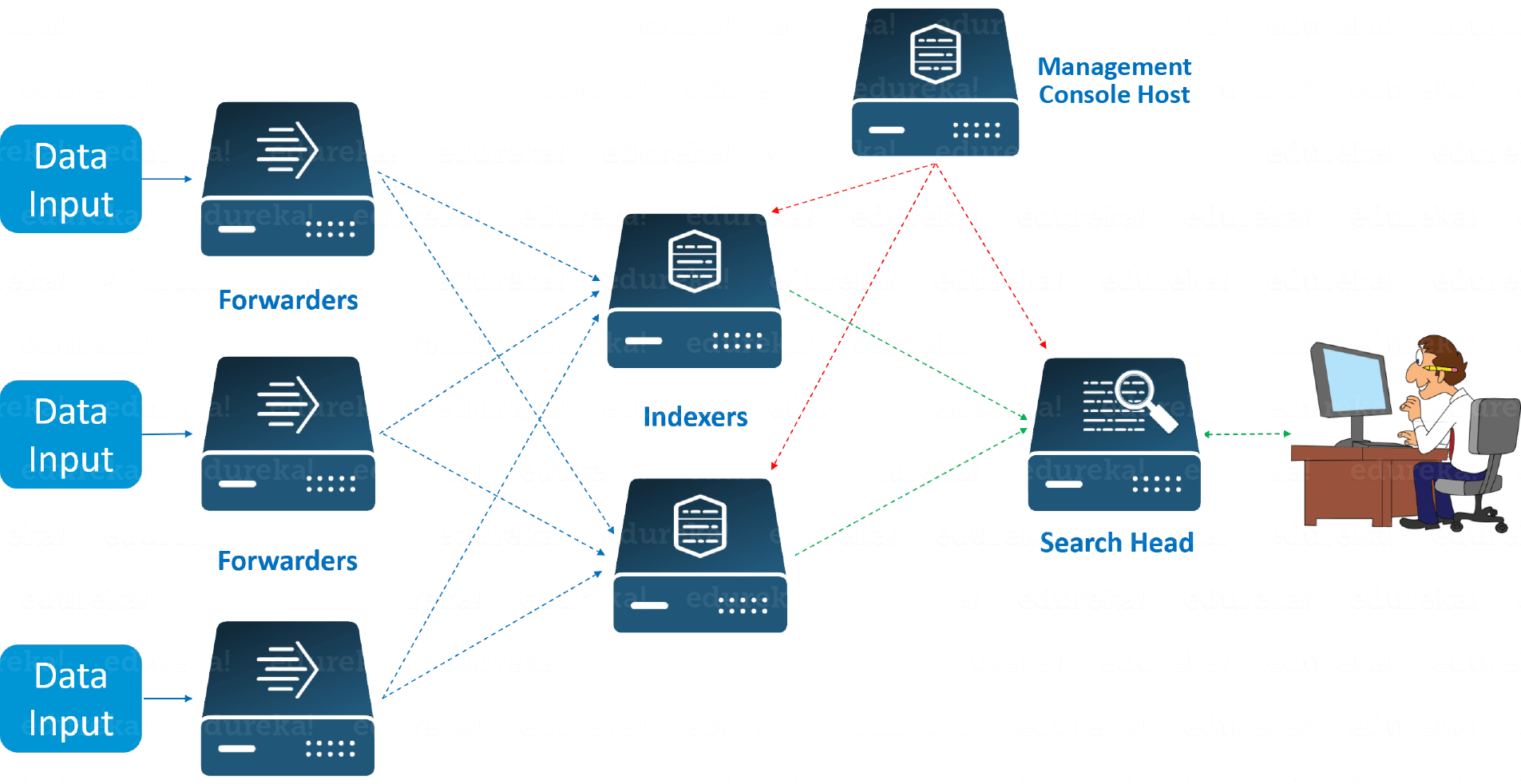
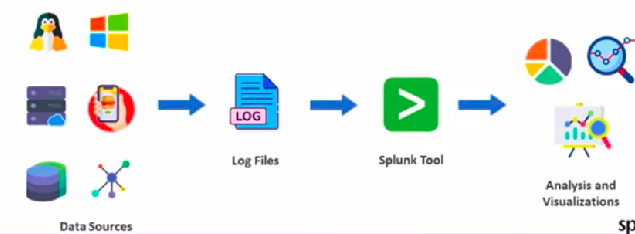
**SPLUNK**

Splunk is a software platform widely used for monitoring, searching, analyzing and visualizing the machine-generated data in real time. It performs capturing, indexing, and correlating the real time data in a searchable container and produces graphs, alerts, dashboards and visualizations.



**This is a simple diagram to show what basically Splunk do-:**

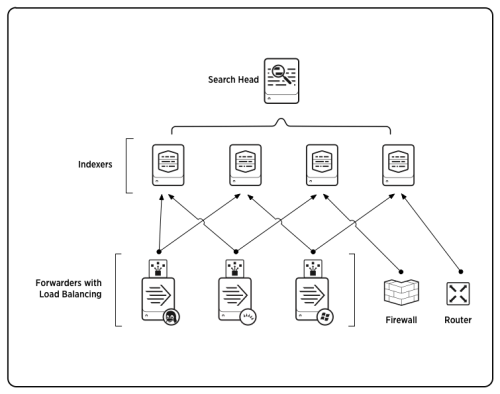
****

# **Splunk Components-:**

There are 3 main components in Splunk:

* **Splunk Forwarder-:** Splunk Forwarder is the component which you have to use for collecting the logs. Suppose, you want to collect logs from a remote machine, then you can accomplish that by using Splunk’s remote forwarders which are independent of the main Splunk instance.
* **Splunk Indexer-:** Indexer is the Splunk component which you will have to use for indexing and storing the data coming from the forwarder. Splunk instance transforms the incoming data into events and stores it in indexes for performing search operations efficiently.

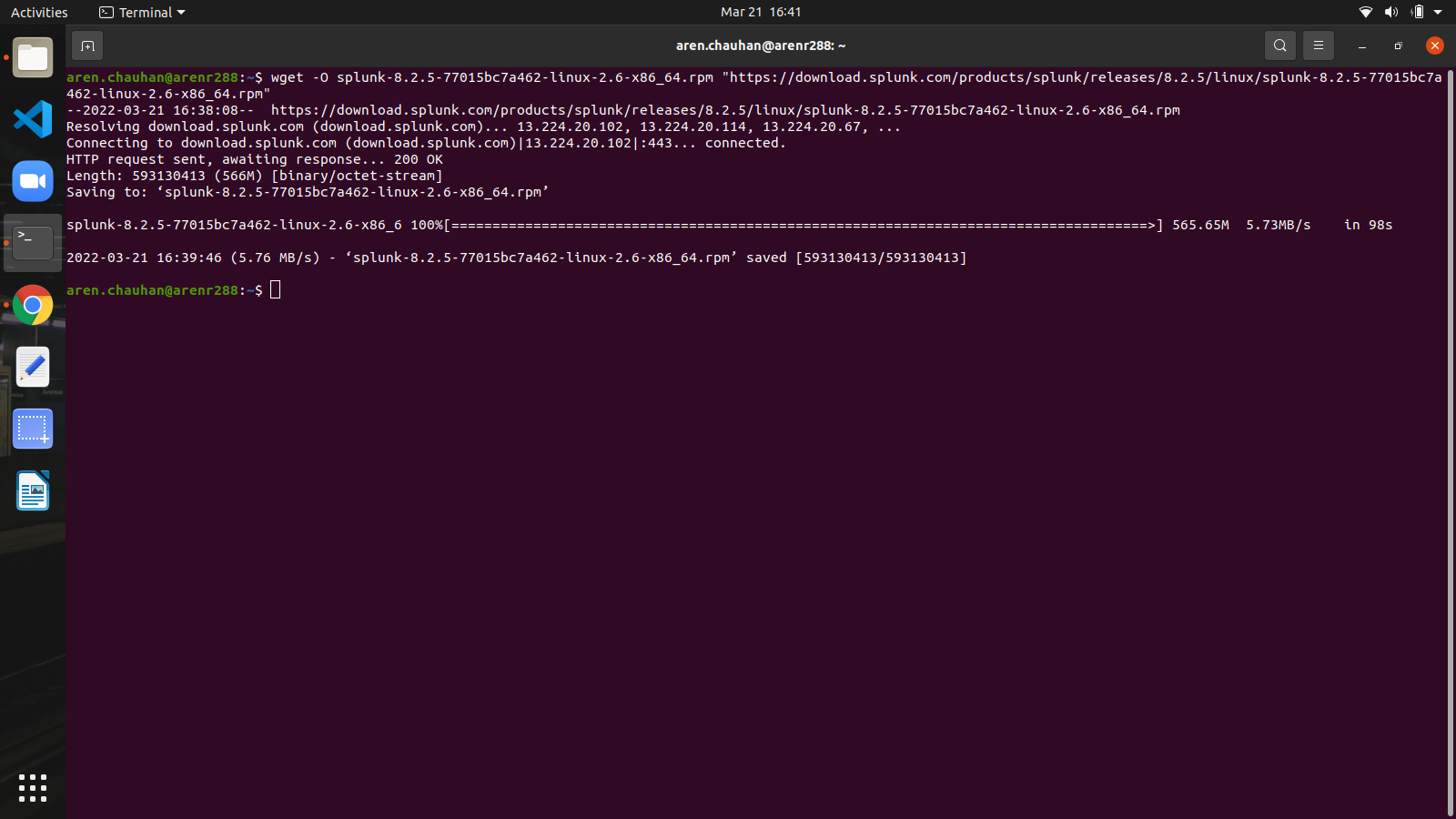
* **Search Head-:** Search head is the component used for interacting with Splunk. It provides a graphical user interface to users for performing various operations. You can search and query the data stored in the Indexer by entering search words and you will get the expected result.



# **How To Install Splunk In Ubuntu**

**Step-1 -: Install by using this Command**

wget -O splunk-8.2.5-77015bc7a462-linux-2.6-amd64.deb "<https://download.splunk.com/products/splunk/releases/8.2.5/linux/splunk-8.2.5-77015bc7a462-linux-2.6-amd64.deb>"

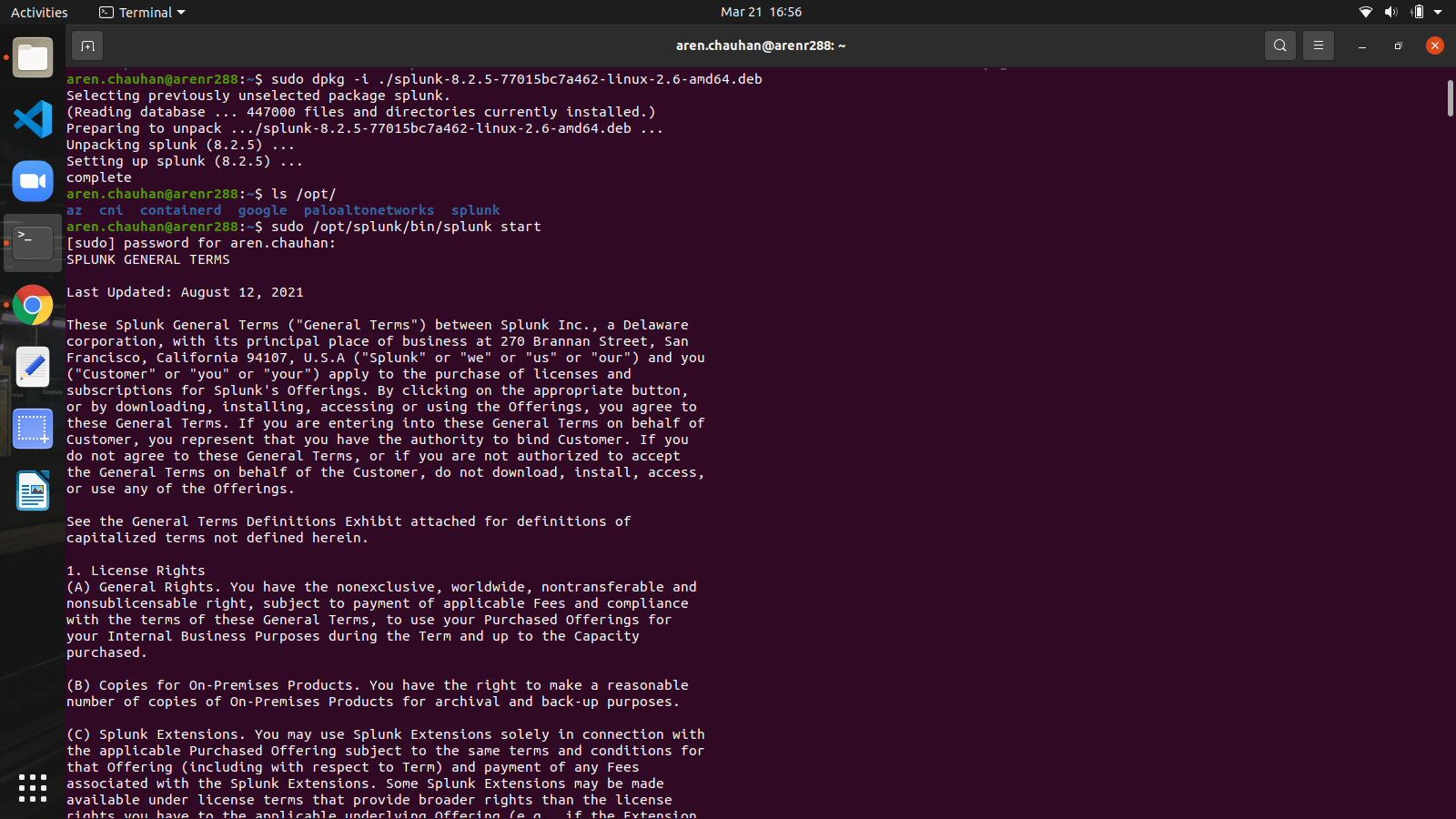


**Step-2 -: Unzip the .deb file and Start the Splunk Portal by using these commands**

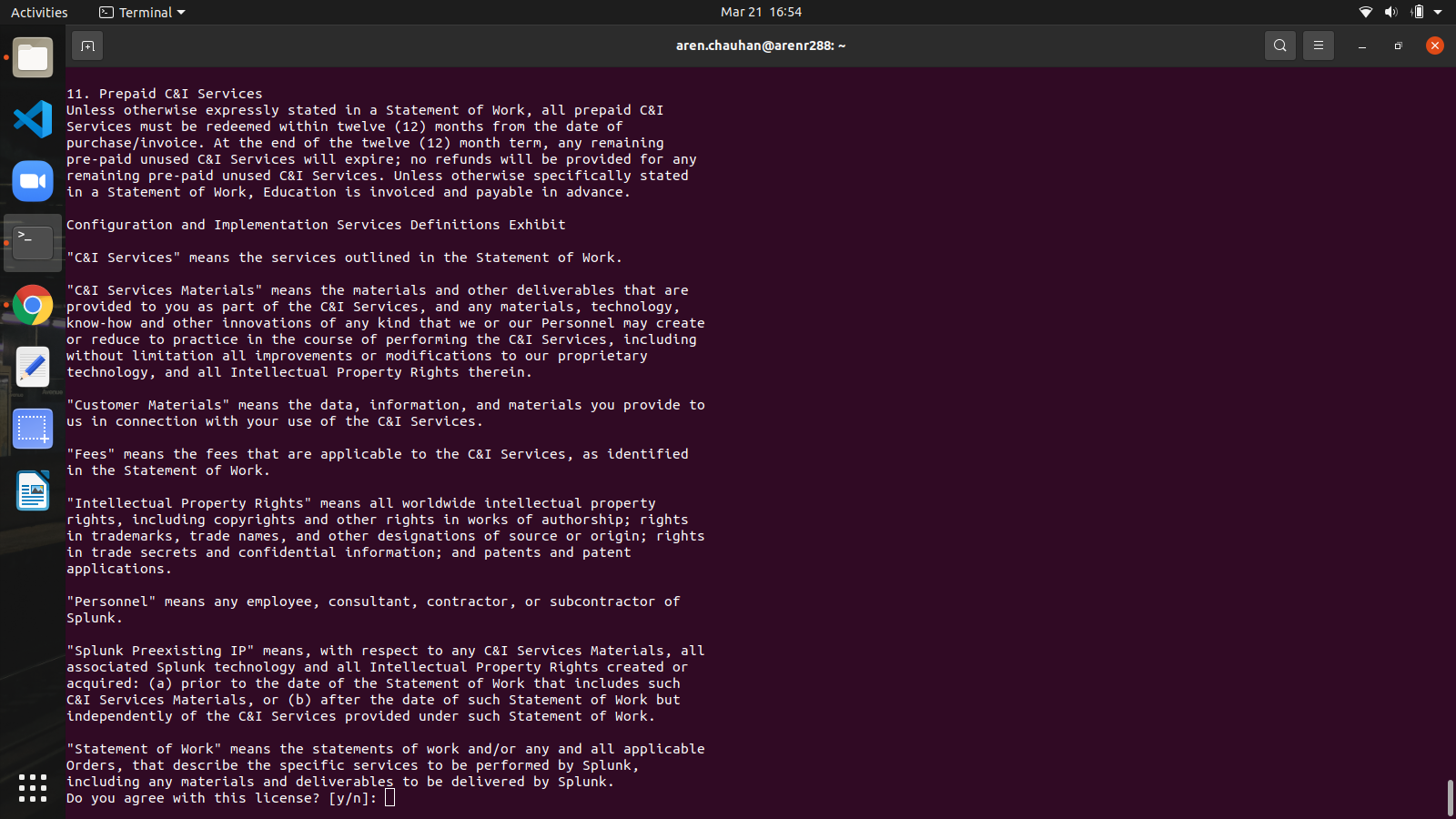
**-:** sudo dpkg -i ./splunk-8.2.5-77015bc7a462-linux-2.6-amd64.deb

**-:** ls /opt/

**-:** sudo /opt/splunk/bin/splunk start



**Step-3 -: Accept the License Agreement**

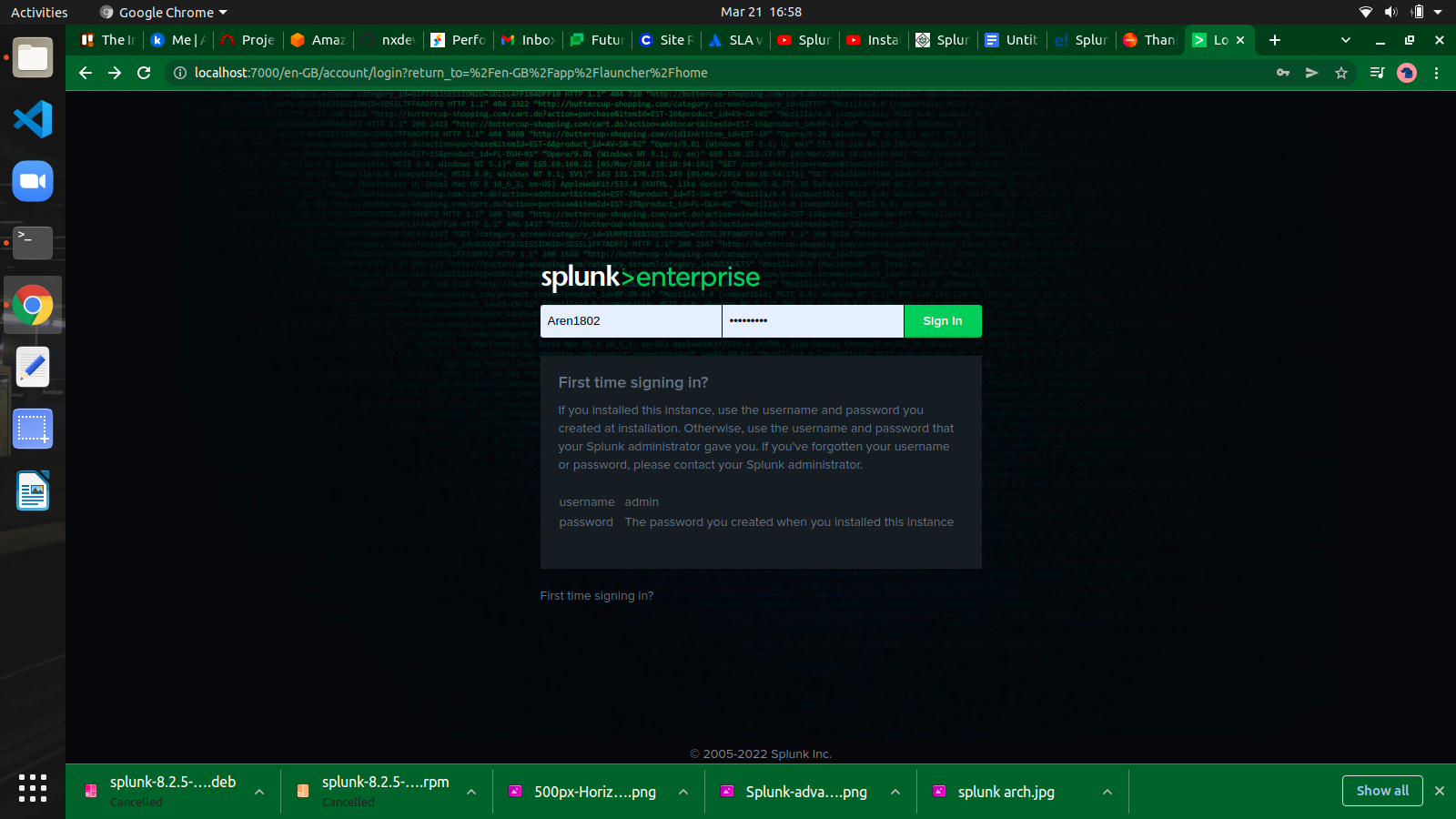


**Step-4 -: Go to your web browser and type the port number**

**(**Basically the default port for splunk is 8000 but i changed the port to 7000**)**

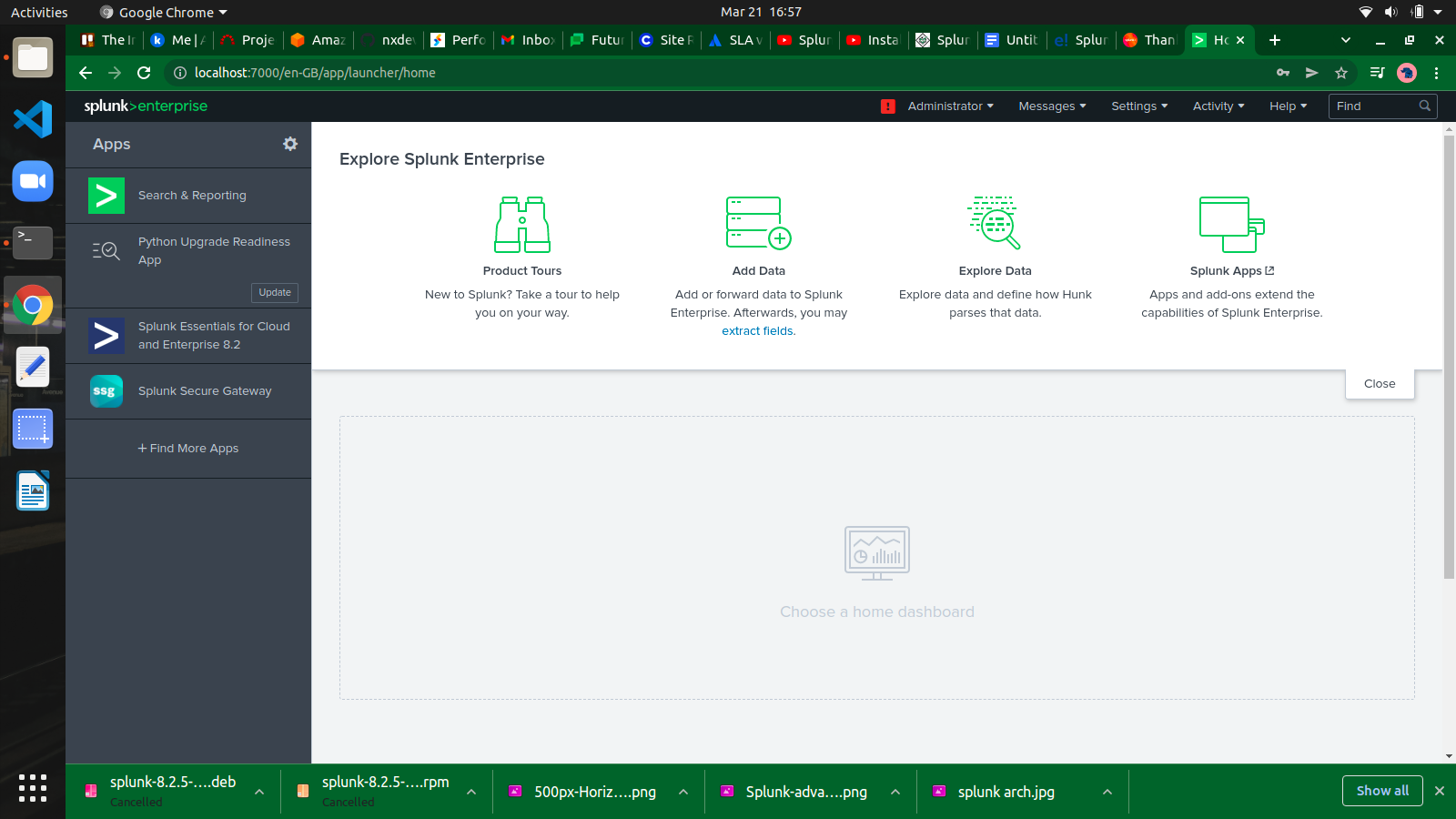
****

**-:** [**http://localhost:7000/**](http://localhost:7000/)

****

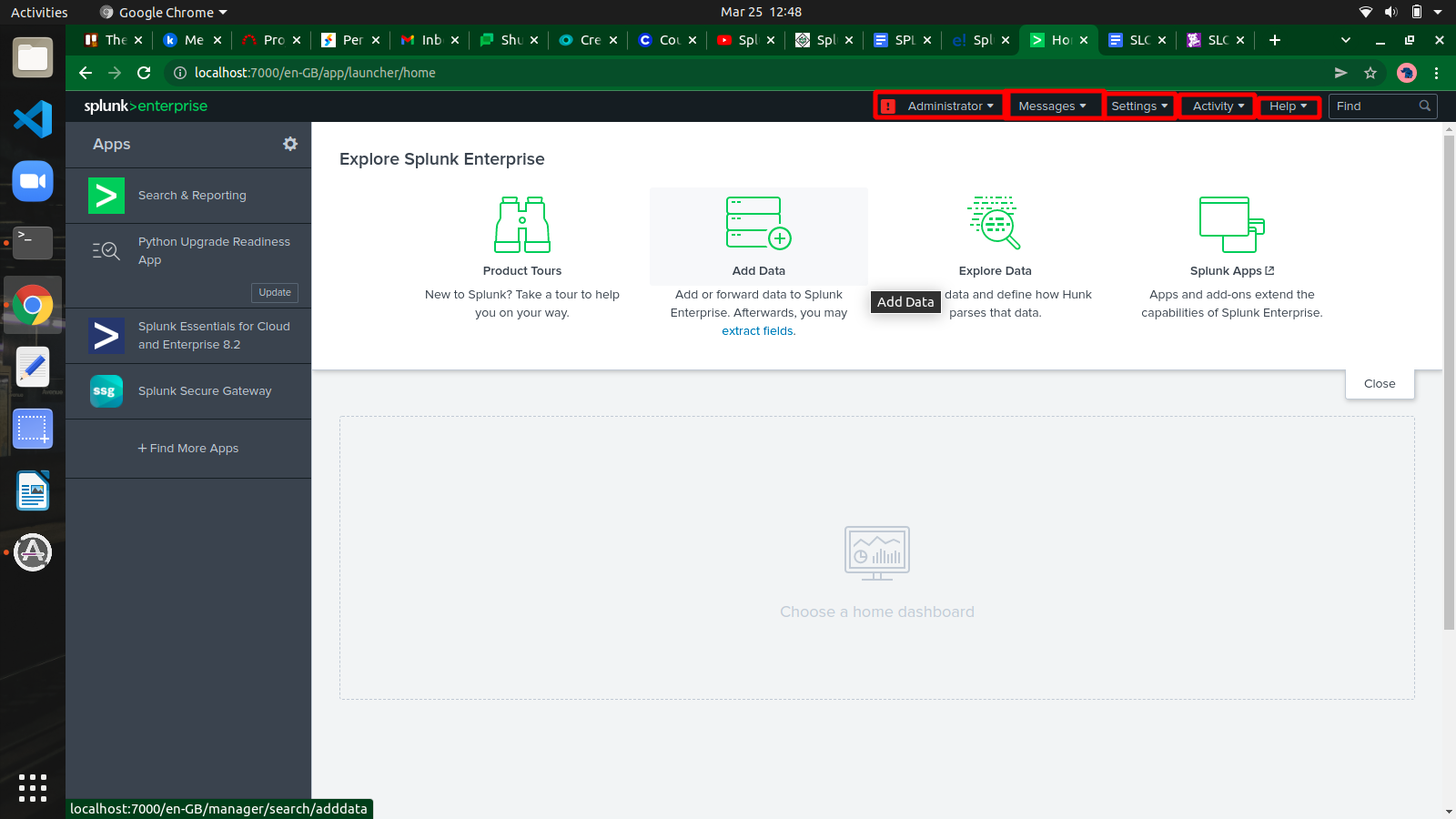
**Step-5 -: Type the Username and Password which u select for your Splunk Portal After Accepting the License Agreement.**

* **Press the LOGIN button.**

****

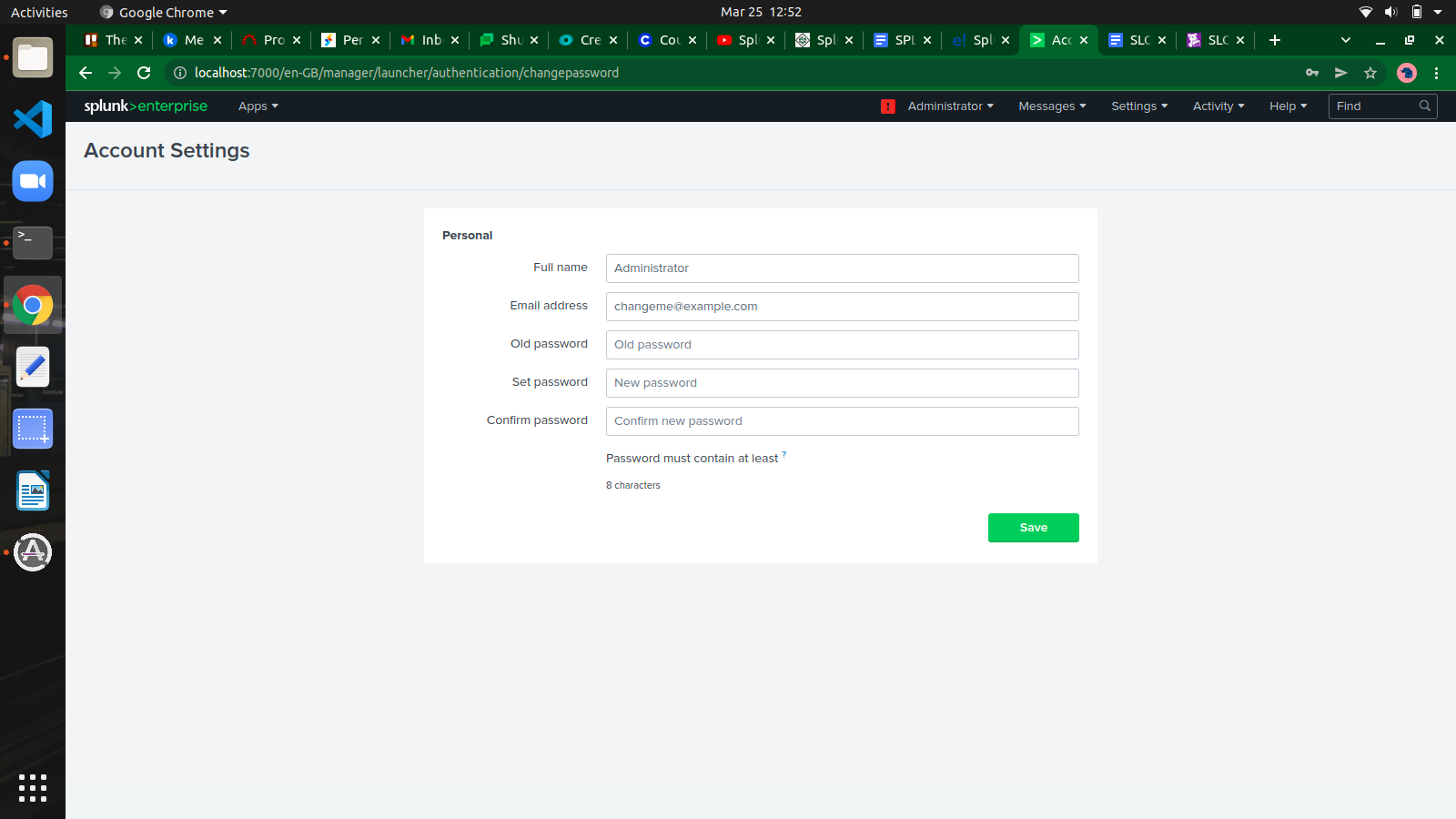
**SPLUNK PORTAL**

The Splunk web interface consists of all the tools you need to search, report and analyze the data that is ingested. The same web interface provides features for administering the users and their roles. It also provides links for data ingestion and the in-built apps available in Splunk.

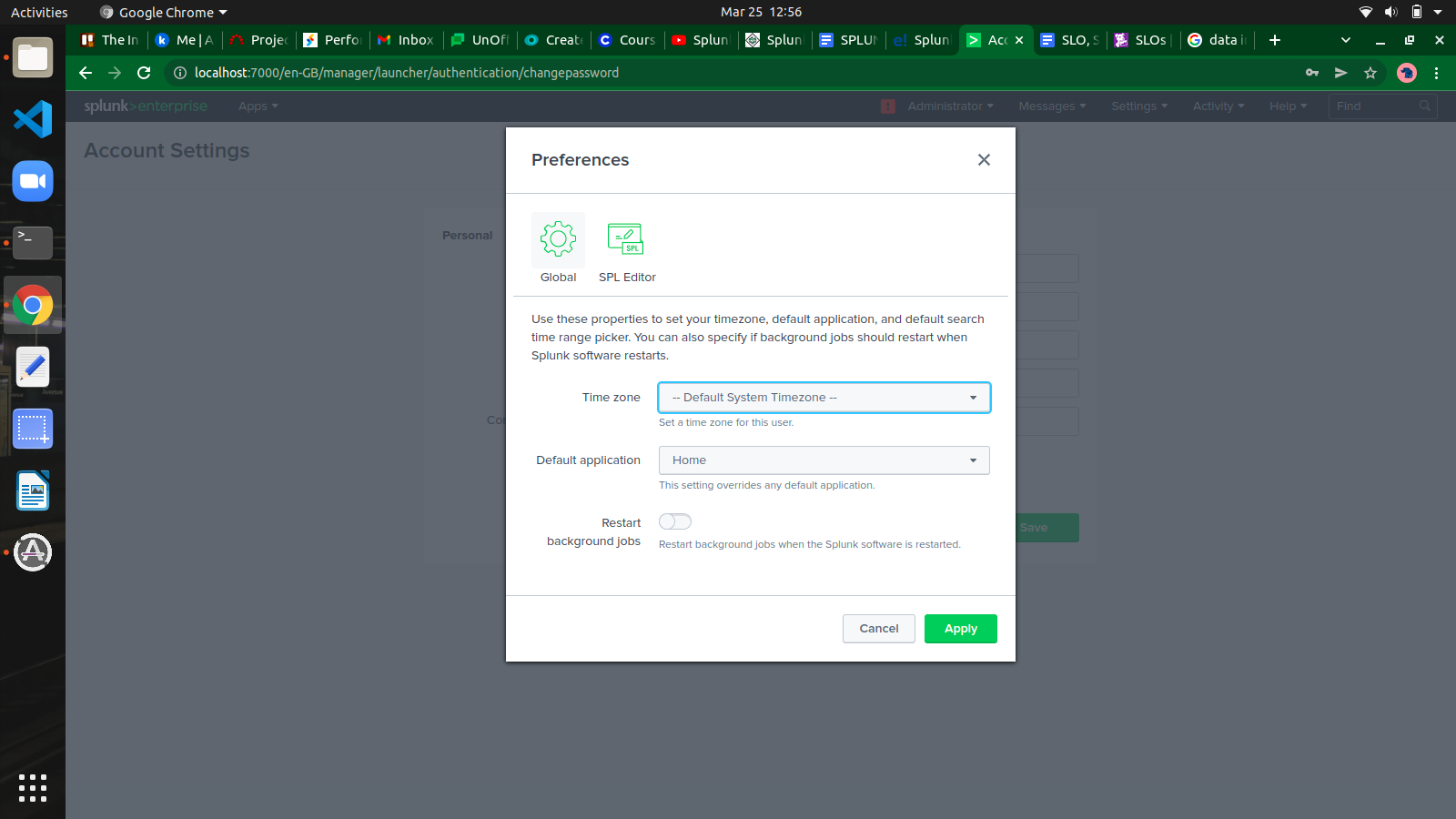


## **Administrator Link**

The Administrator drop down gives the option to set and edit the details of the administrator. We can reset the admin email ID and password using the below screen-

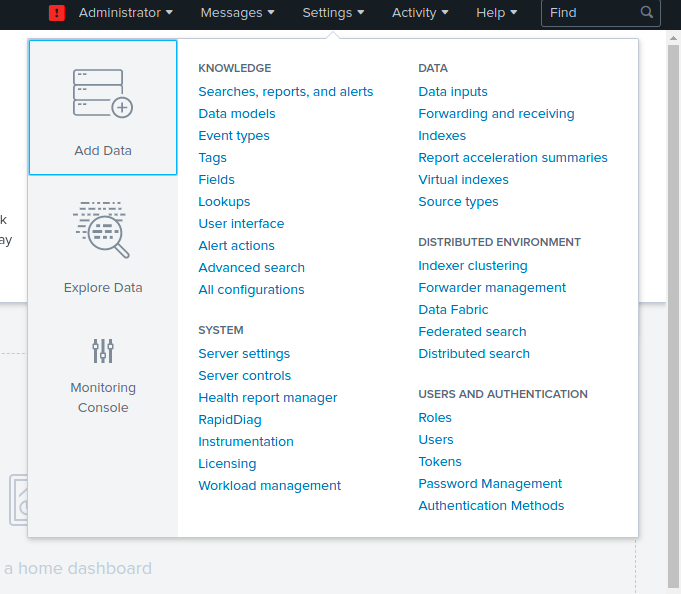


Further from the administrator link, we can also navigate to the preferences option where we can set the time zone and home application on which the landing page will open after your login. Currently, it opened on the Home page as shown below -



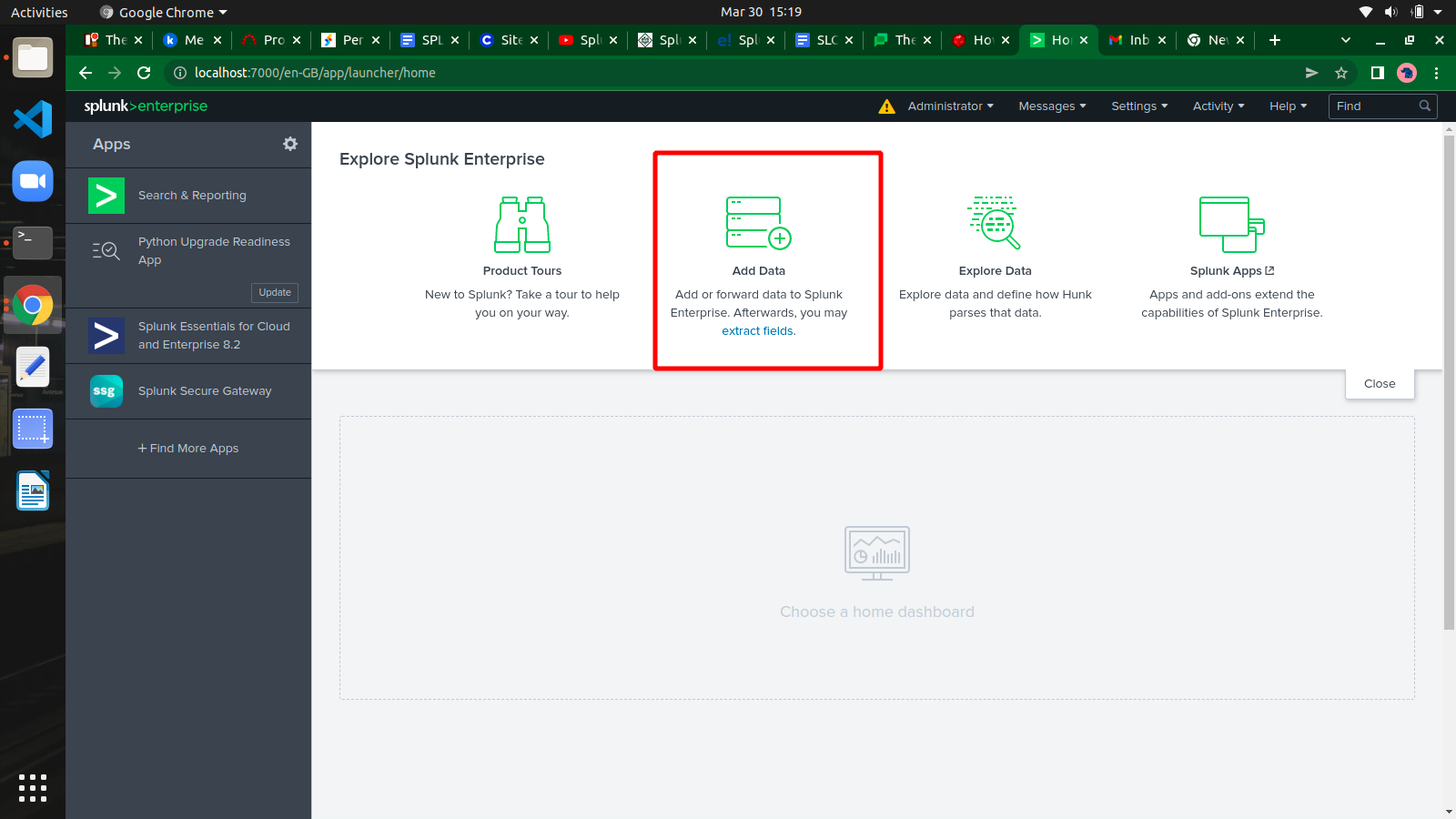
## **Settings Link**

This is a link which shows all the core features available in Splunk.



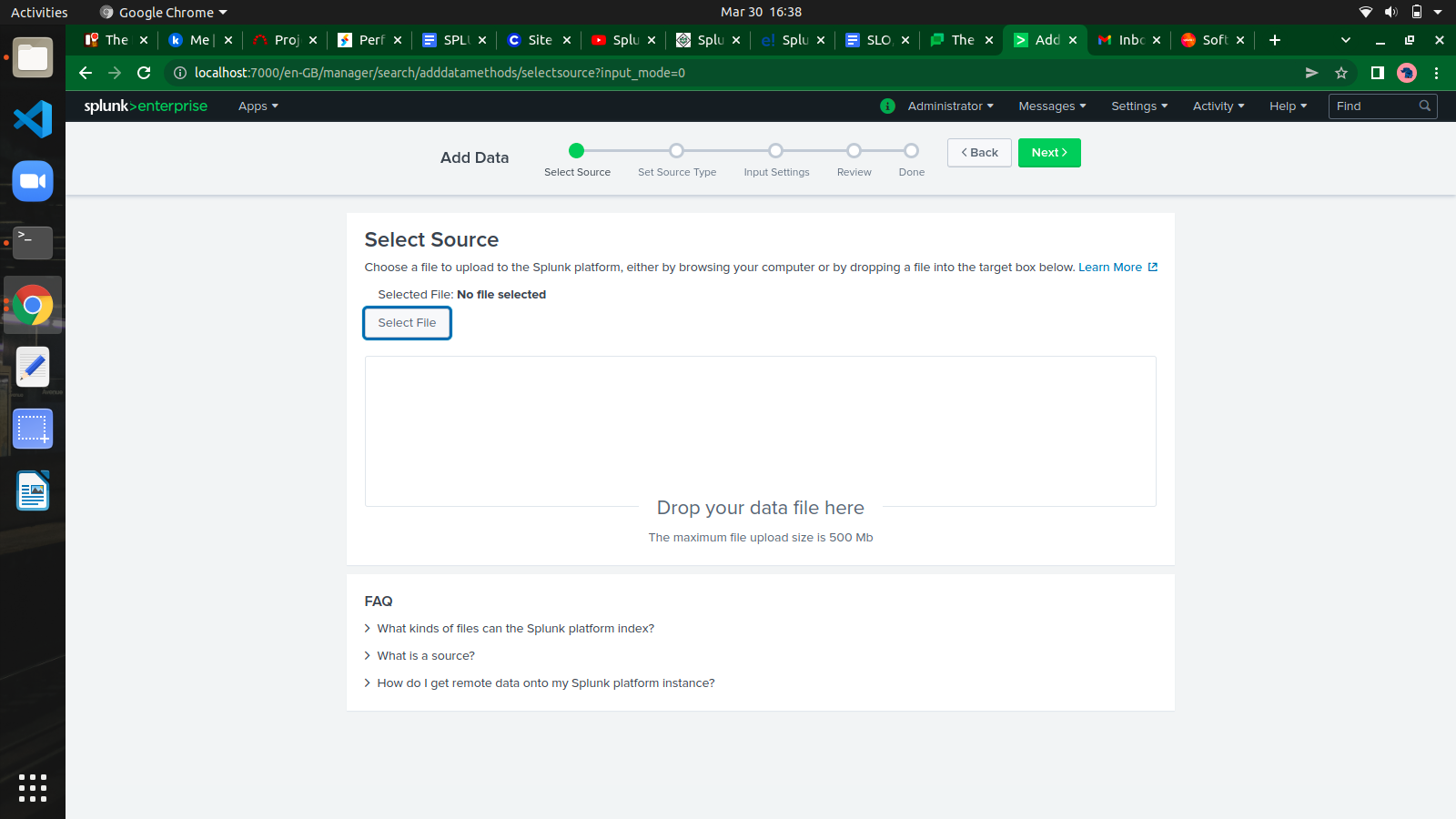
**Data Ingestion**

Data ingestion in Splunk happens through the Add Data feature which is part of the search and reporting app. After logging in, the Splunk interface home screen shows the Add Data icon-:



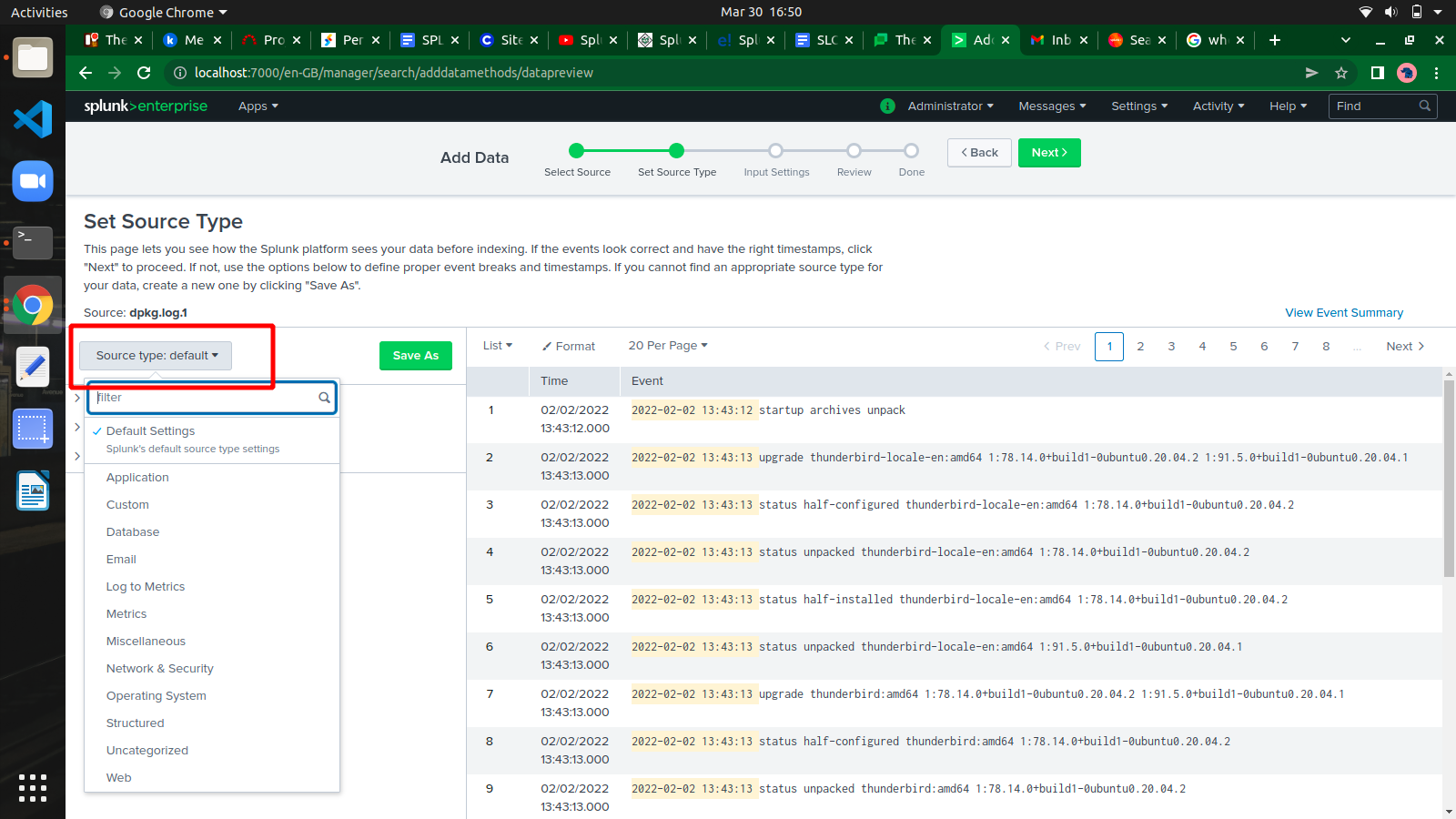
## **Uploading data**

Next, we choose the file, which we have kept in our local system. After selecting the file, we move to the next step using the green coloured next button in the top right corner.



## **Selecting Source Type**

Splunk has an in-built feature to detect the type of the data being ingested. It also gives the user an option to choose a different data type than the one chosen by Splunk.



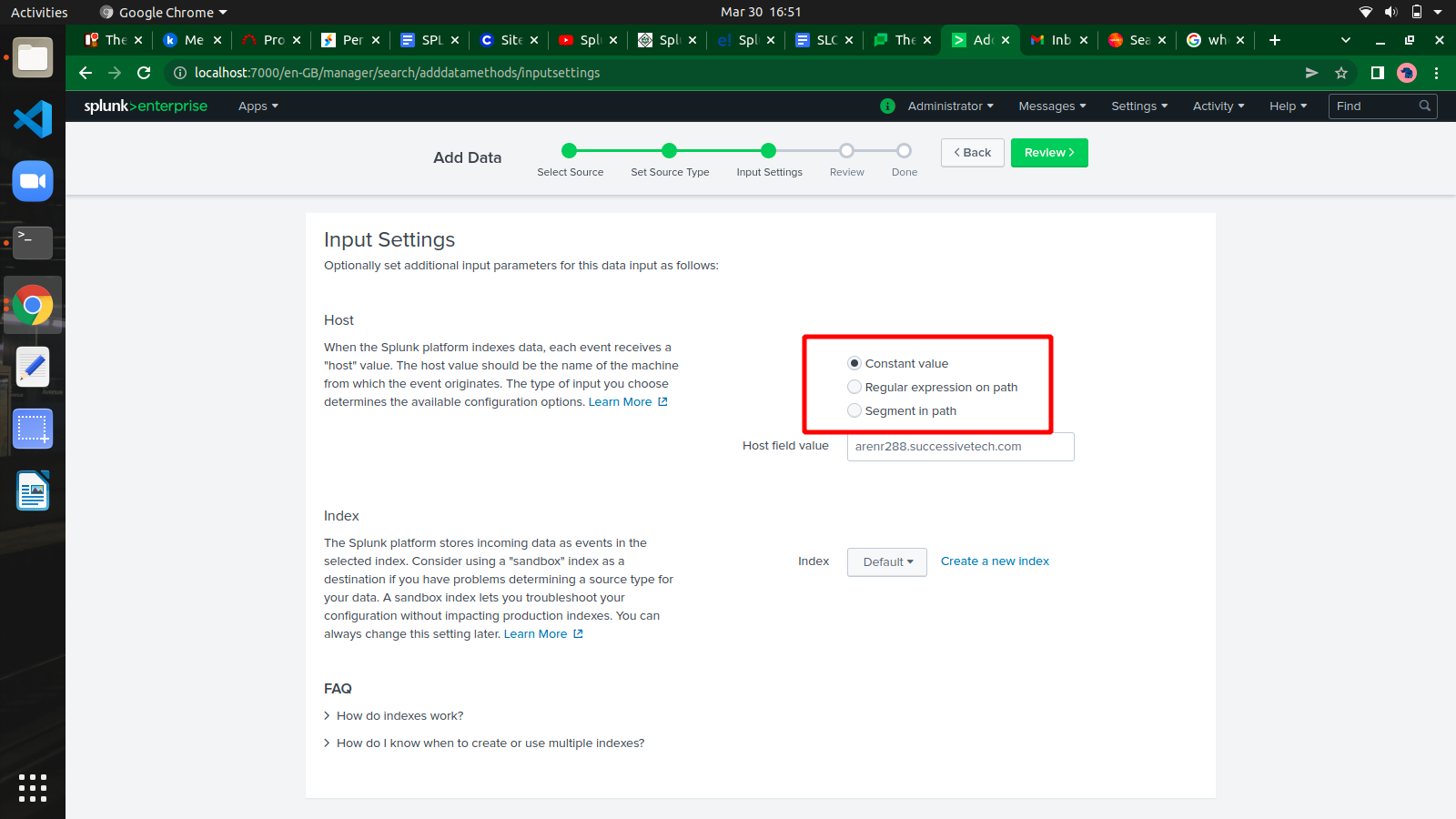
## **Input Settings**

In this step of data ingestion, we configure the host name from which the data is being ingested.

**Constant value-:** It is the complete host name where the source data resides.

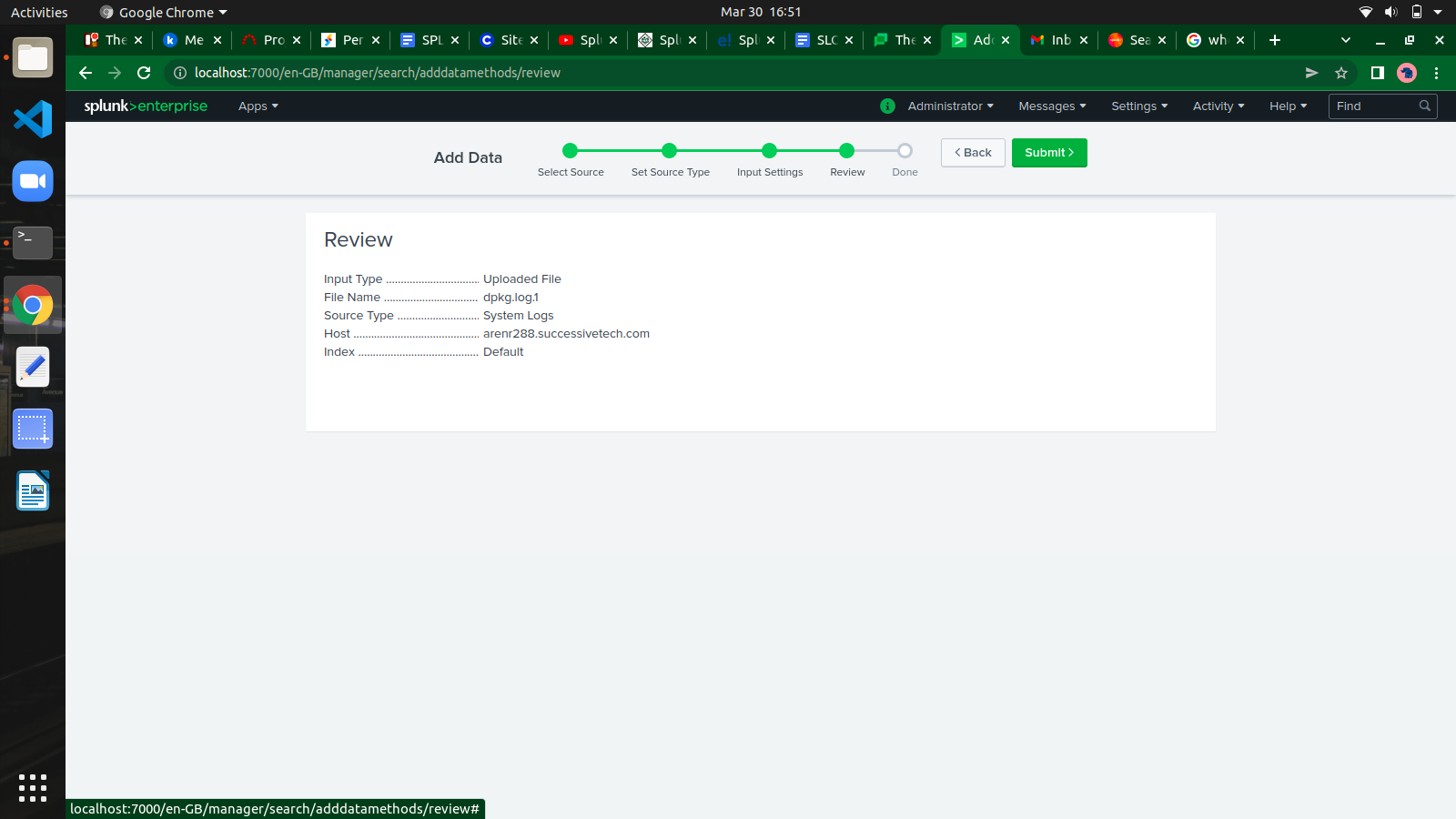
**Regex on path-:** When you want to extract the host name with a regular expression. Then enter the regex for the host you want to extract in the Regular expression field.

**Segment in path-:** When you want to extract the host name from a segment in your data source's path, enter the segment number in the Segment number field.

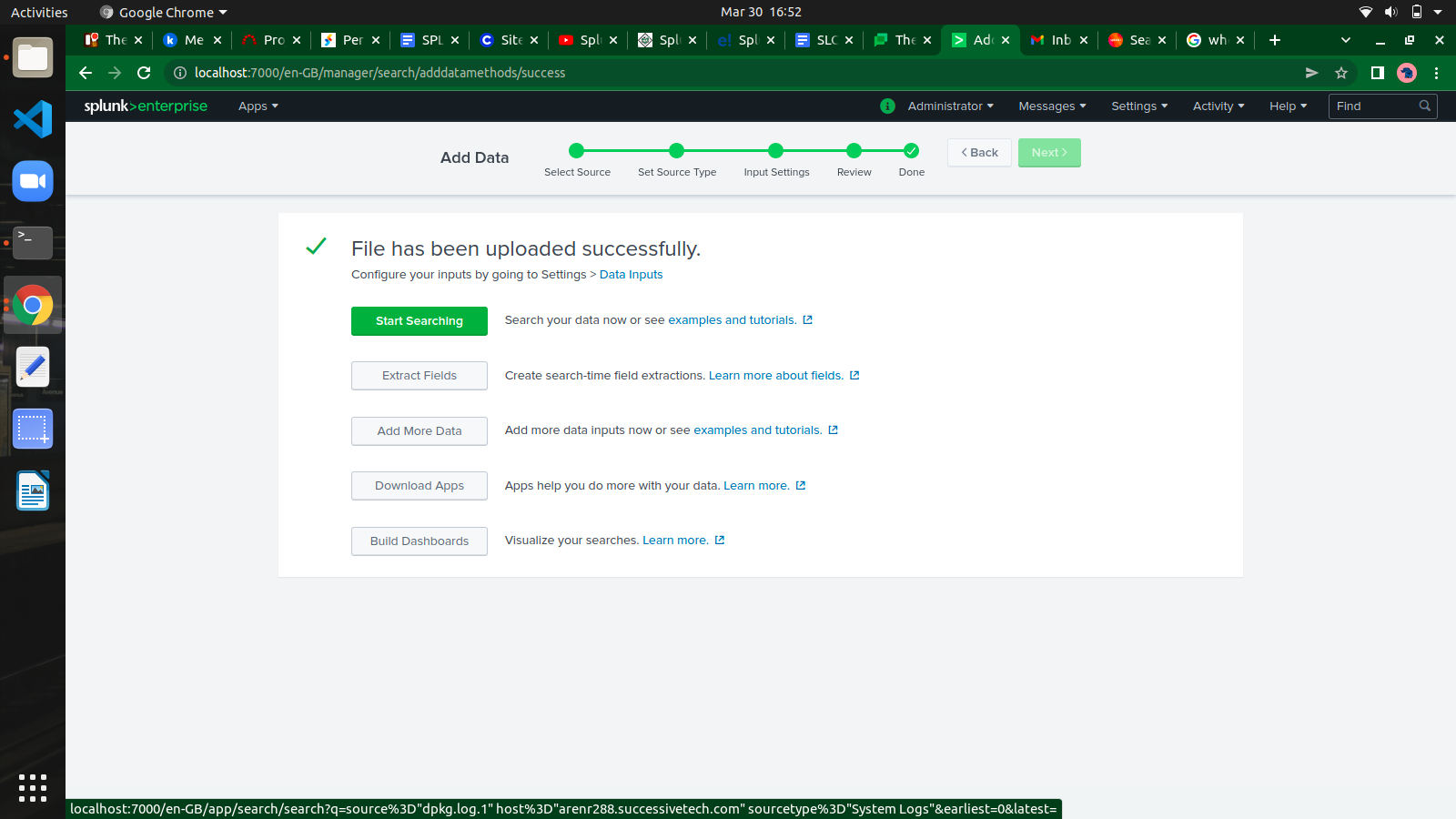


## **Review Settings**

After clicking on the next button, we see a summary of the settings we have chosen. We review it and choose Next to finish the uploading of data.



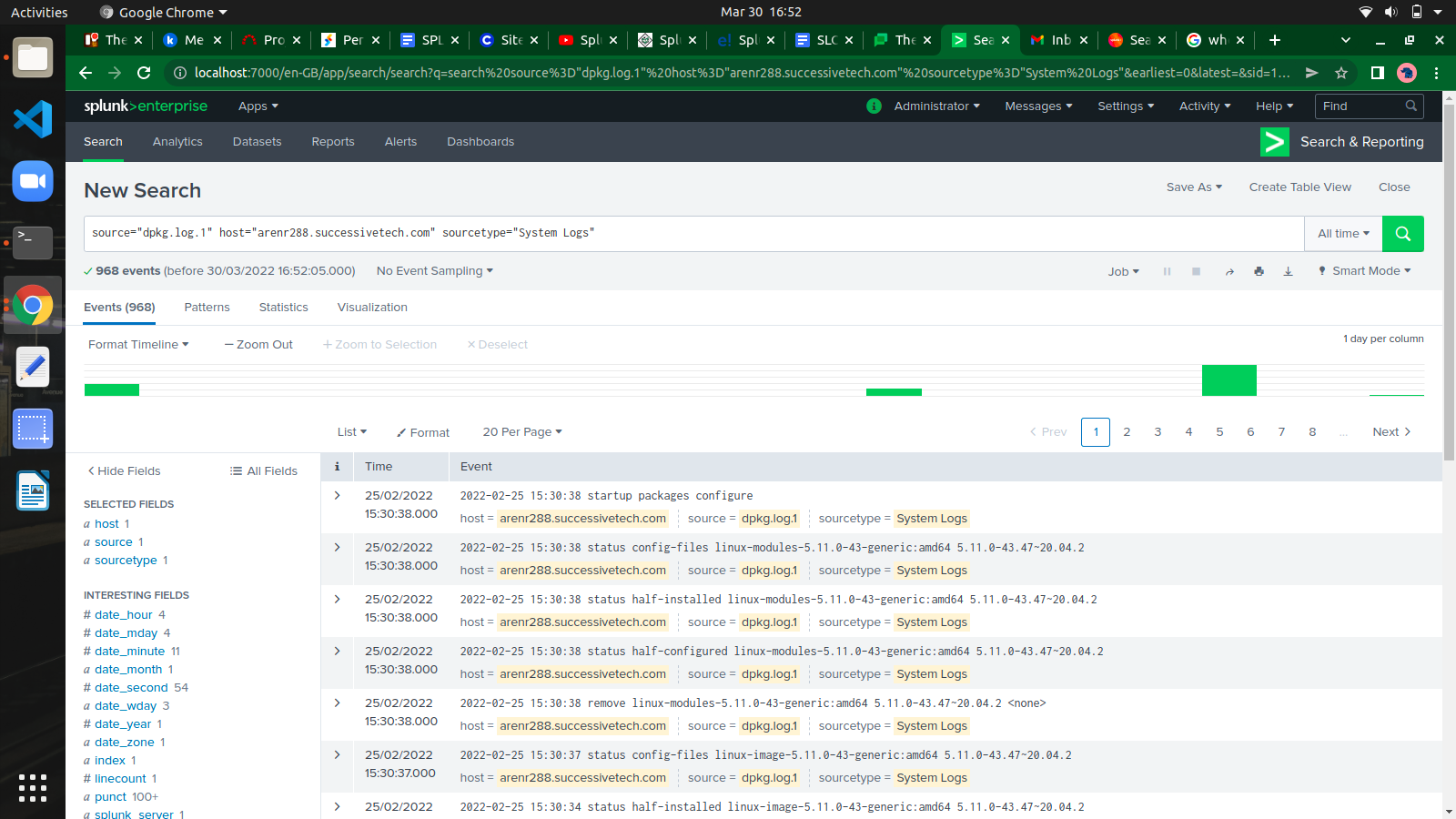
On finishing the load, the below screen appears which shows the successful data ingestion and further possible actions we can take on the data.



**Search And Reporting**

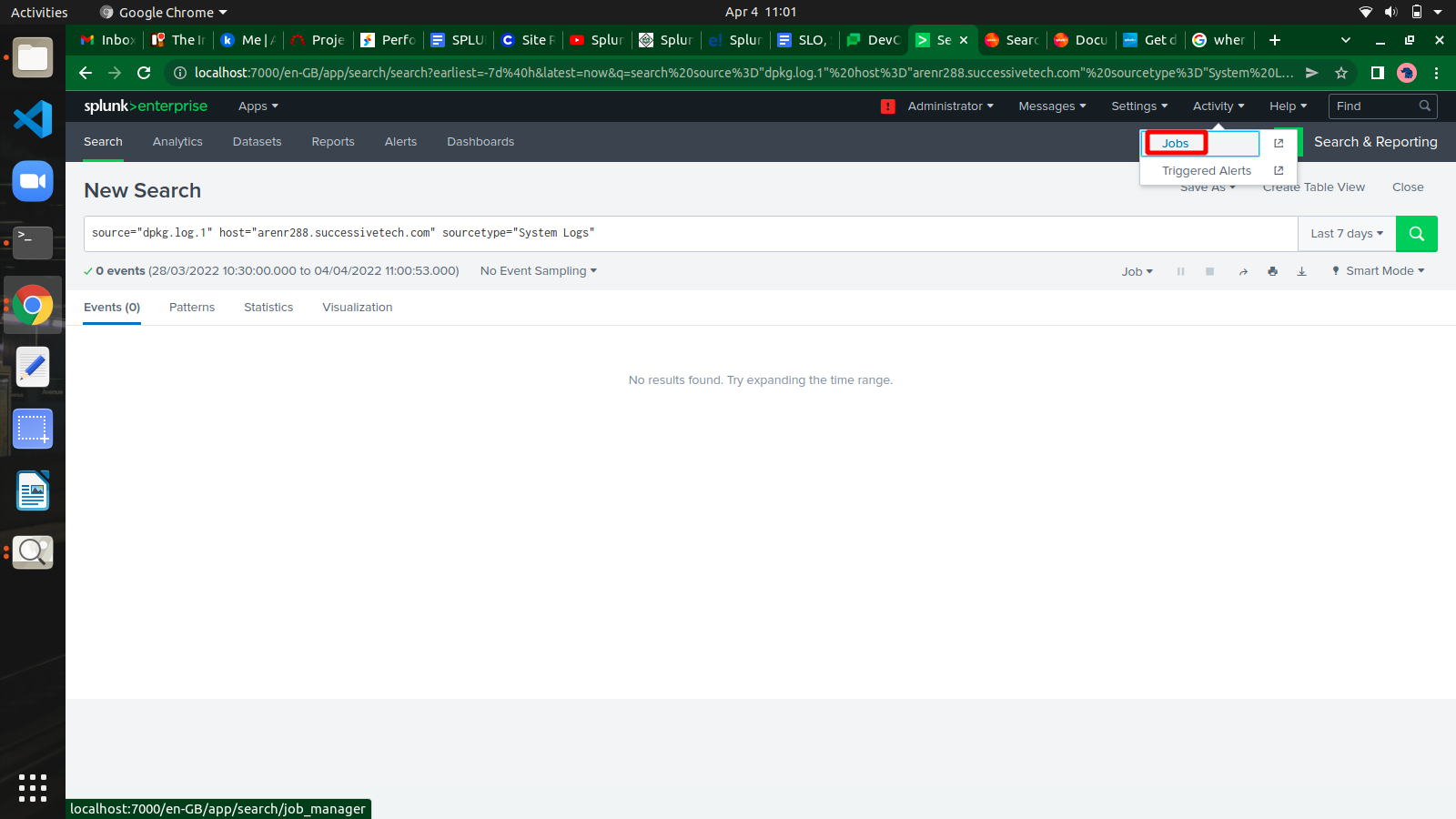
Splunk has a robust search functionality which enables you to search the entire data set that is ingested. This feature is accessed through the app named Search & Reporting.

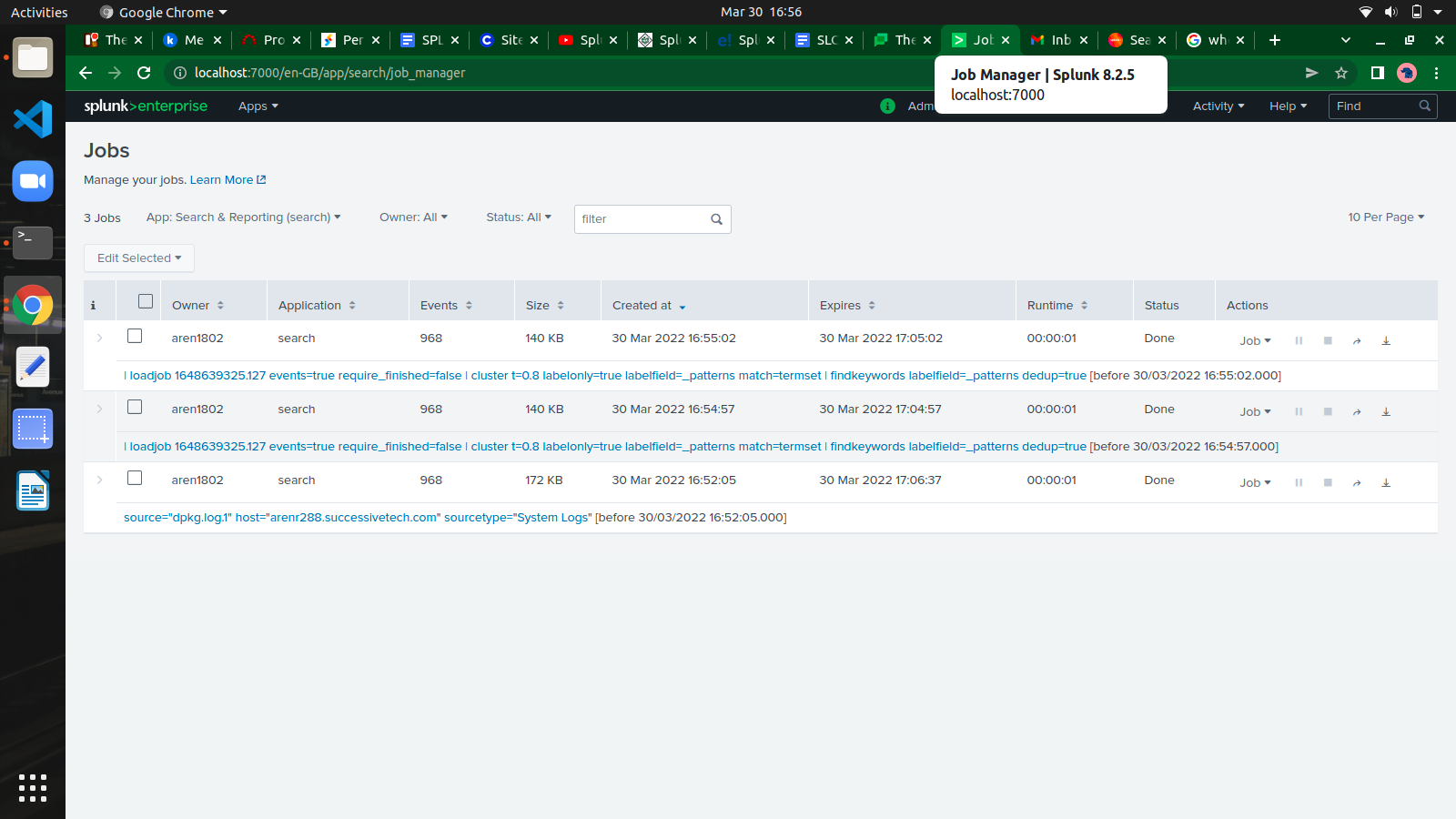
On clicking on the search & Reporting app, we are presented with a search box, where we can start our search on the log data that we uploaded.



**Jobs**

The jobs that are saved to be used by all users with appropriate permissions can be located by looking for the jobs link under the activity menu in the top right bar of the Splunk interface.



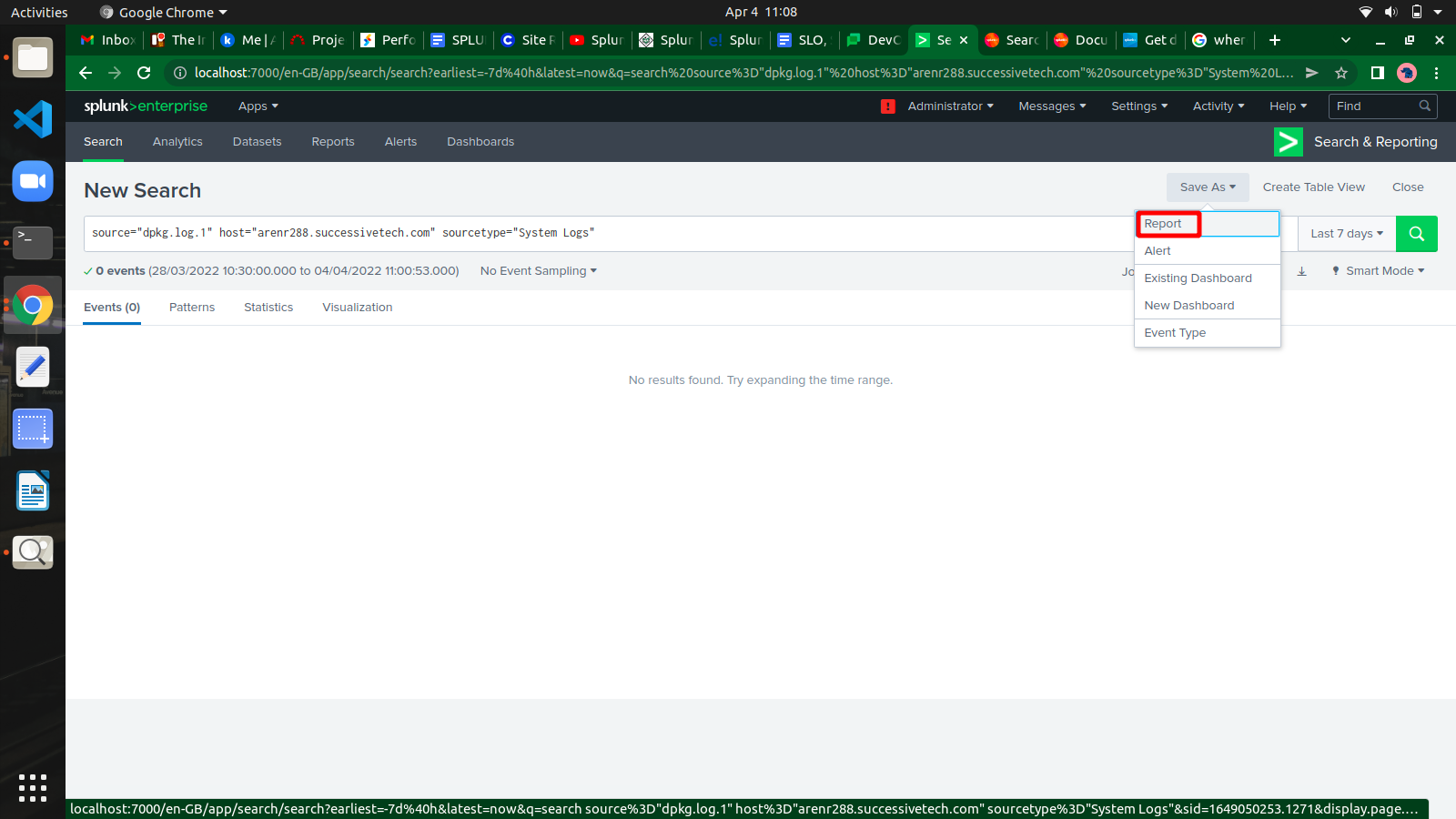


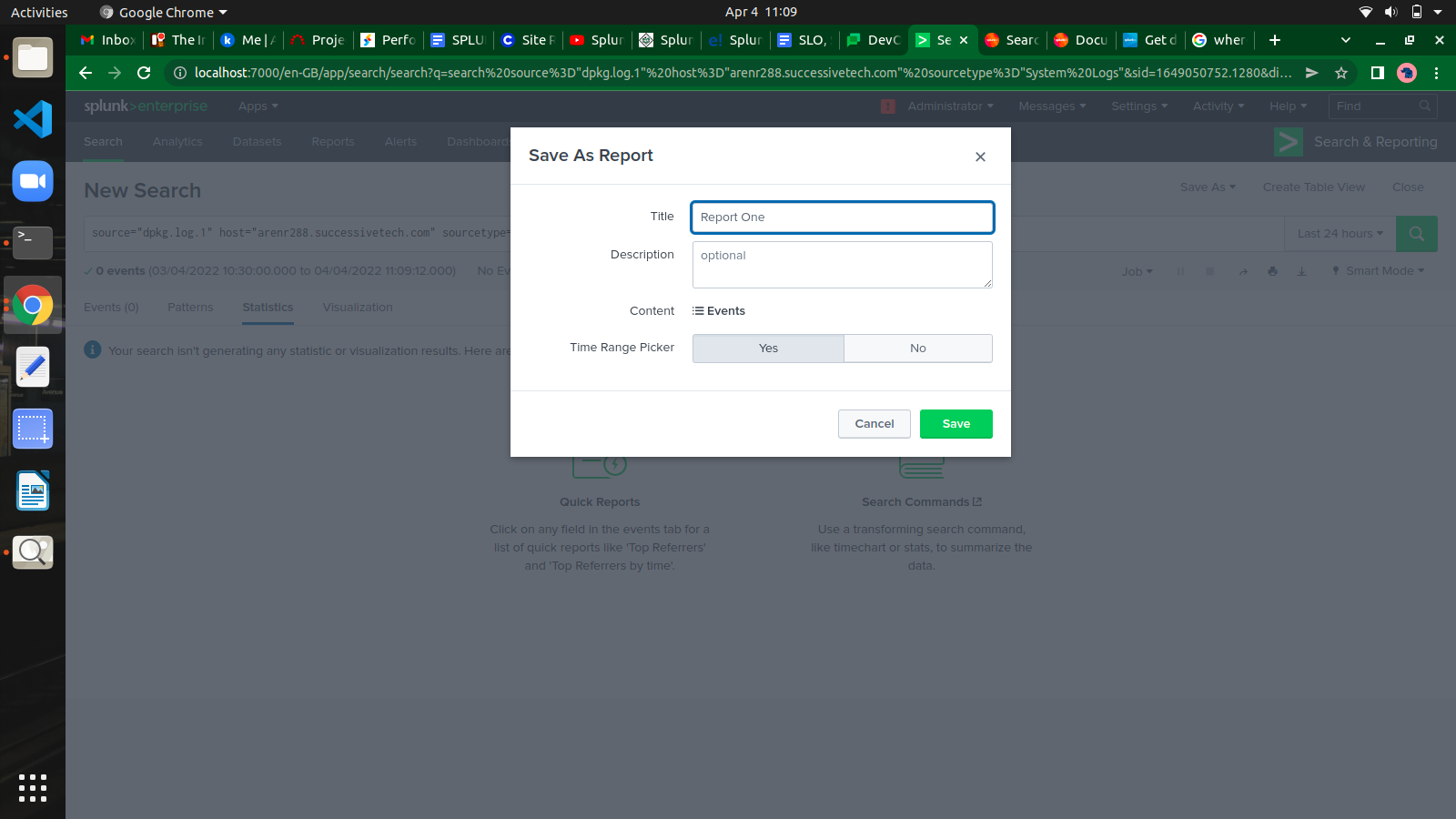
**Reports**

Splunk reports are results saved from a search action which can show statistics and visualizations of events. Reports can be run anytime, and they fetch fresh results each time they are run. The reports can be shared with other users and can be added to dashboards.

## **Report Creation**

Report creation is a straightforward process where we use the Save As option to save the result of a search operation.

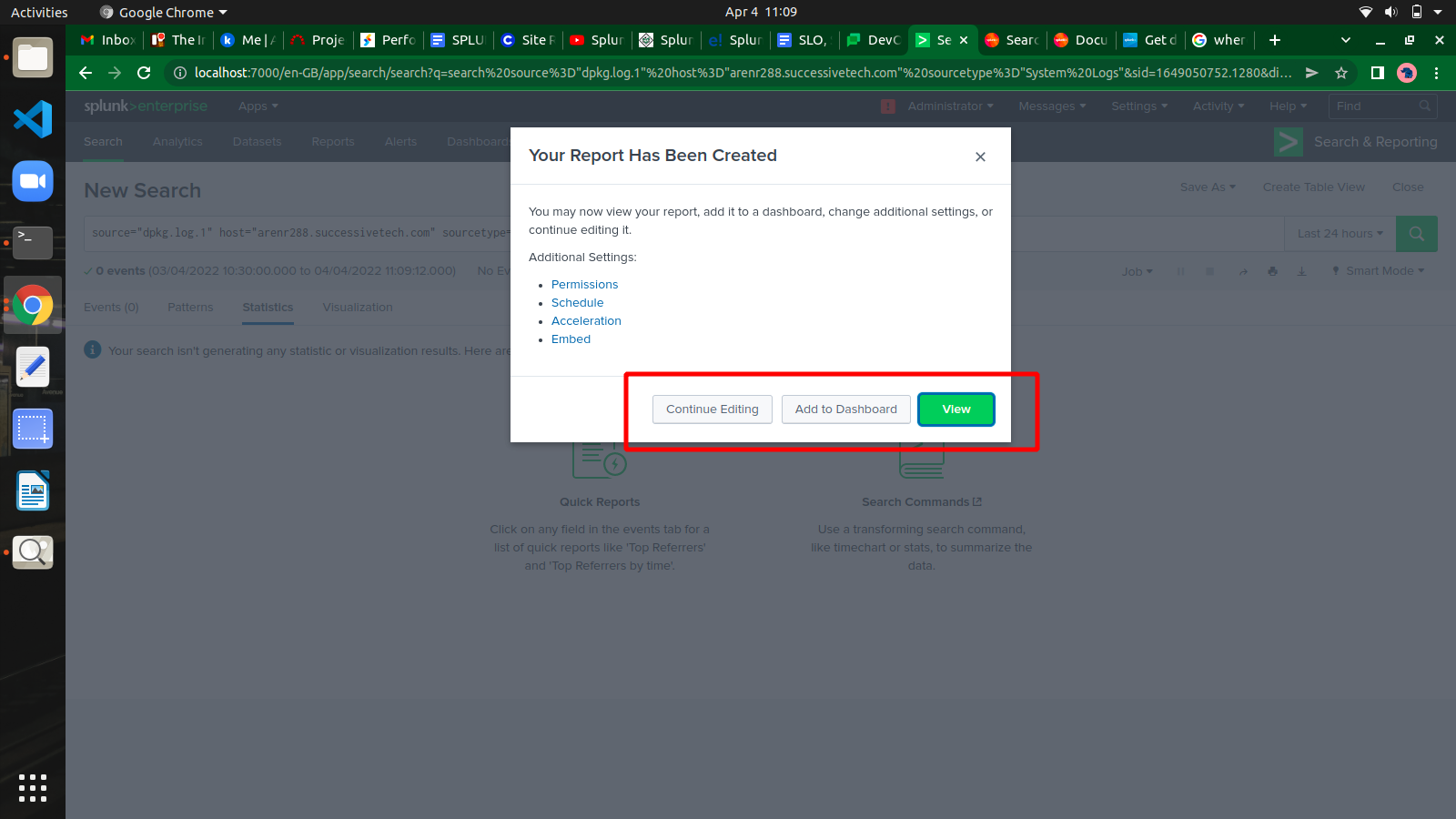




## **Report Configuration**

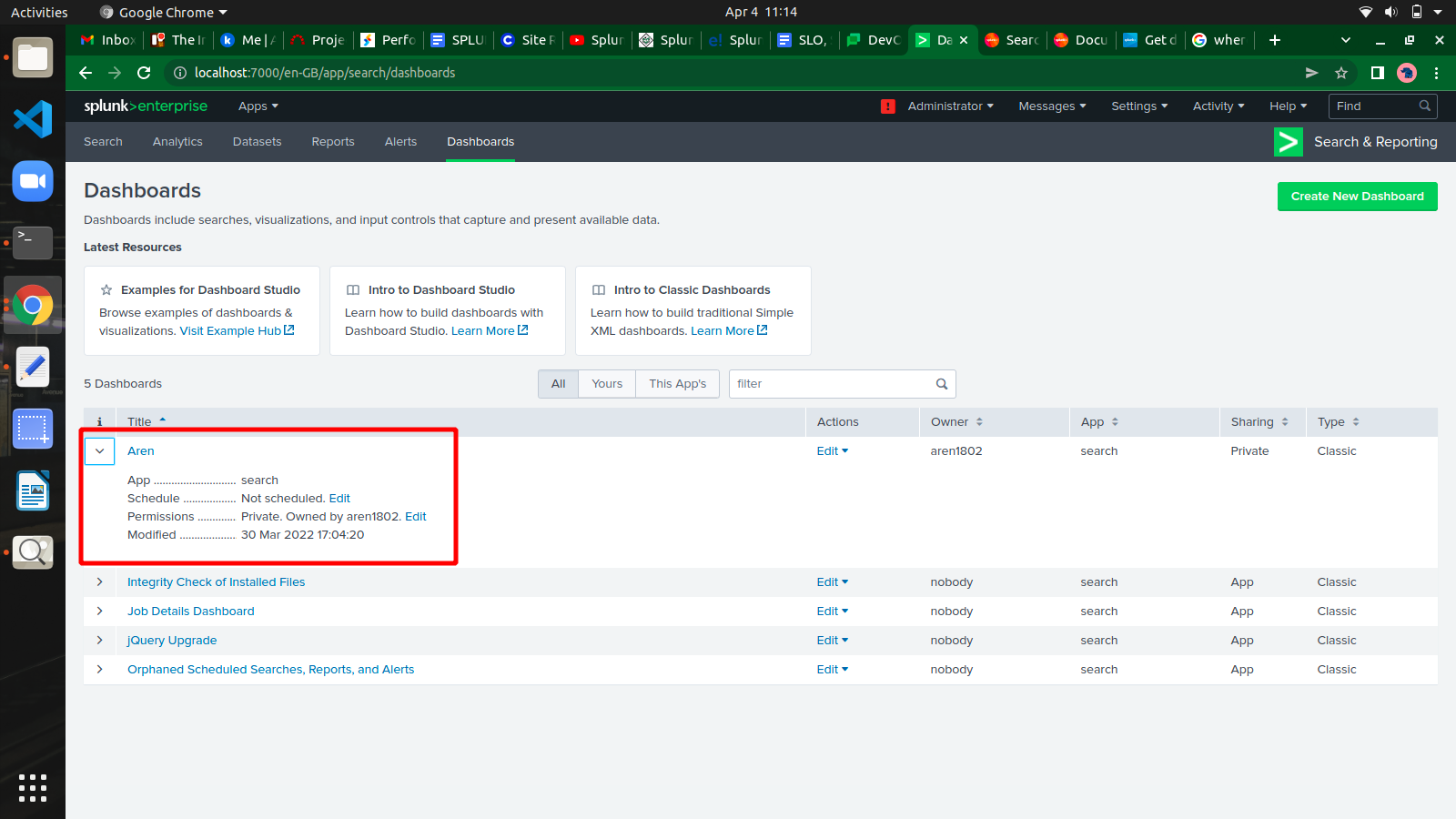
After clicking save to create the report in the above step, we get the next screen asking for configuring the report.

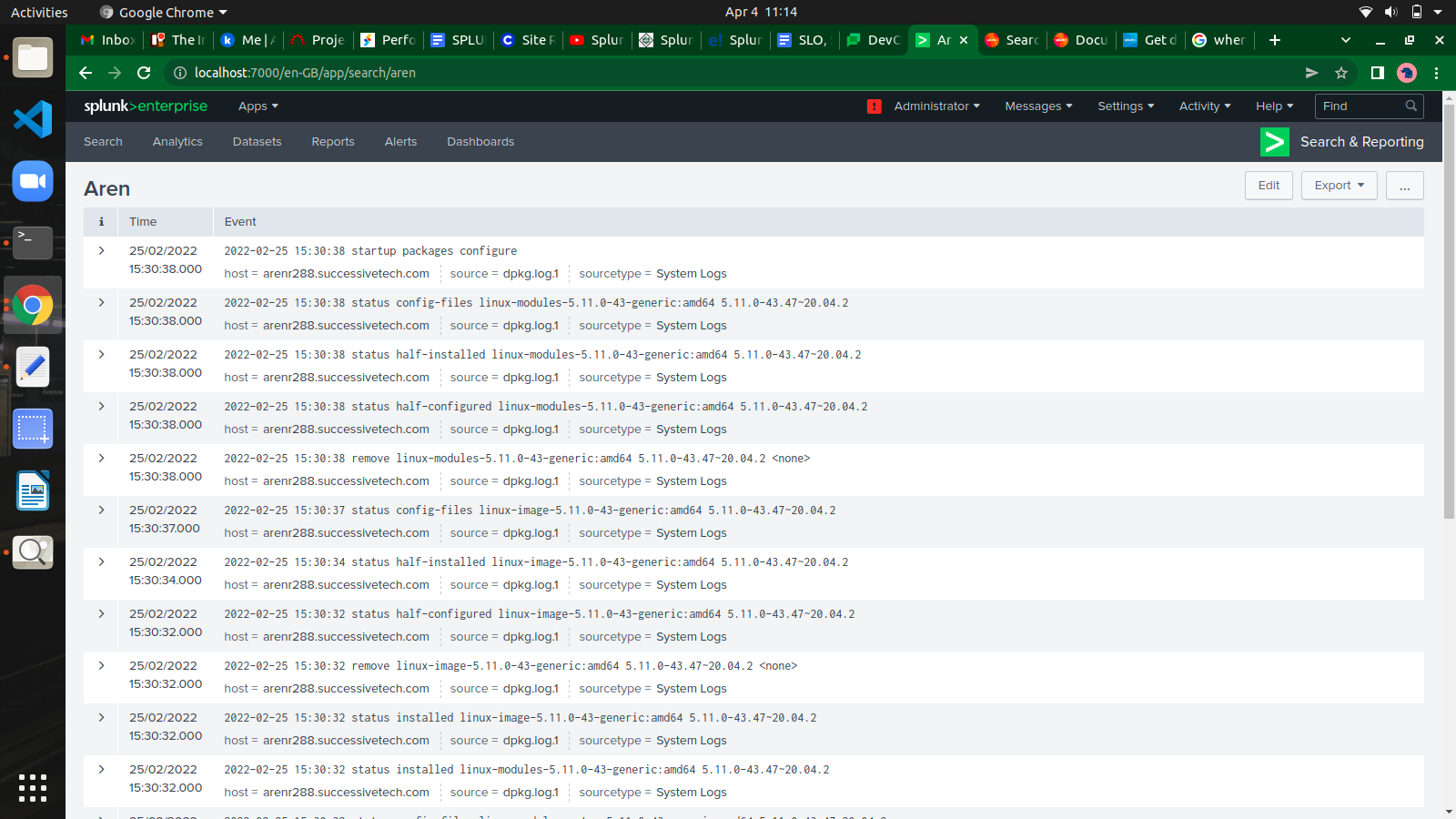
We also get an option to go to the next step and add the report to a dashboard.



**Dashboard**

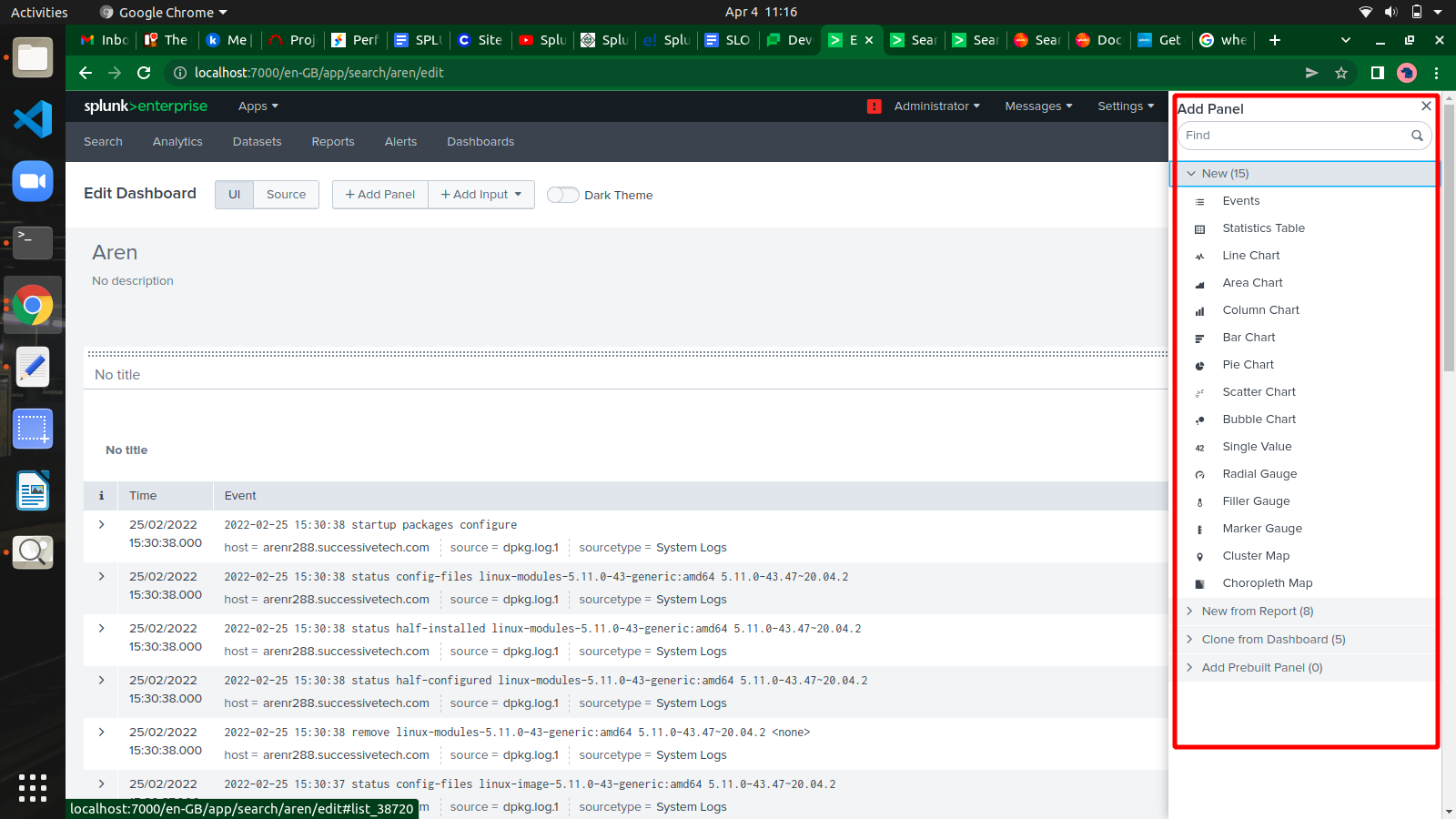
A dashboard is used to represent tables or charts which are related to some business meaning. It is done through panels. The panels in a dashboard hold the chart or summarized data in a visually appealing manner. We can add multiple panels, and hence multiple reports and charts to the same dashboard.





**Editing a Dashboard**

We can add panels to our dashboard i.e. statistics table, Pie chart, Area chart, Bar chart and many more.

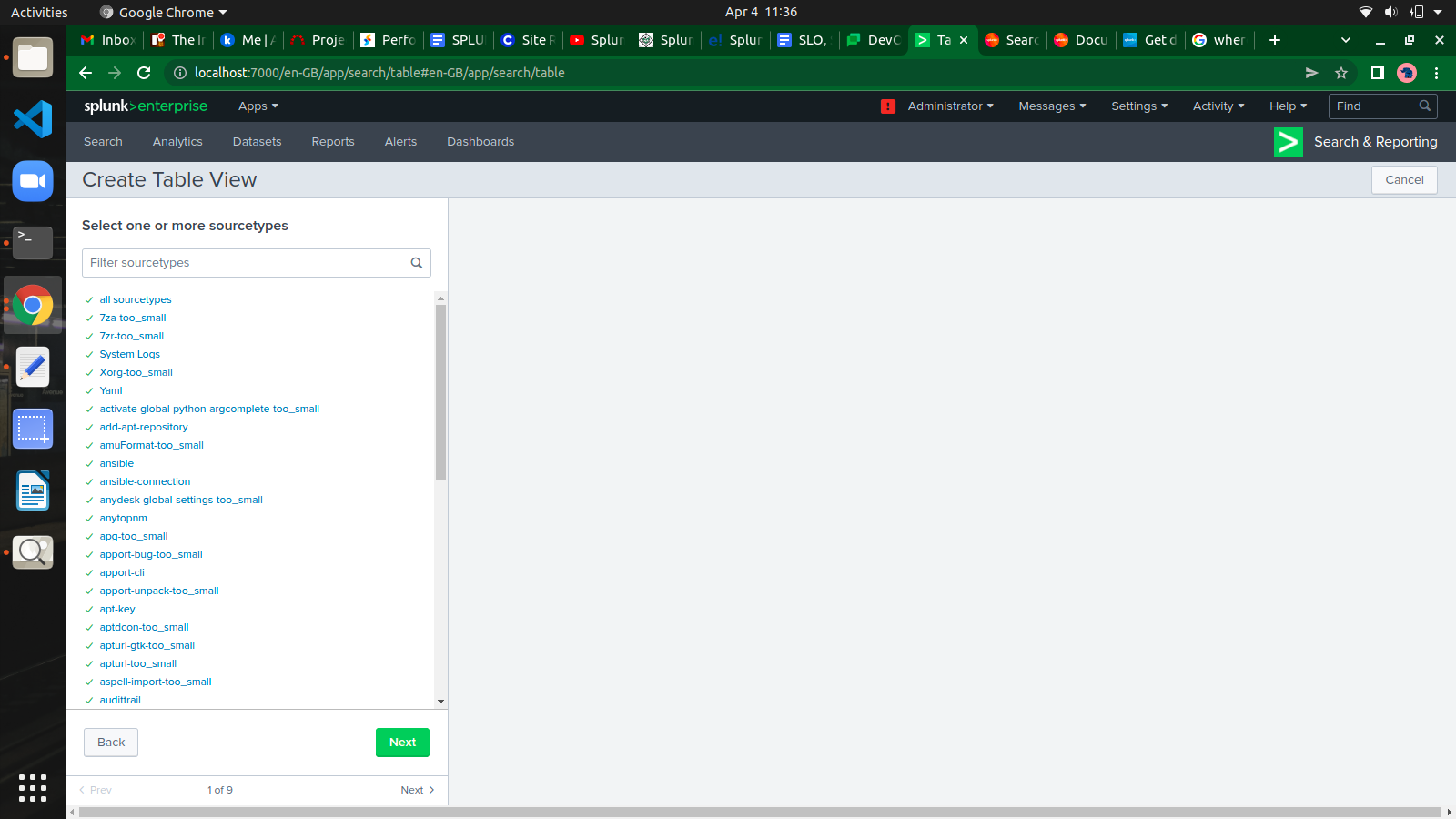


**Datasets**

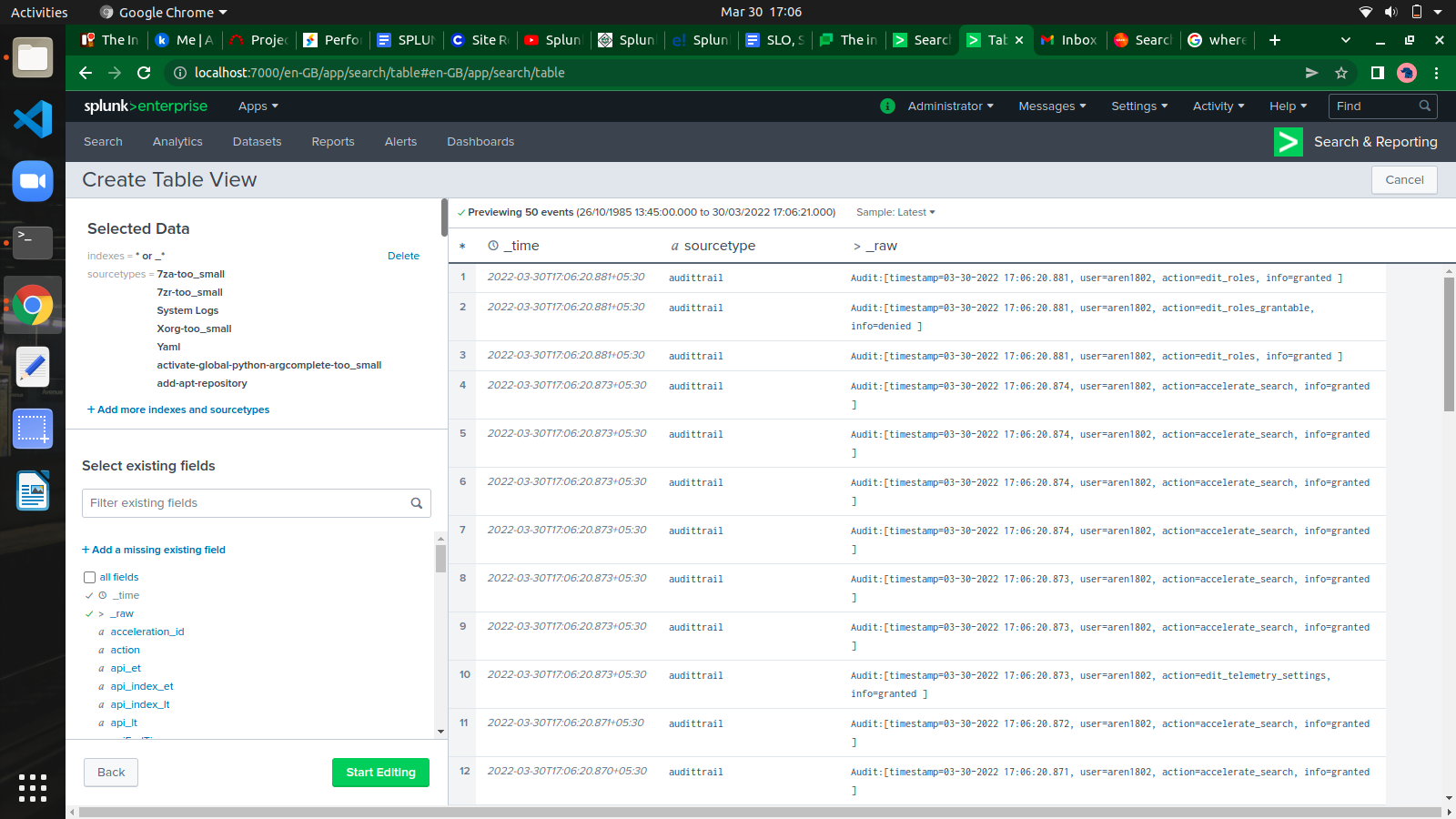
Splunk can ingest different types of data sources and build tables which are similar to relational tables. These are called table dataset or just tables. They provide easy ways to analyze and filter the data and lookups, etc.

## **Selecting a Dataset**

* **Indexes and Source Types** − Choose from an existing index or source type which are already added to Splunk through the Add Data app.
* **Existing Datasets** − You might have already created some dataset previously which you want to modify by creating a new dataset from it.
* **Search** − Write a search query and the result can be used to create a new dataset.



we get the final dataset table with all the selected fields, as seen below. Here the dataset has become similar to a relational table. We save the dataset with save as an option available in the top right corner.



**Alerts**

Splunk alerts are actions which get triggered when a specific criterion is met which is defined by the user. The goal of alerts can be logging an action, sending an email or output a result to a lookup file, etc.

### **Creating an Alert**

You create an alert by running a search query and saving its result as an alert. In the below screenshot, we take the search for day wise file count and save the result as an alert by choosing the Save As option.

