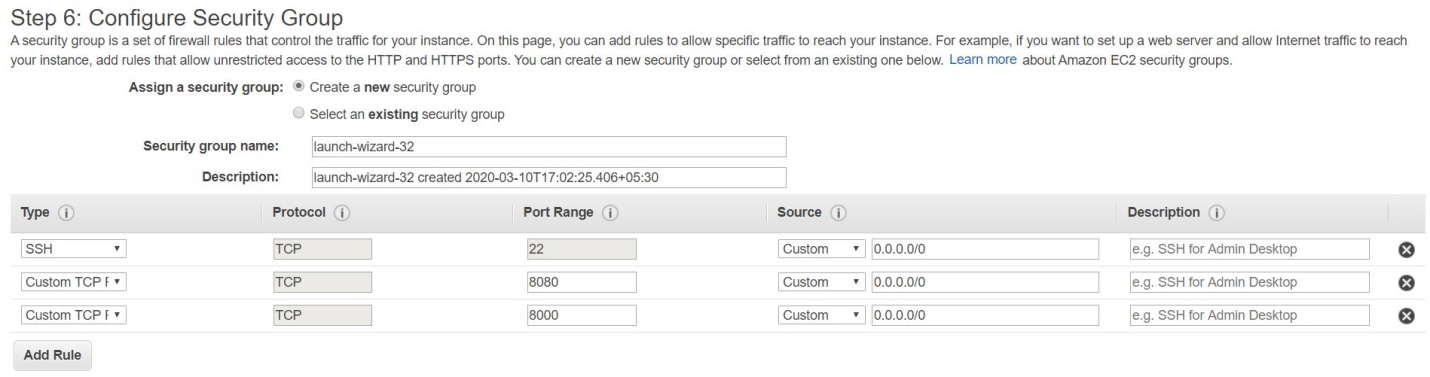
**How to forward your application logs to Splunk**

**Pre-Requisites:**

* Java
* Git
* Maven
* Docker
* Docker-Compose

Create instance with t2.xlarge and allow below port numbers



Clone our application from Git:

git clone <https://github.com/Naresh240/spring-boot-splunk.git>

Build artefact:

mvn clean install

Build docker image:

docker build -t naresh240/spring-boot-splunk .

Login to Docker-hub:

docker login -u naresh240 –p

Push docker image to docker-hub:

docker push naresh240/spring-boot-splunk

We need to create docker compose file to forward our application logs to Splunk:

vi docker-compose.yml

version: '2.1'

services:

demo-application:

image: naresh240/spring-boot-splunk

environment:

- LOGGING\_FILE=/logs/demo-application.log

ports:

- "8080:8080"

volumes:

- log\_volume:/logs

splunk:

image: splunk/splunk

hostname: splunk

environment:

- SPLUNK\_START\_ARGS=--accept-license

- SPLUNK\_USER=root

- SPLUNK\_PASSWORD=Naresh#240

- SPLUNK\_ENABLE\_LISTEN=9997

ports:

- "8000:8000"

splunkforwarder:

image: splunk/universalforwarder:6.5.3-monitor

hostname: splunkforwarder

environment:

- SPLUNK\_START\_ARGS=--accept-license --answer-yes

- SPLUNK\_FORWARD\_SERVER=splunk:9997

- SPLUNK\_USER=root

- SPLUNK\_PASSWORD=Naresh#240

- SPLUNK\_ADD=monitor /logs

restart: always

depends\_on:

- splunk

volumes:

- log\_volume:/logs

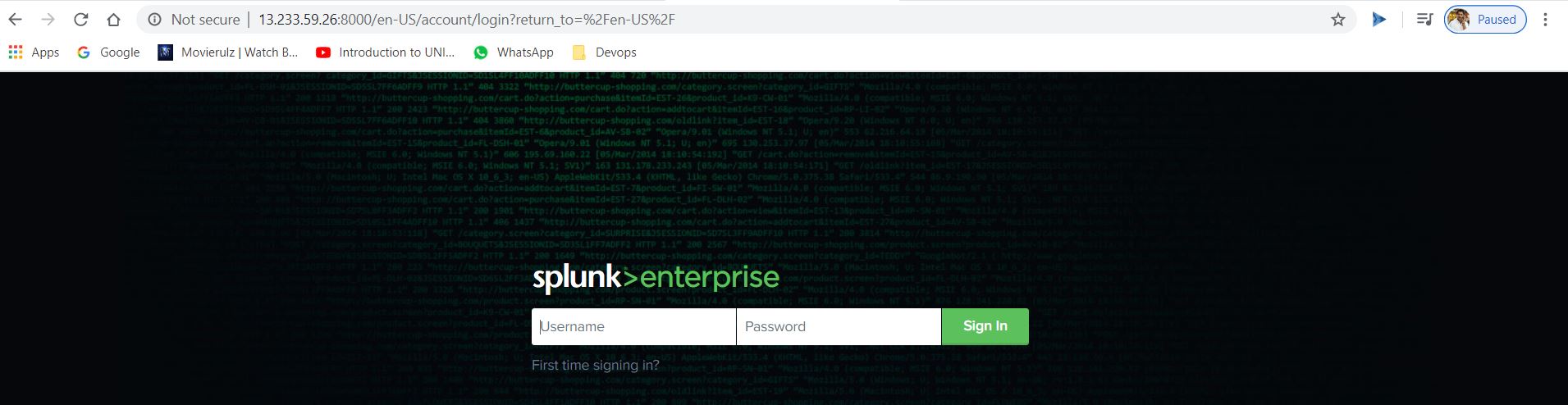
volumes:

log\_volume:

Now our application:

docker-compose up

Now open Splunk in UI:

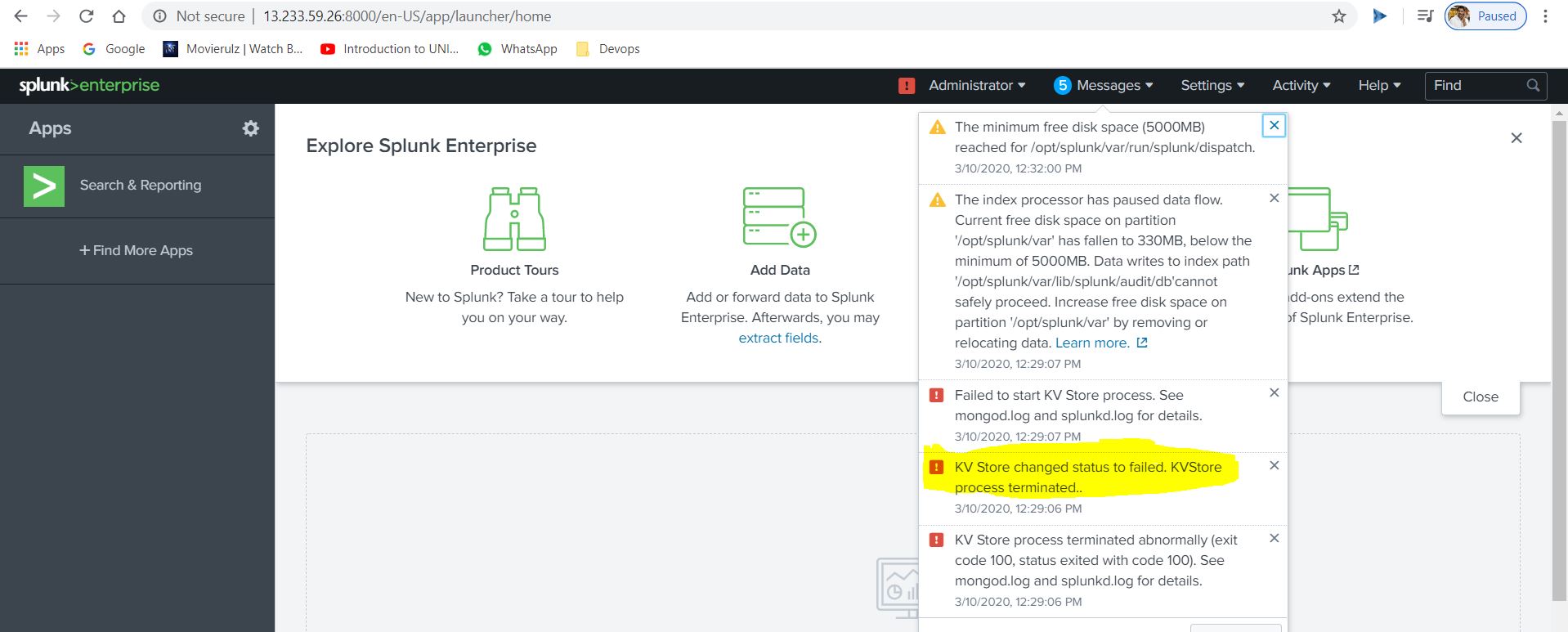


Give user name and password:

Username: admin

Password: Naresh#240

(Here I given this in docker composefile)

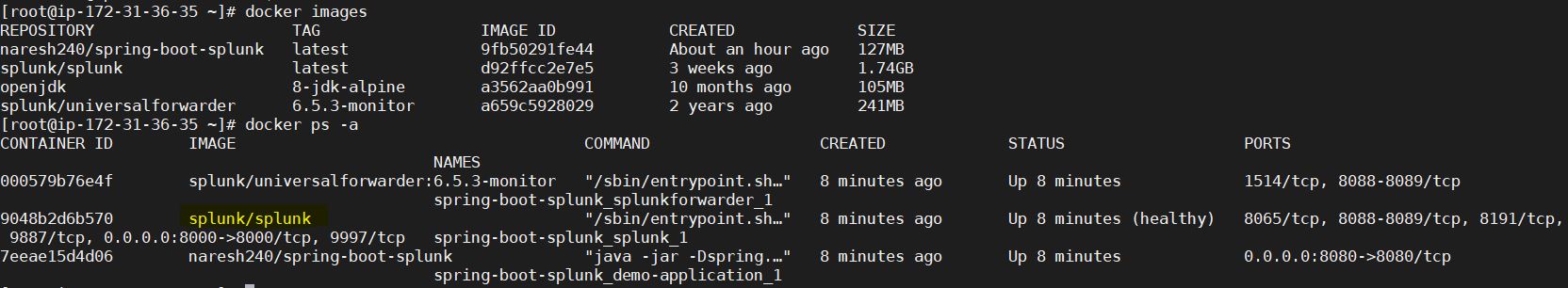


Here we get some error like **KV Store changed status to failed. KVStore process terminated..**

For this we need to give DiskSpace in **/opt/splunk/etc/system/local/server.conf** file

docker images

docker ps -a

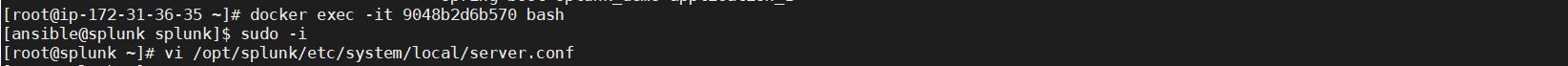


For this first we need to login into Splunk container

docker exec -it 9048b2d6b570 bash

sudo -i

vi /opt/splunk/etc/system/local/server.conf



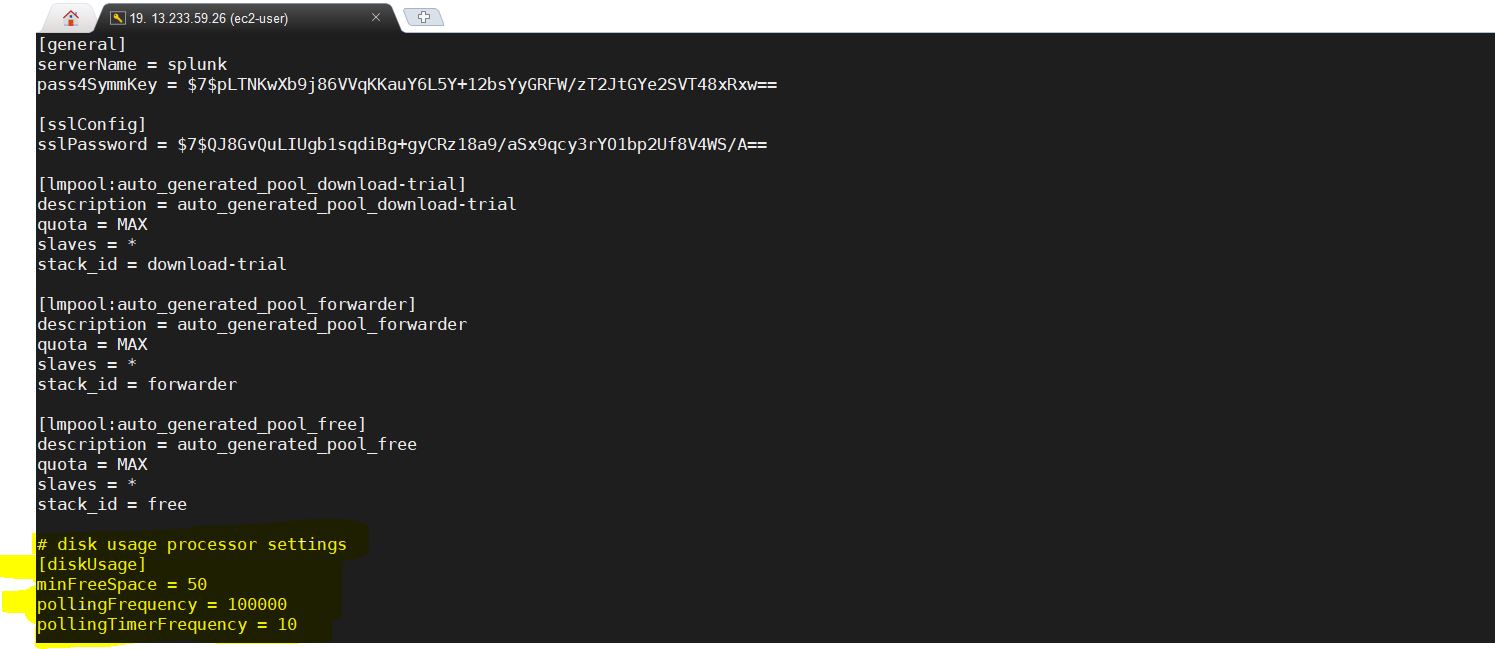
# disk usage processor settings

[diskUsage]

minFreeSpace = 50

pollingFrequency = 100000

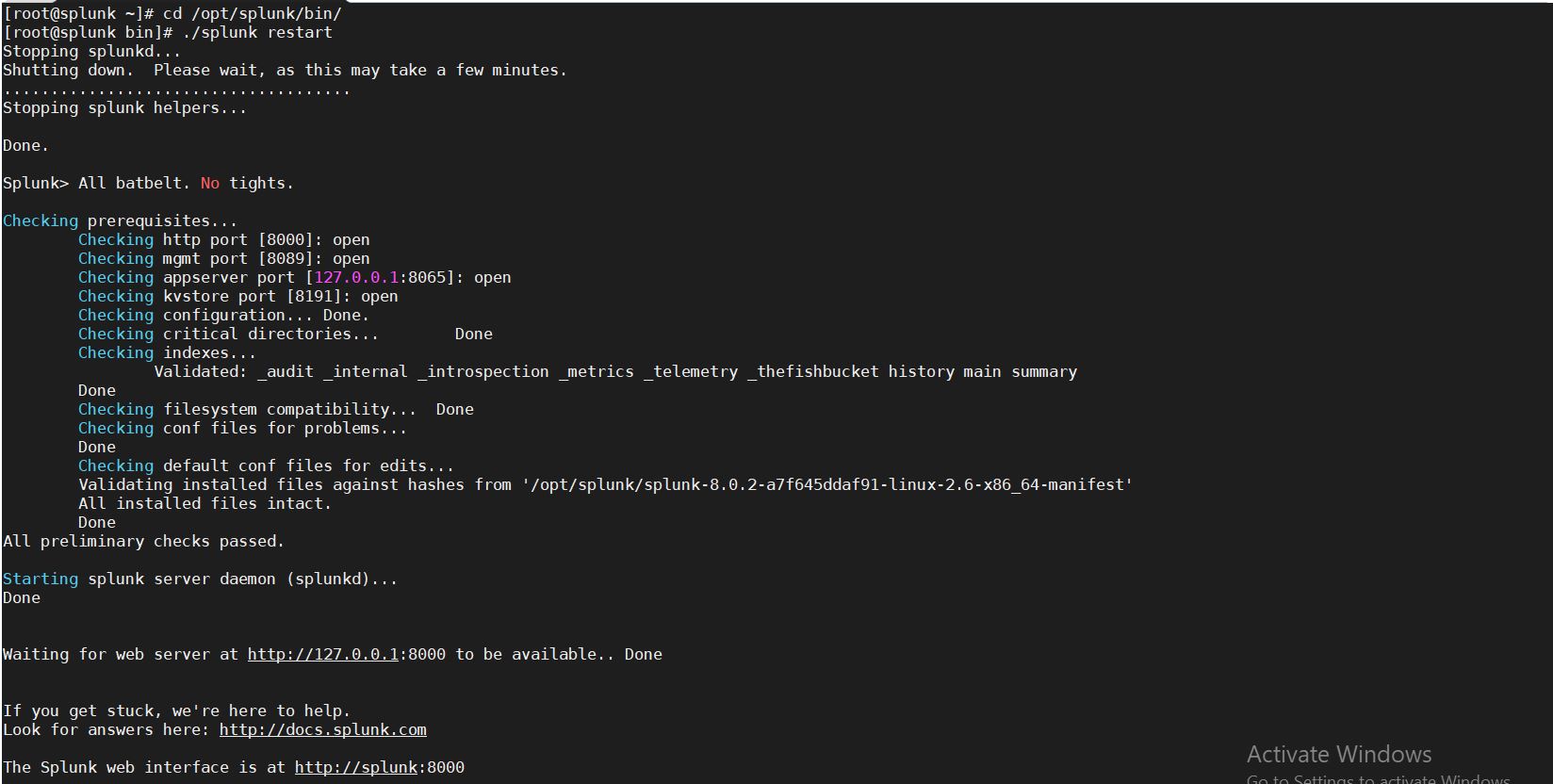
pollingTimerFrequency = 10



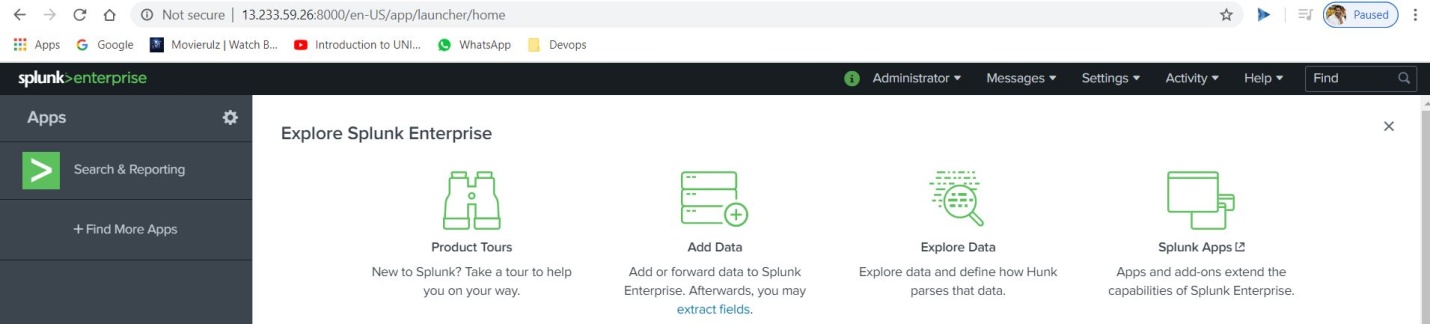
Now Restart Splunk:

cd /opt/splunk/bin/

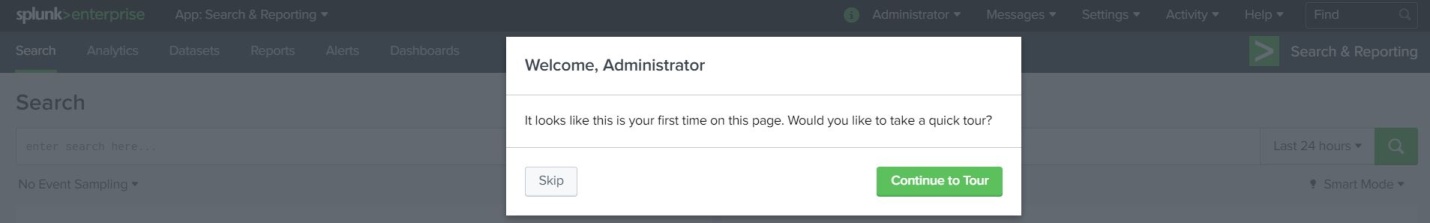
./splunk restart



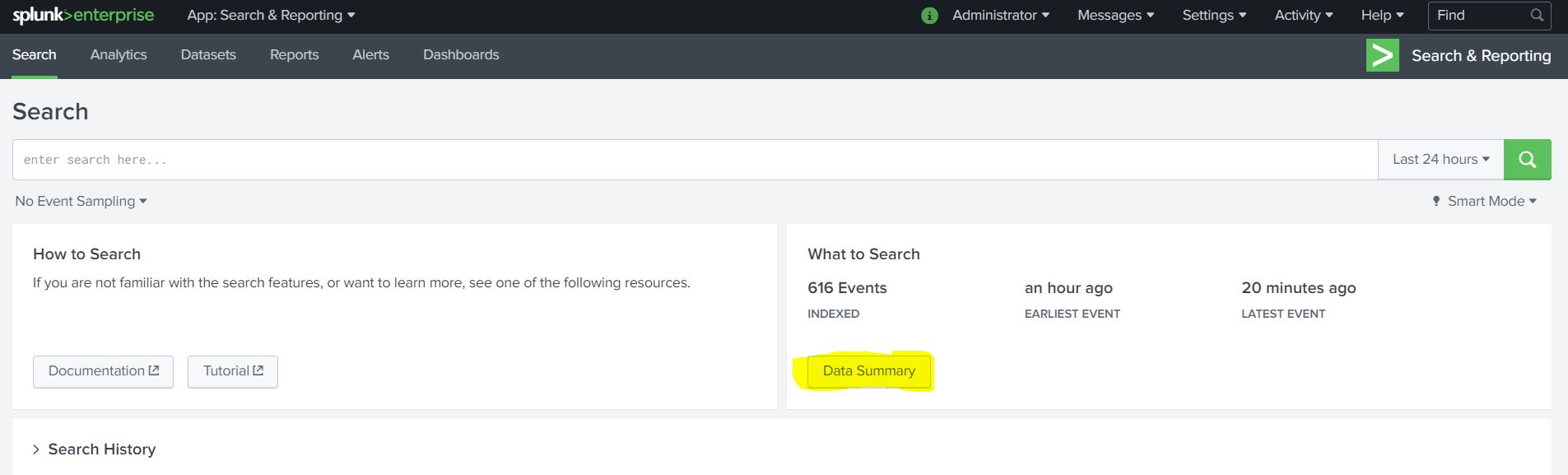
Open UI and check whether the error is there or not:



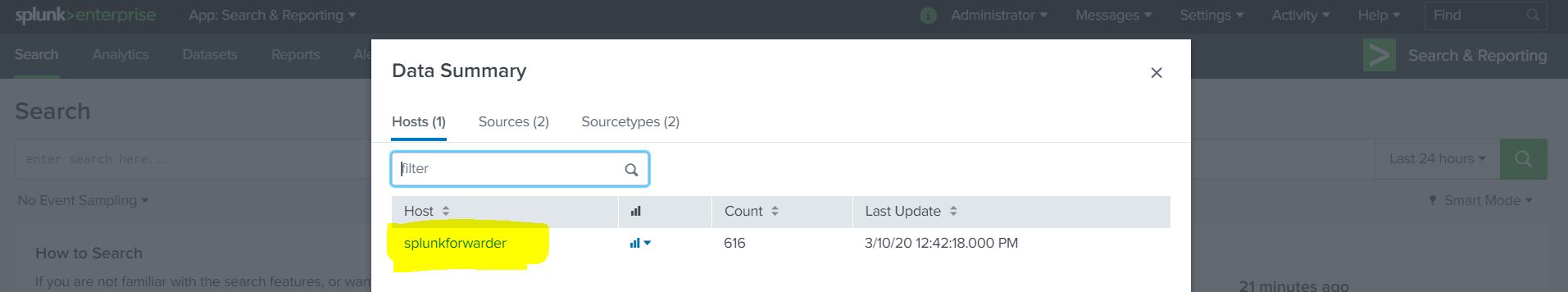
Click on Search & Reporting



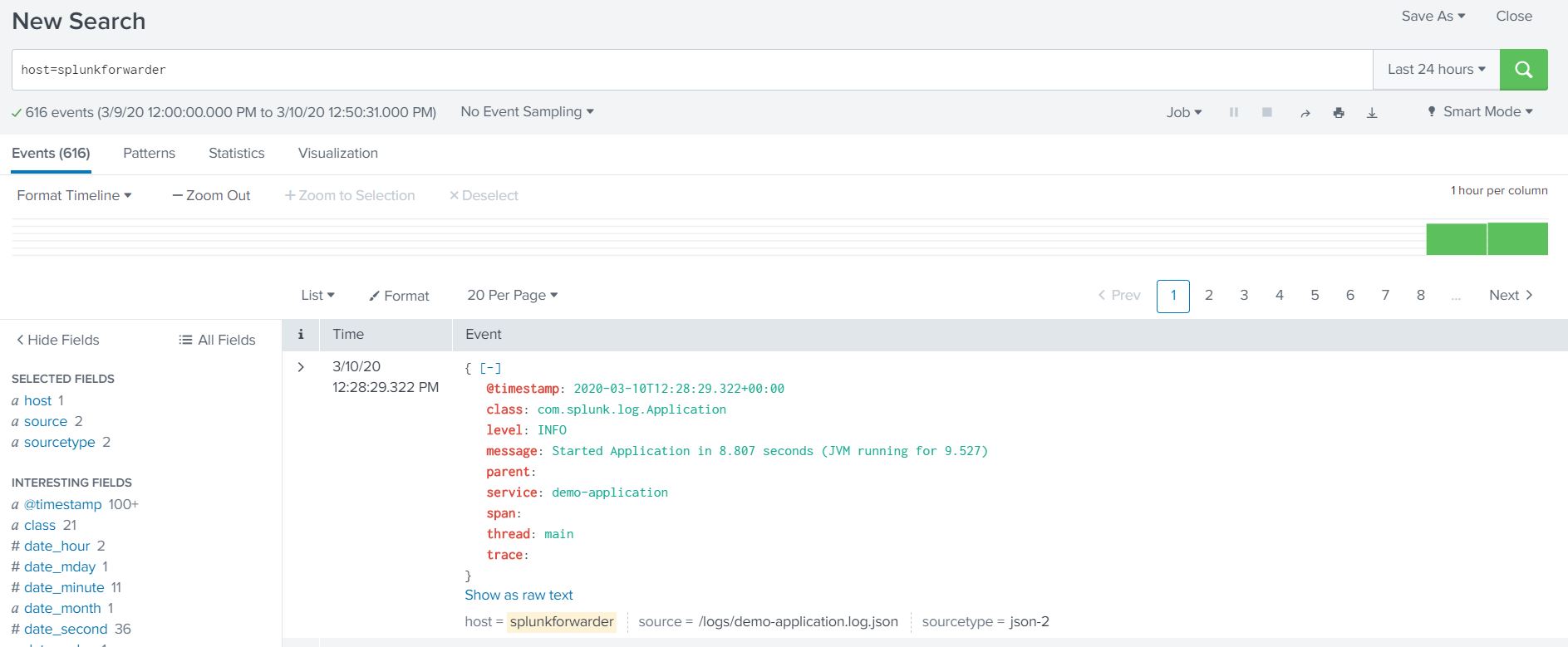
Ckick on Skip



Click on Data Summary



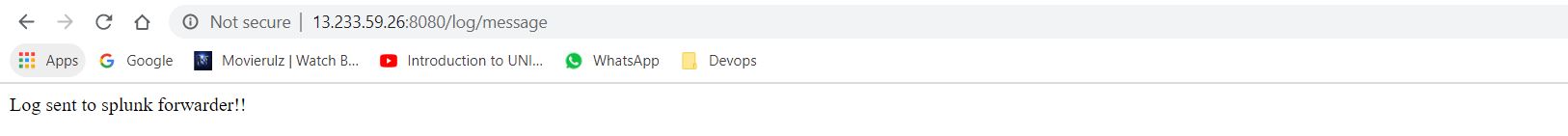
Click on Splunkforwarder



Now got Web UI and give URL:

<http://13.233.59.26:8080/log/message>

<ip-address>:8080/log/message



Now check log message in Splunk in web UI:

