Problem.3

The most open ended question. Create a log aggregation tool for a application log and having following structure. The log aggregation tool could be a desktop tool. The application log is rotated based on size as well as date. The naming convention of log is -

\\server-name\application-name\component\version\component-dd\_mm\_yyyy.log

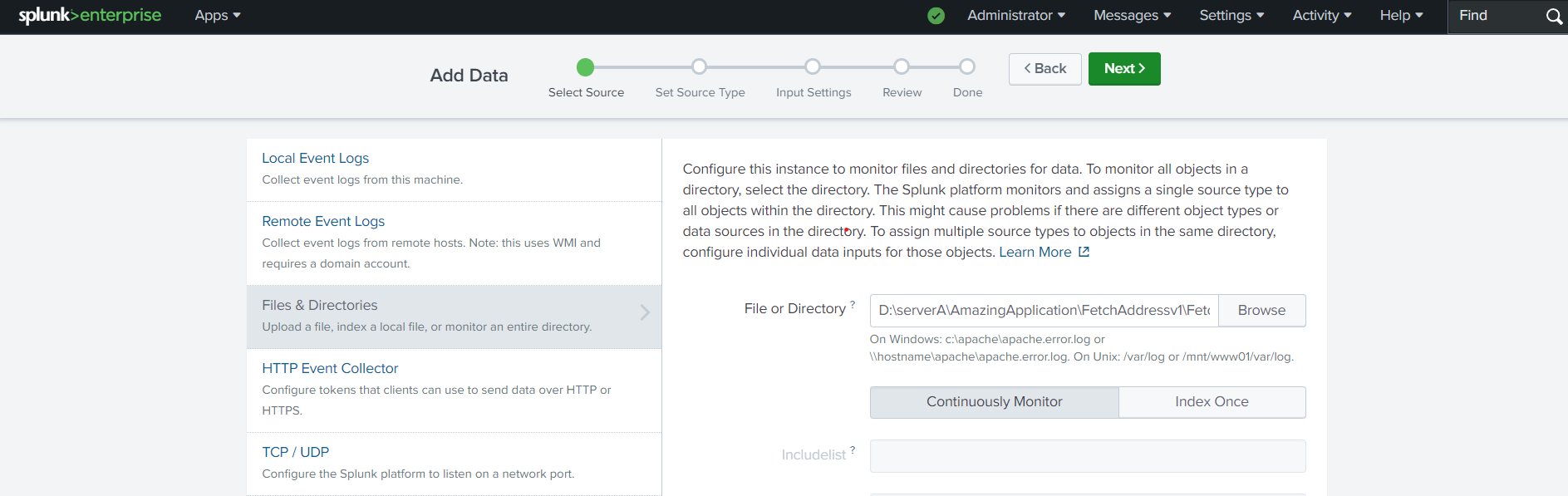
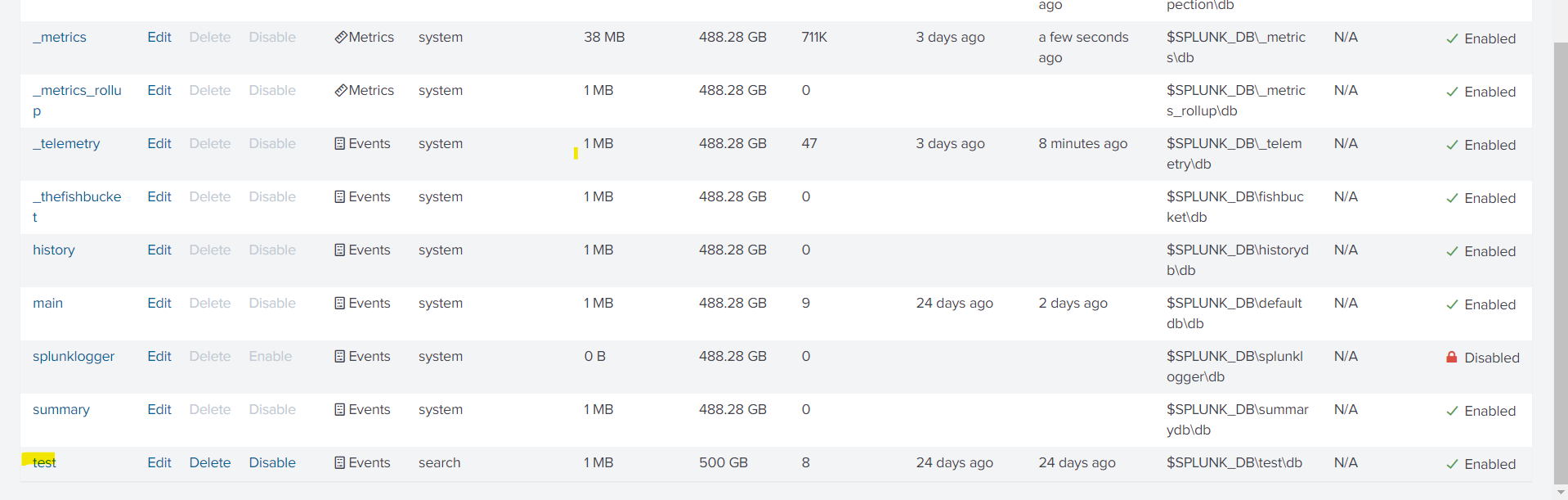
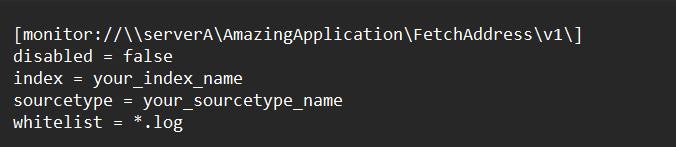
Solution :

For the above problem I have used Splunk for log aggregation as it’s a powerful tool designed specifically for collecting, searching, and analyzing log data.

**Pre-requisite**

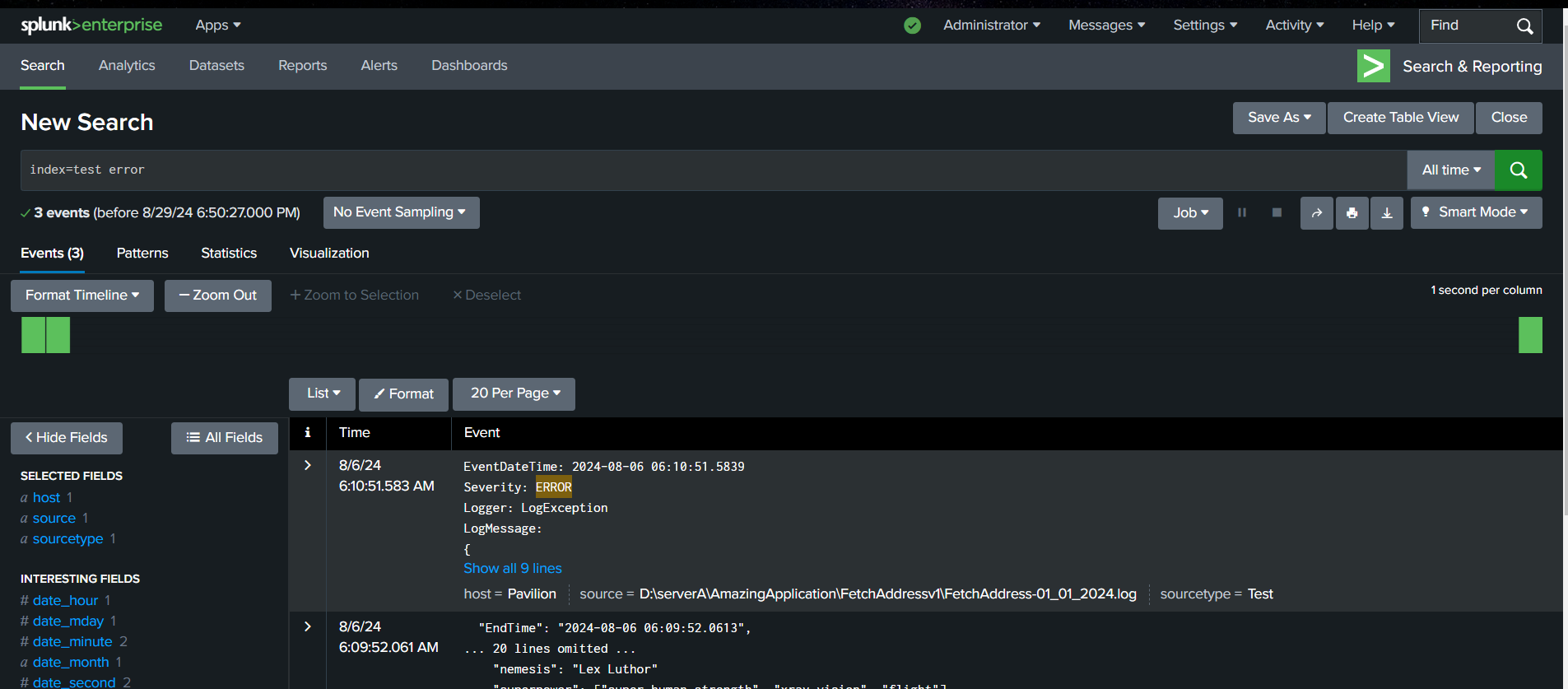
* Download and install Splunk Enterprise or use Splunk Cloud, in this case I have downloaded Splunk Enterprise in my local system.
* After installation, you can access the Splunk web interface, typically via <http://localhost:8000>.

**Steps to Use :**

* First to use Splunk and visualize the data, we need to Configure Data InputsIn Splunk through which we will ingest data to Splunk.
* Navigate to Settings > Data Inputs, Choose Files & Directories to monitor logs from the specific directory structure.
* Specify the directory path that matches your log structure, e.g., [\\server-name\application-name\component\version\](file:///\\server-name\application-name\component\version\).
* 
* Create a new index in Splunk to store these logs (e.g.,test), This will help you to organize your logs separately from other data in Splunk.
* 
* Here we are directly specifying the file which Splunk need to ingest, if we want Splunk to read the given directory and take logs.
* Go to input.conf in this path C:\Program Files\Splunk\etc\system\local and change the file content like the below screenshot.
* 
* Save the file and restart your splunk.
* Now use the Search & Reporting app in Splunk to create searches that aggregate your logs.
* You can filter by date, component, or log content using SPL (Search Processing Language).
* Example SPL query:

index=my\_application\_logs error

* Splunk can handle rotated logs automatically as long as the file names are consistent with the pattern you defined.
* Ensure that the data inputs are configured to continuously monitor the directory so that new log files are indexed as they are created.



Improvement :

Using Splunk Universal Forwarder we can configure Splunk to get logs to Splunk cloud from other servers.

We can also use Field extractions to help Splunk identify and categorize different parts of your log files, making searches more efficient.