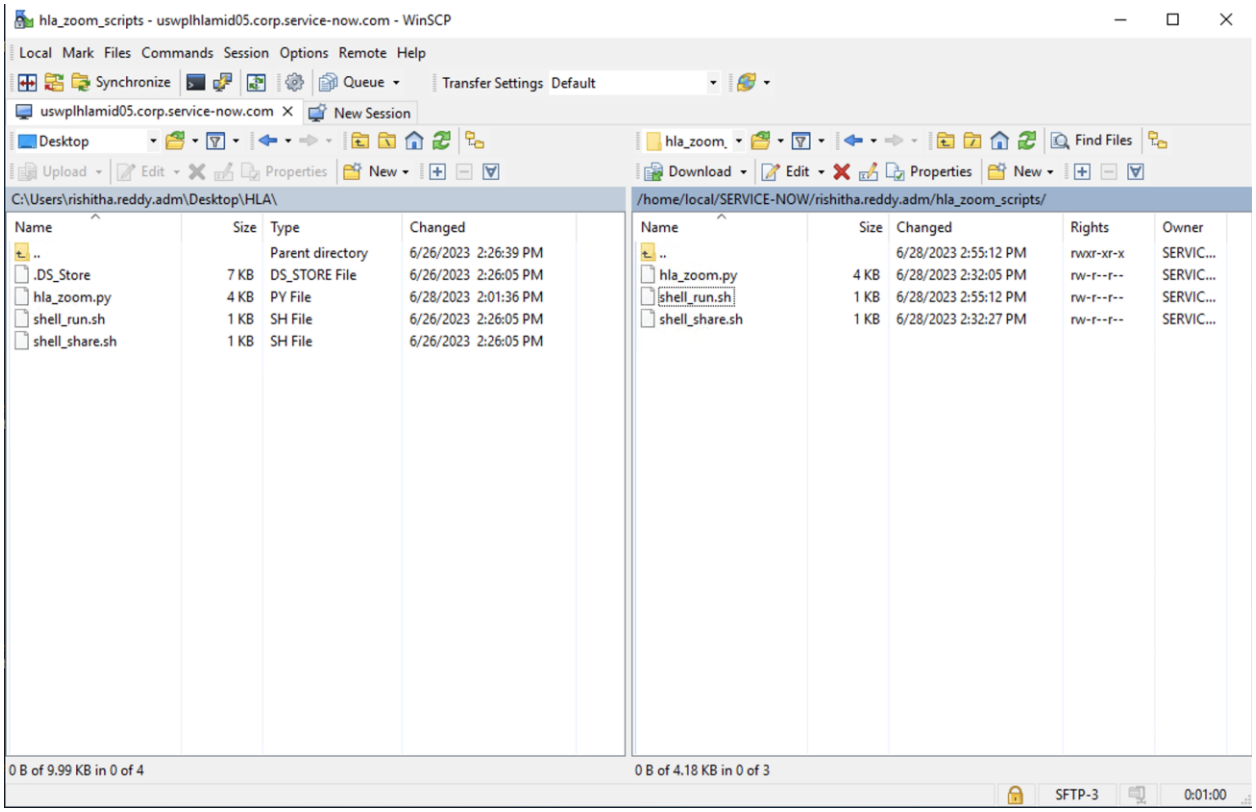

Figure 6: WinSCP file transfer

11. Login with ADM account credentials in PuTTY.
12. Schedule a cronjob using “crontab -e” command for the shell script to run accordingly.

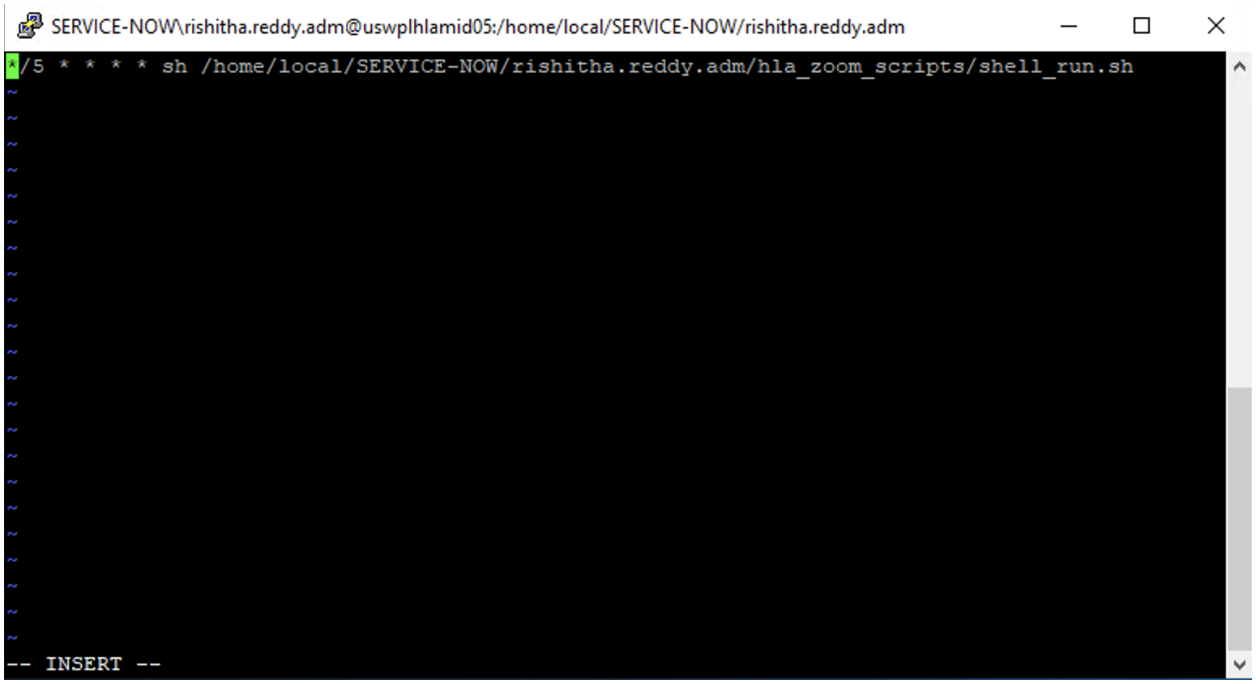

Figure 7: Cronjob to run script every 5 minutes

13. Check the data input mapping for the raw input samples retrieved from Splunk.

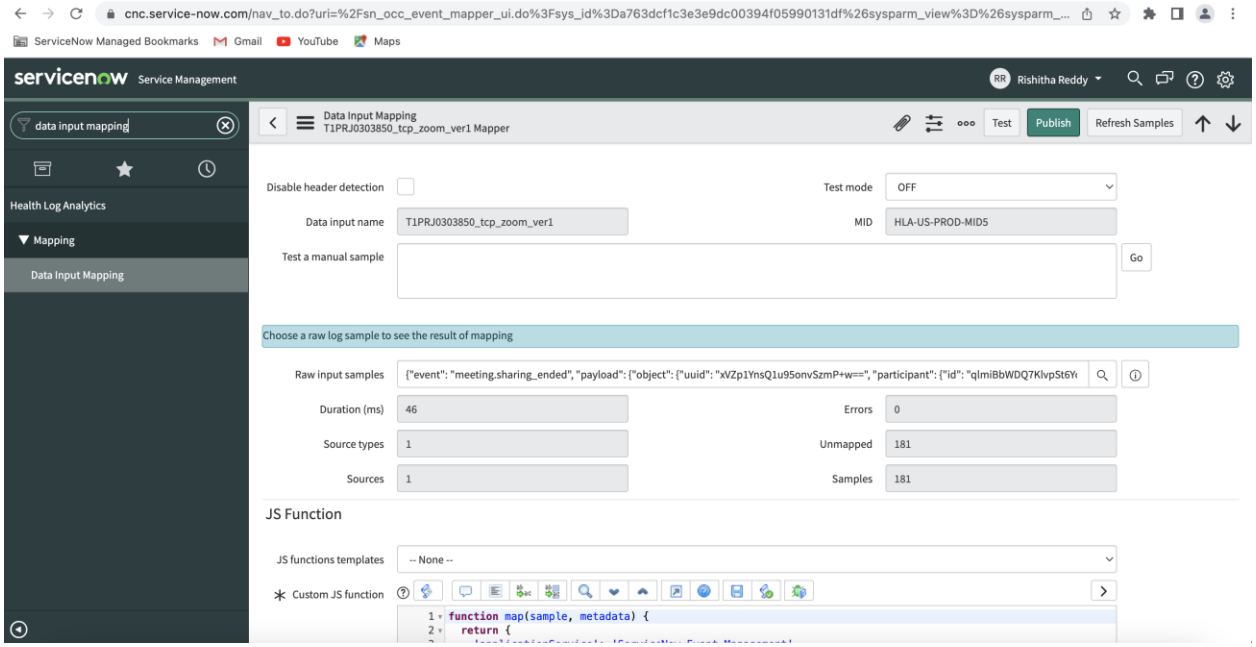

Figure 8: Data Input Mapping

14. Configure JavaScript function in source type structure to change or apply different classifications or labels to each of the key value pairs.

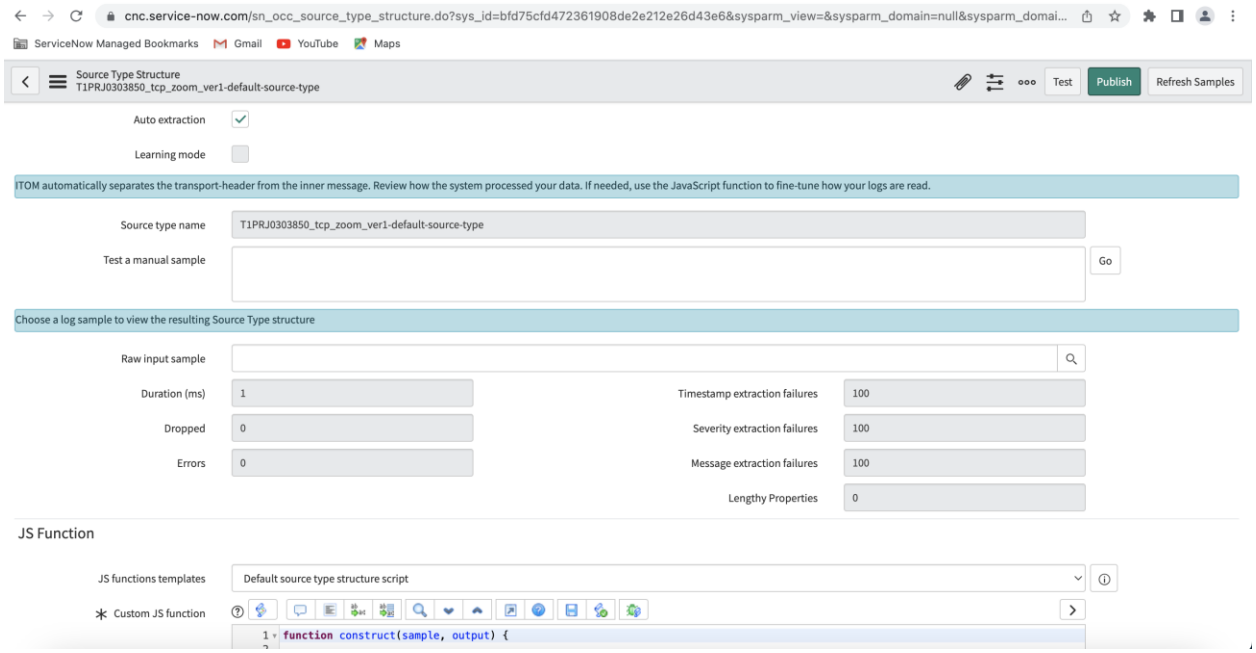

Figure 9: Source Type Structure

15. Actively streaming log sources are stored in the table. Their data behaviors will be learned automatically by AI and will create alerts for any anomalies it detects.

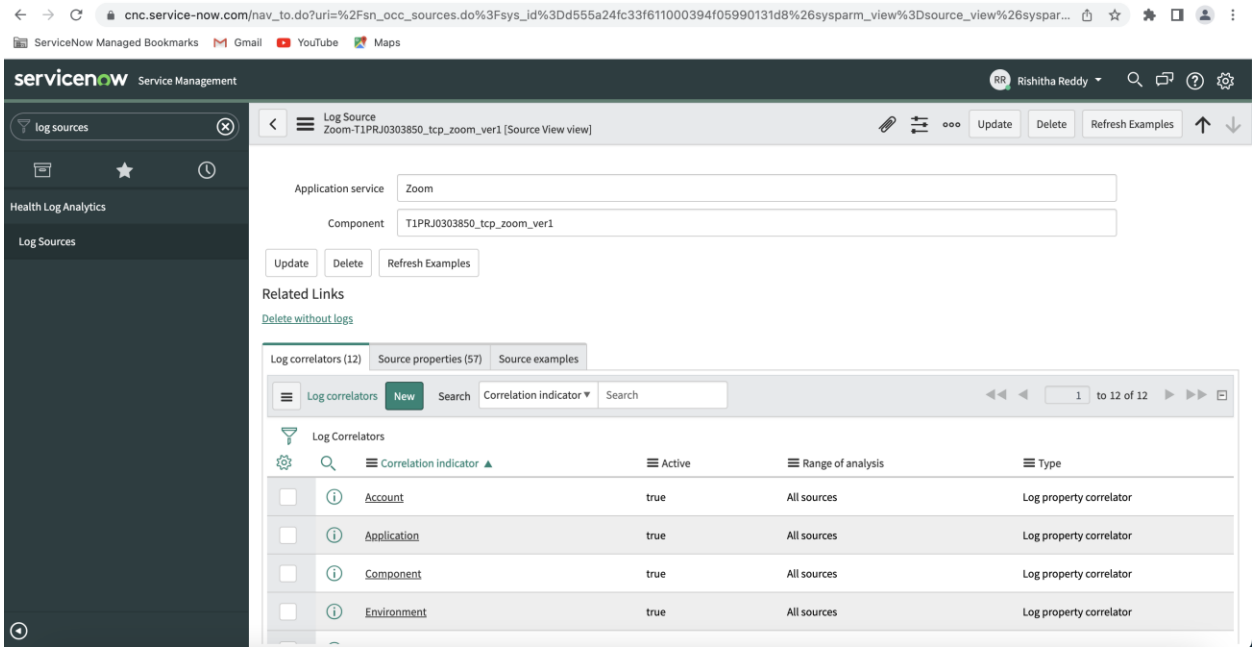

Figure 10: Log Sources

4. Revision History

Version	Written By	Section(s)	Summary
1 [06/07/2023]	Rishitha Reddy Kallu	All	Initial version of the document