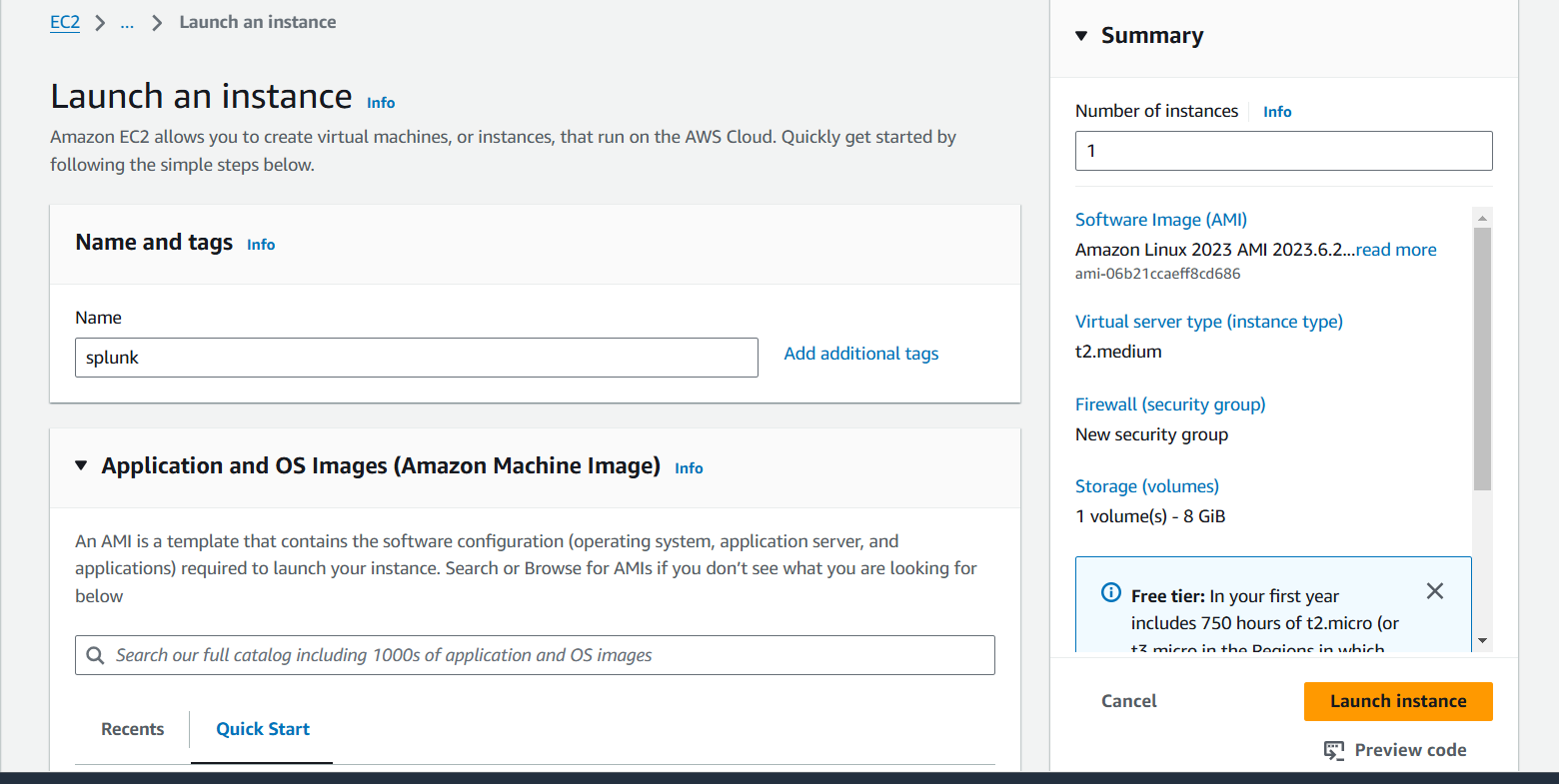
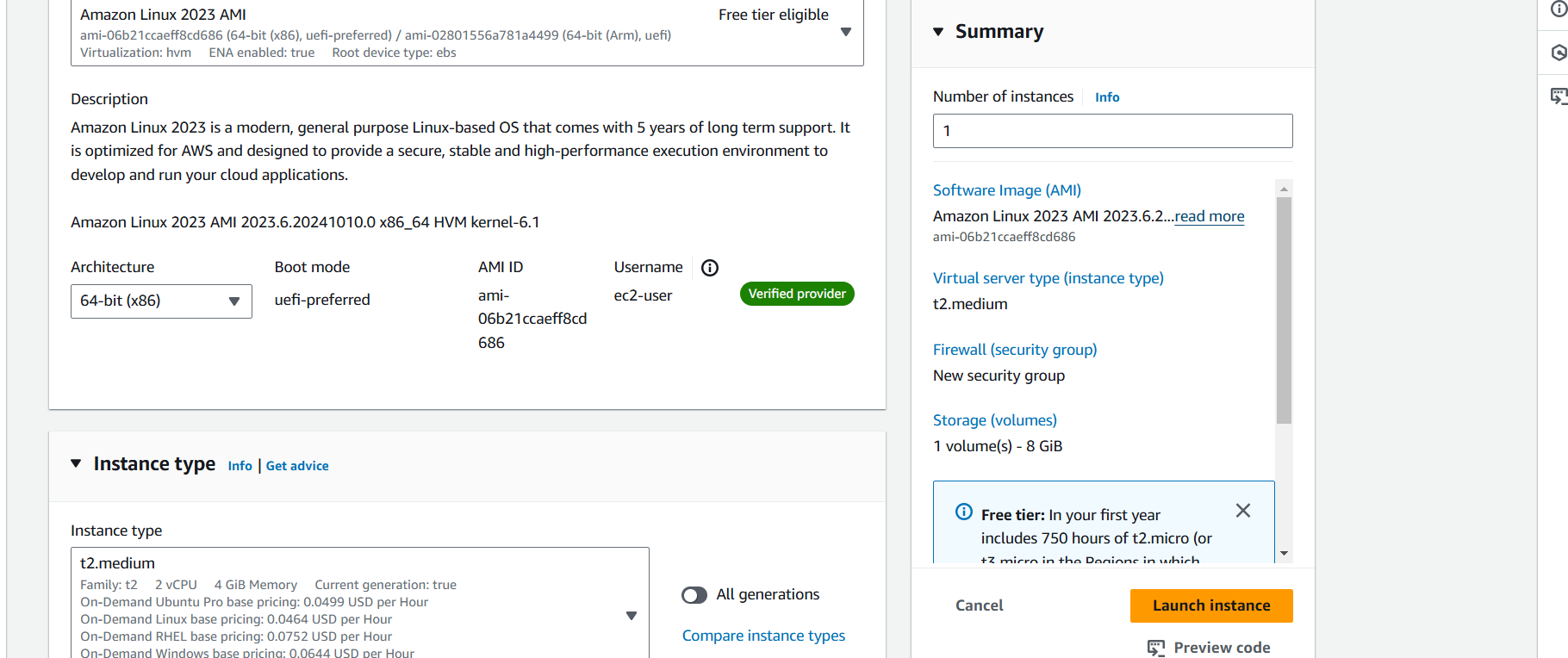
SPLUNK LOGS

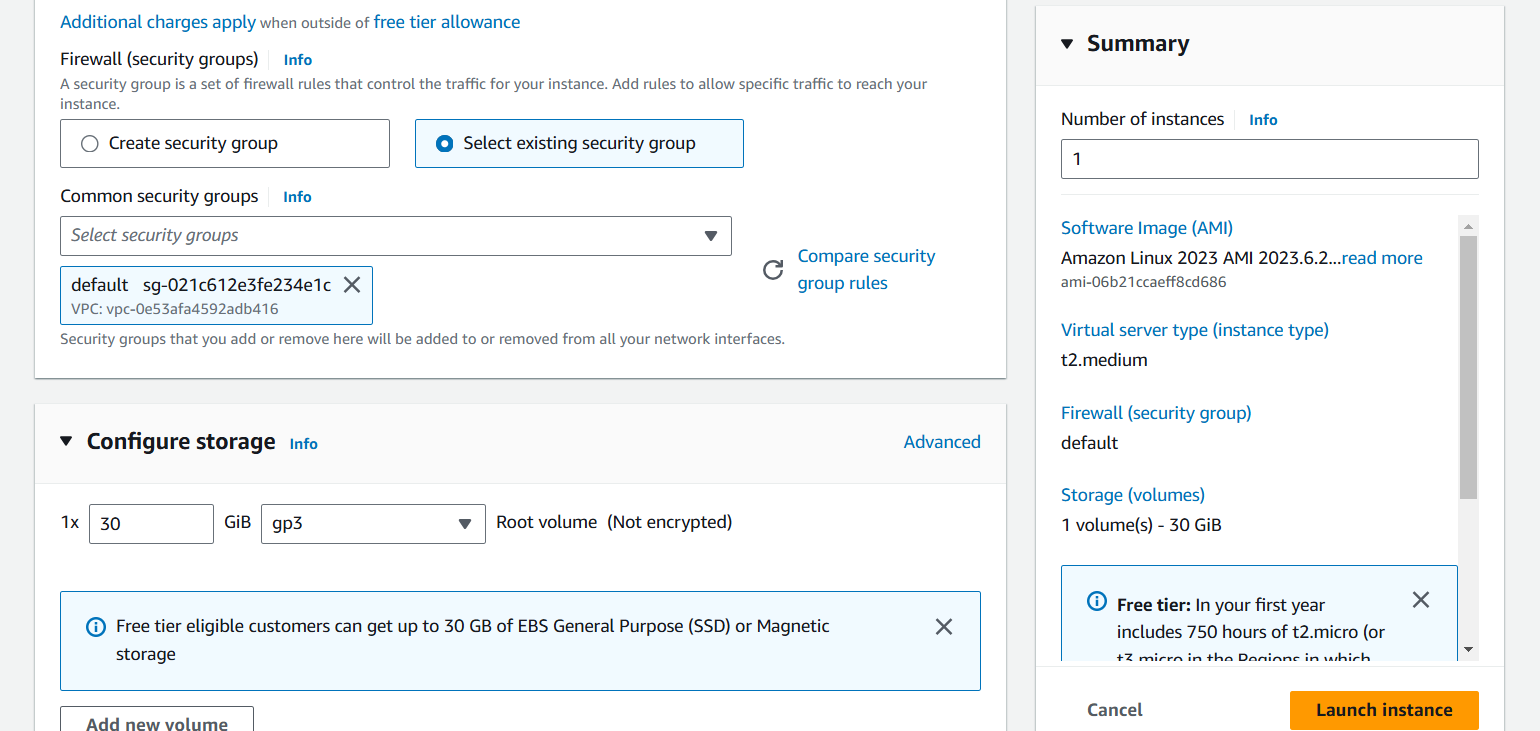
Create ec2 with below specifications



* Instance type is t2.medium

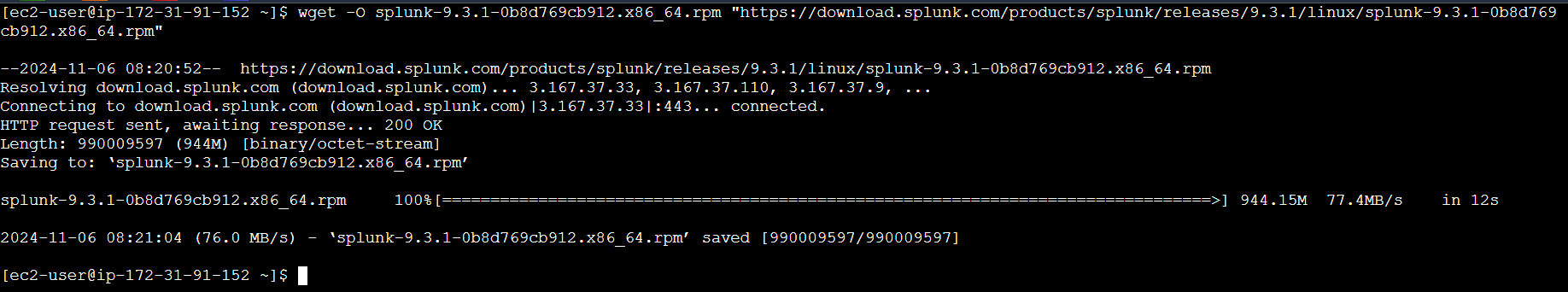


* Select sg and allow all traffic
* Take ebs volume 30gb



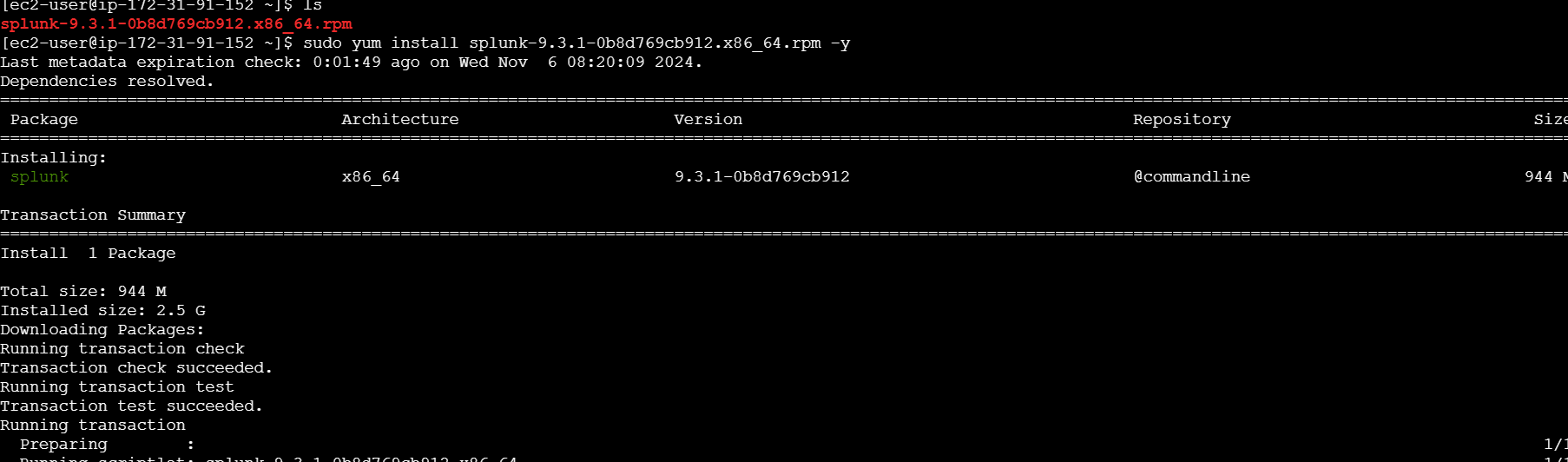
* Connect to instance install splunk

wget -O splunk-9.3.1-0b8d769cb912.x86\_64.rpm "https://download.splunk.com/products/splunk/releases/9.3.1/linux/splunk-9.3.1-0b8d769cb912.x86\_64.rpm"



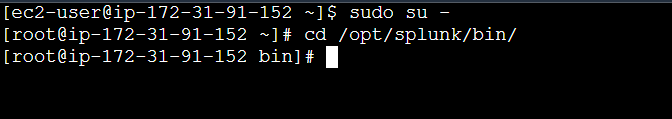
* Install downloaded rpm package

sudo yum install splunk-9.3.1-0b8d769cb912.x86\_64.rpm -y



* Switch to root user then go to splunk bin directory

cd /opt/splunk/bin/



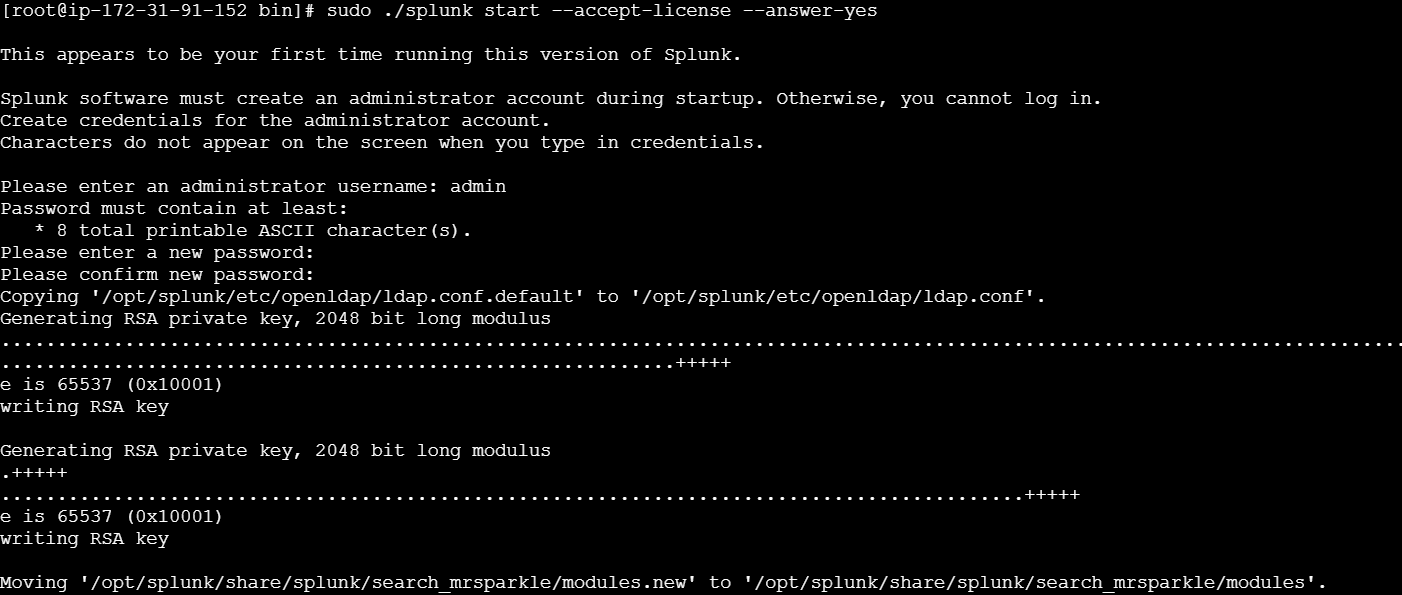
* Strat the splunk

sudo ./splunk start --accept-license --answer-yes

* It will ask usename password

Username :admin

Password : admin1234 [give your custom password]

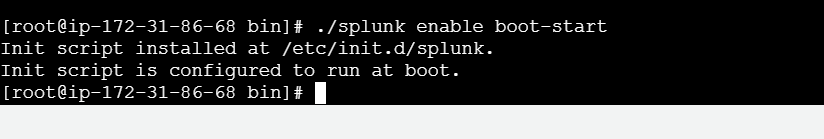


* Successfully started the splunk

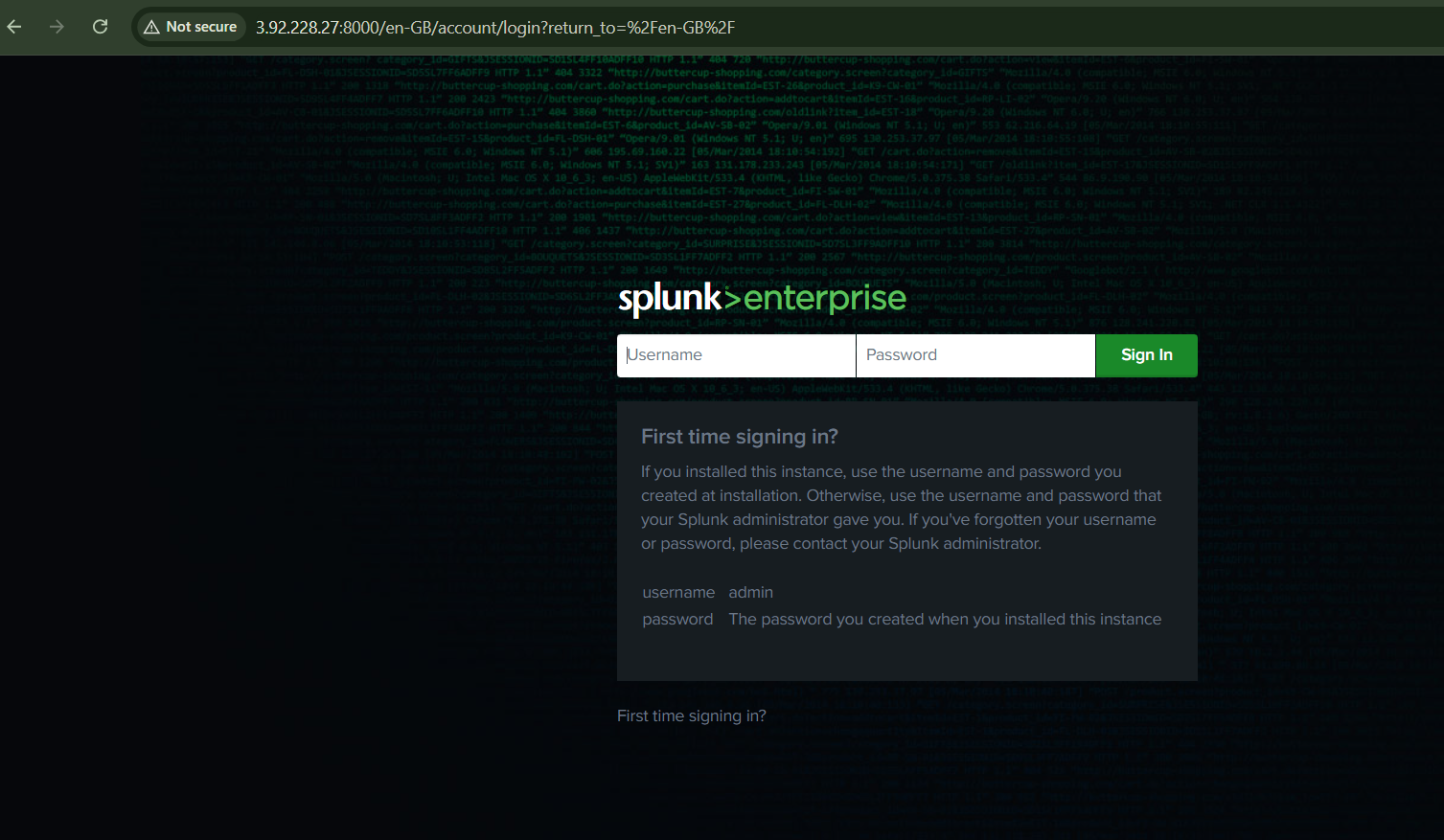


* Enable the splunk

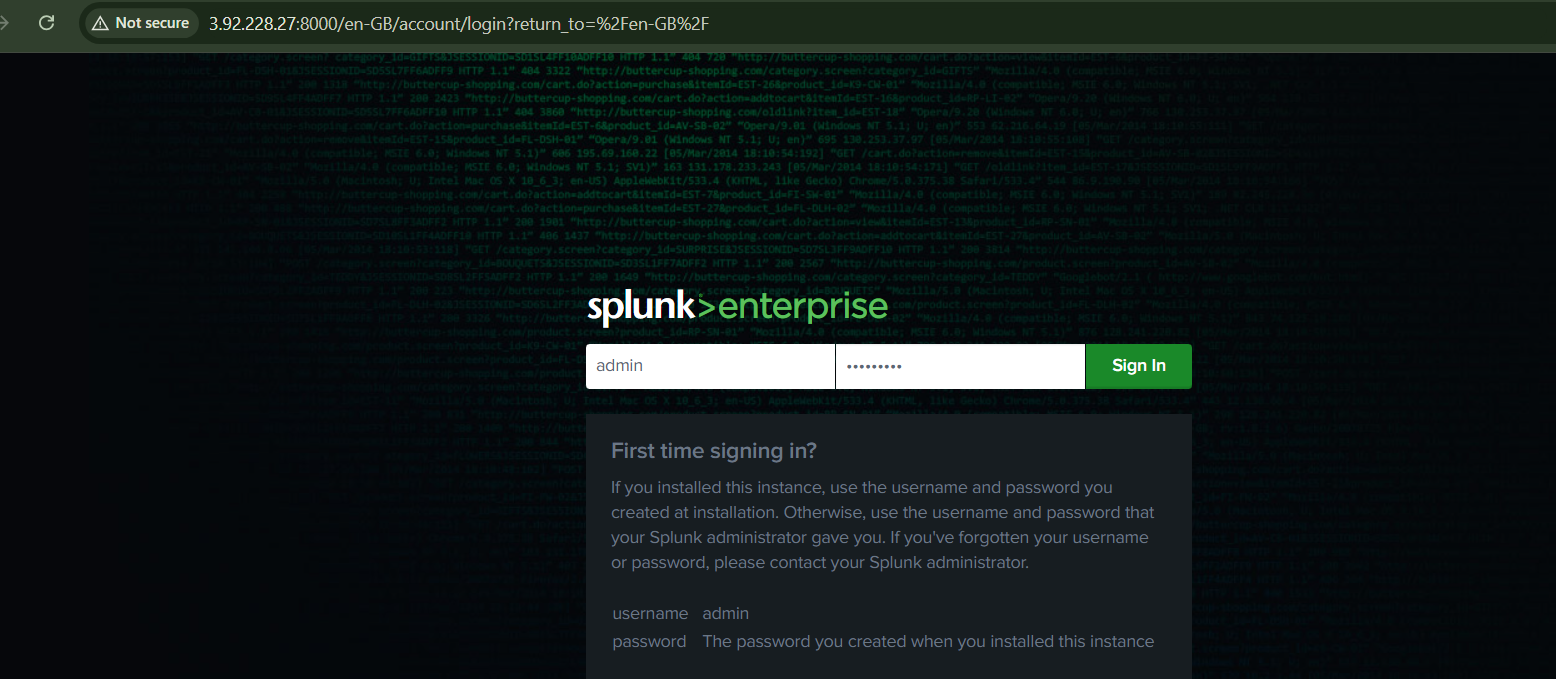
./splunk enable boot-start



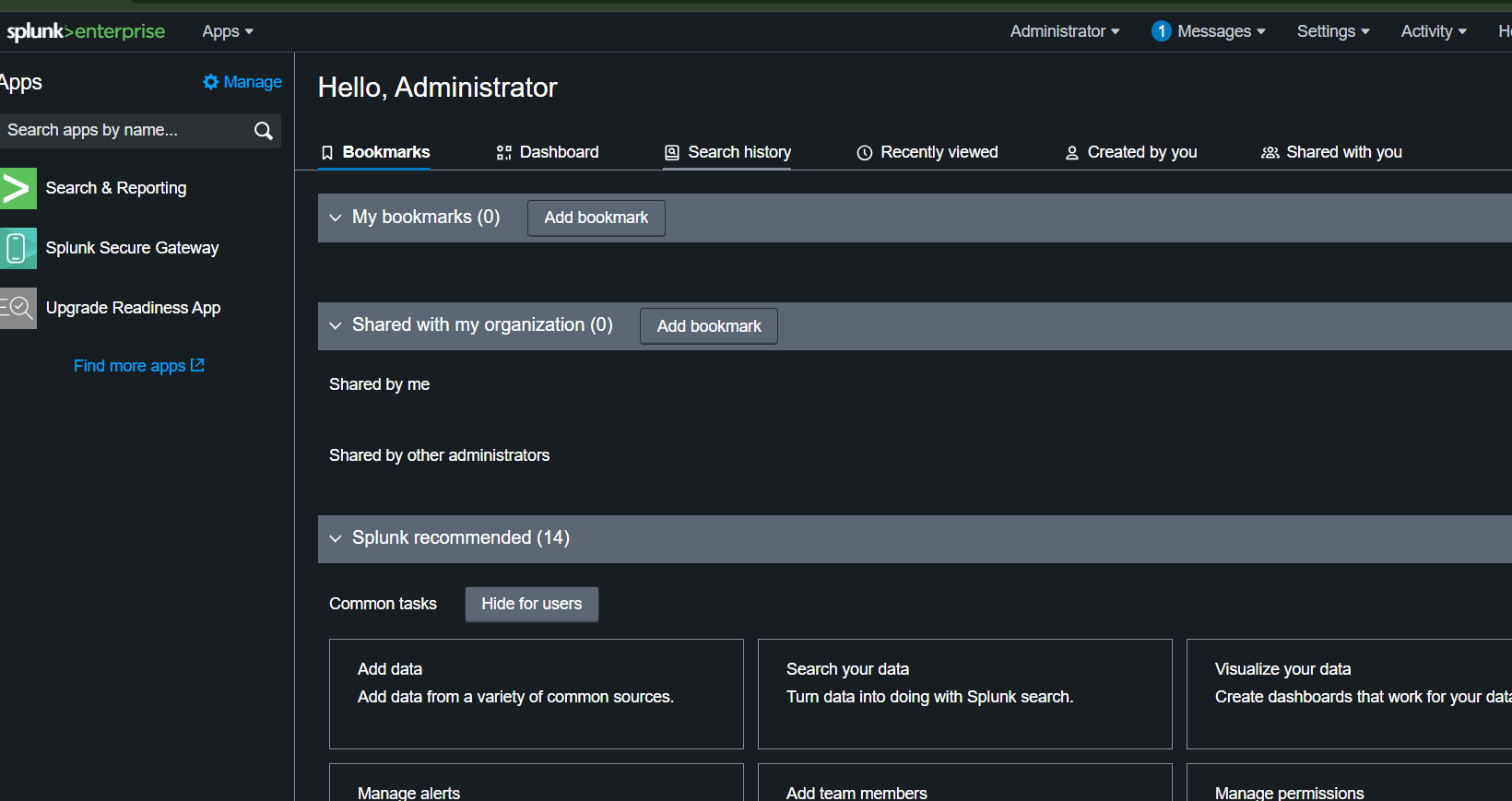
* the public ip and enter port
* http://3.92.228.27:8000



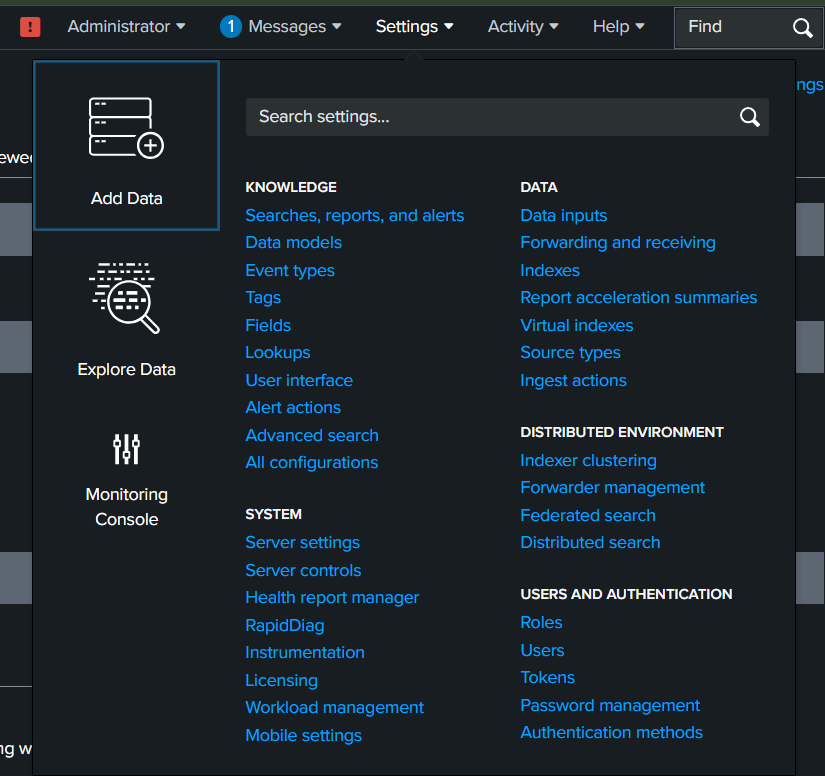
* enter the user name and password



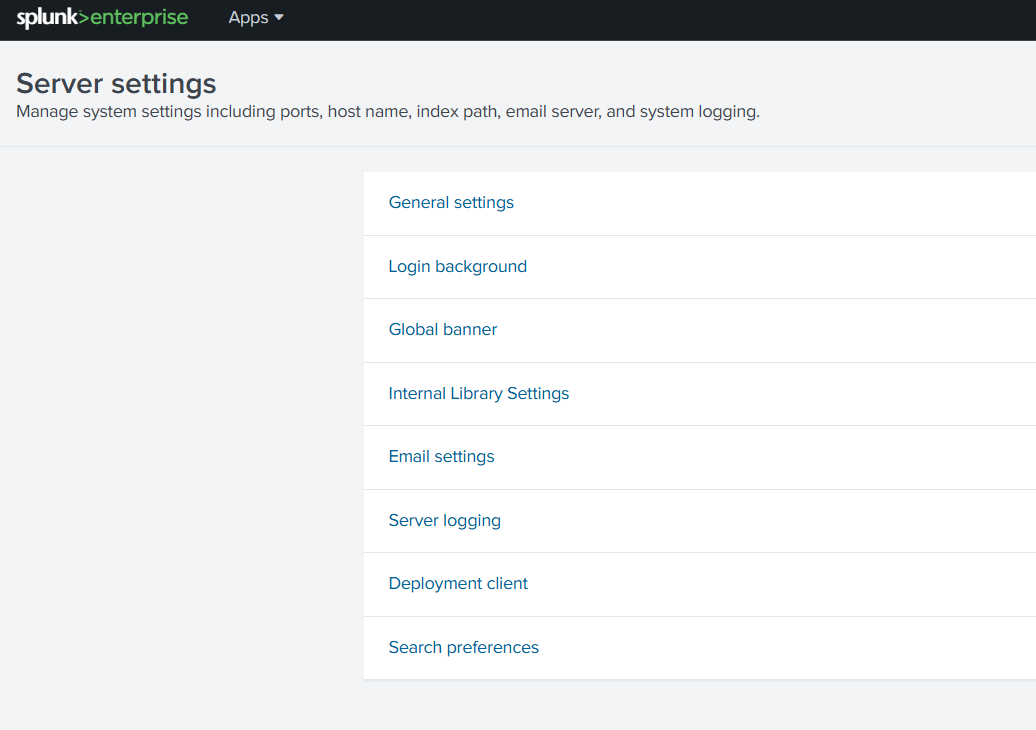
* this is the dashboard of splunk



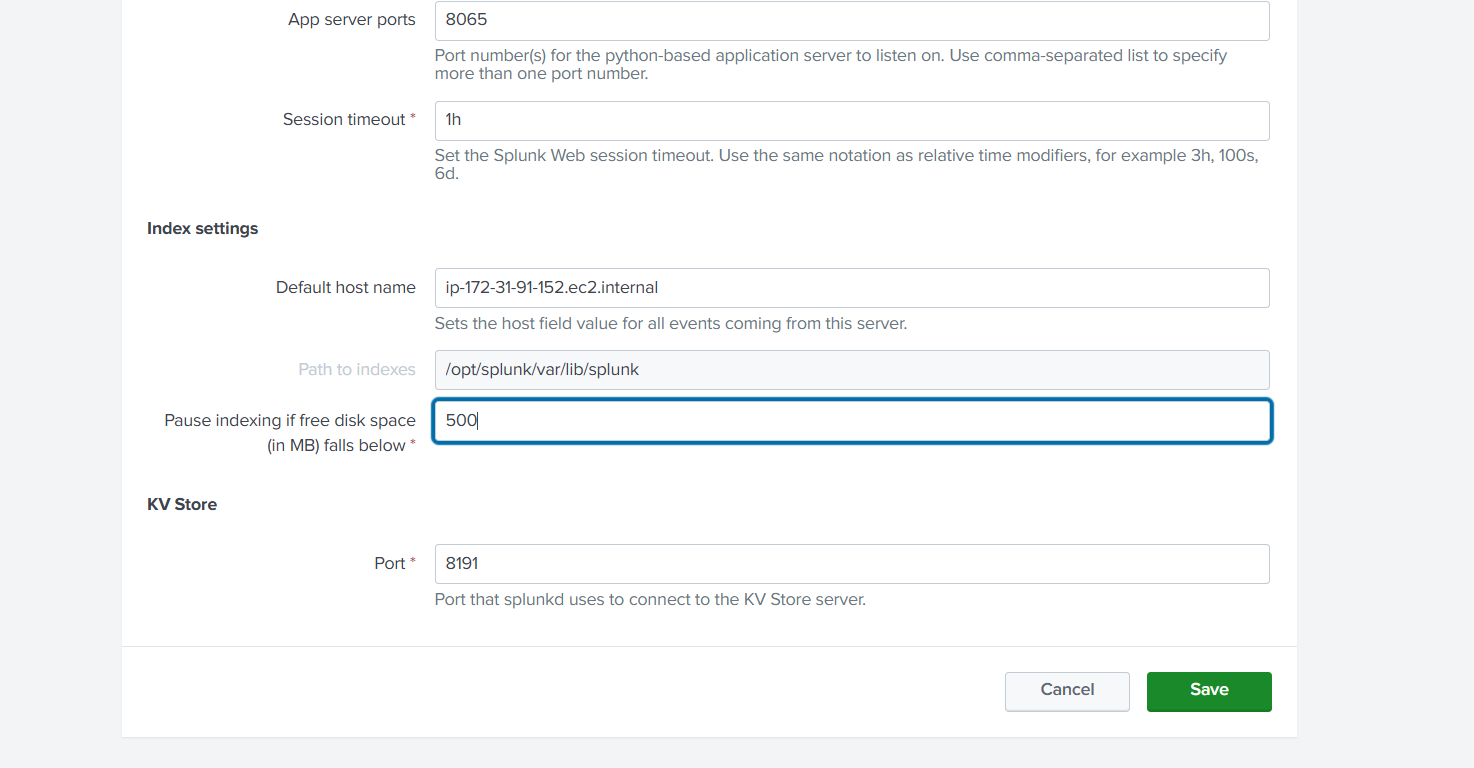
* click on settings
* select server settings



* after selecting server settings
* click on general settings

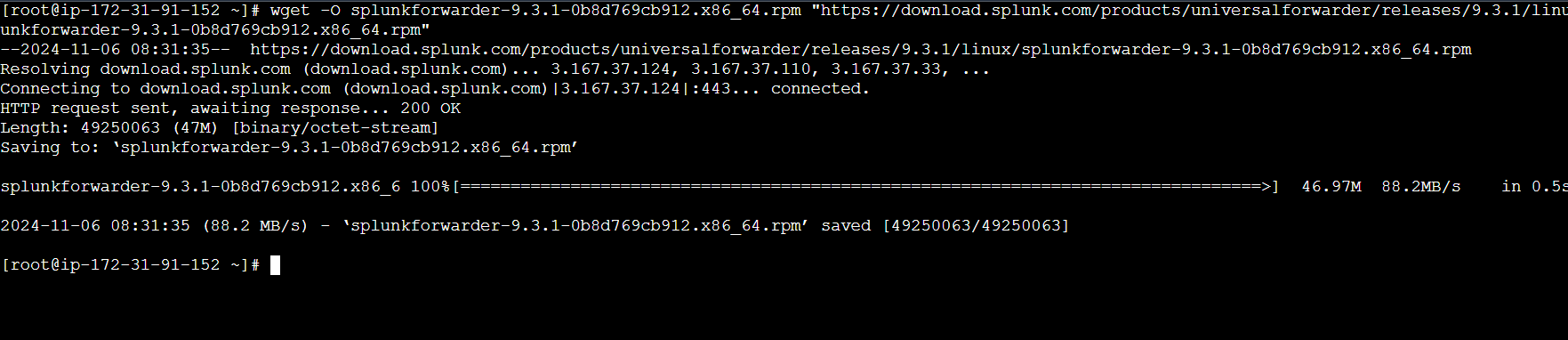


* change free disk space 5000 to 500
* than save it



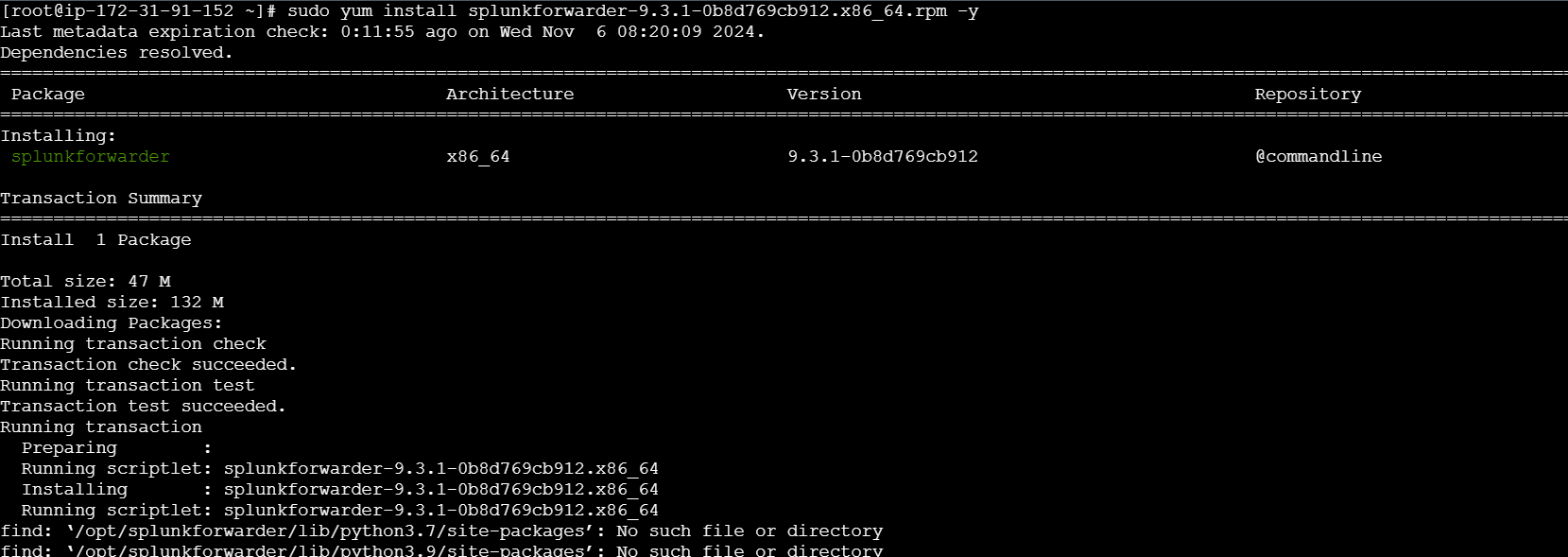
* Now its time to install splunk forwader

wget -O splunkforwarder-9.3.1-0b8d769cb912.x86\_64.rpm "https://download.splunk.com/products/universalforwarder/releases/9.3.1/linux/splunkforwarder-9.3.1-0b8d769cb912.x86\_64.rpm"



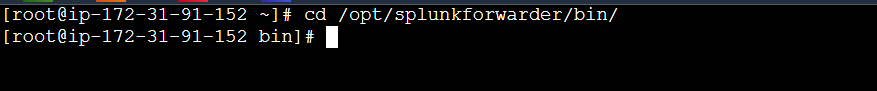
* Install downloaded rpm package

sudo yum install splunkforwarder-9.3.1-0b8d769cb912.x86\_64.rpm -y



* Switch to splunkforwarder bin directory

cd /opt/splunkforwarder/bin/



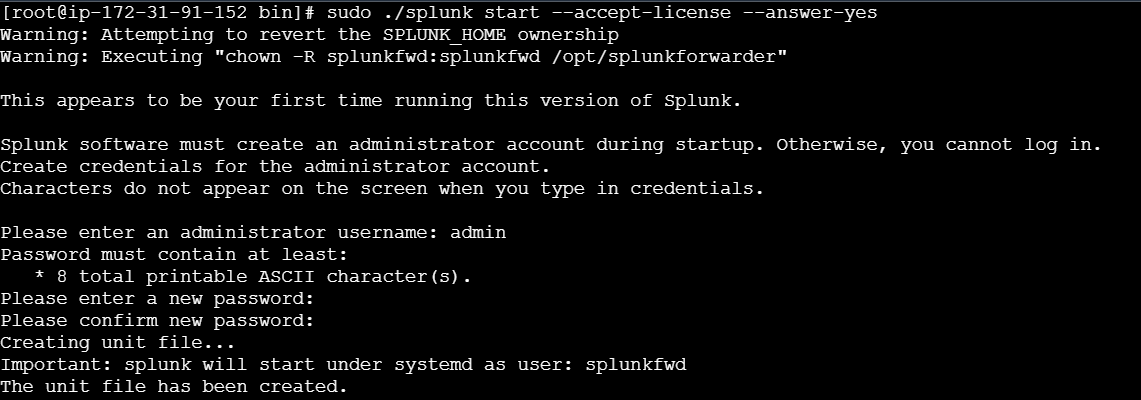
* Strat the splunk

sudo ./splunk start --accept-license --answer-yes

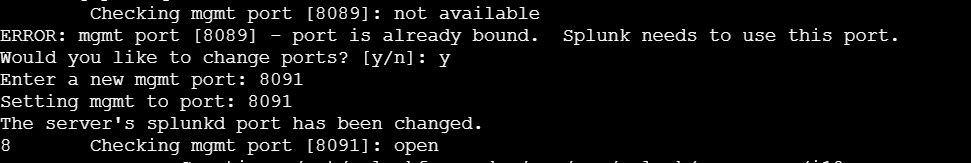
* It will ask usename password
* Better to give splunk credentials

Username :admin

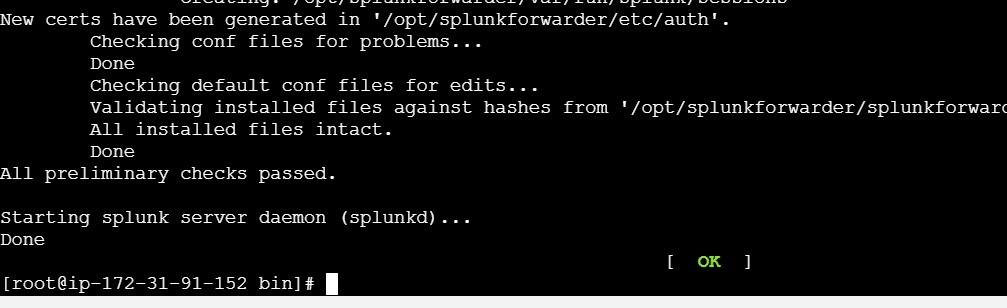
Password : admin1234 [give your custom password]



* It will ask mgmt port change just give yes
* Then enter port number 8091



* Splunk forwarder is successfully started

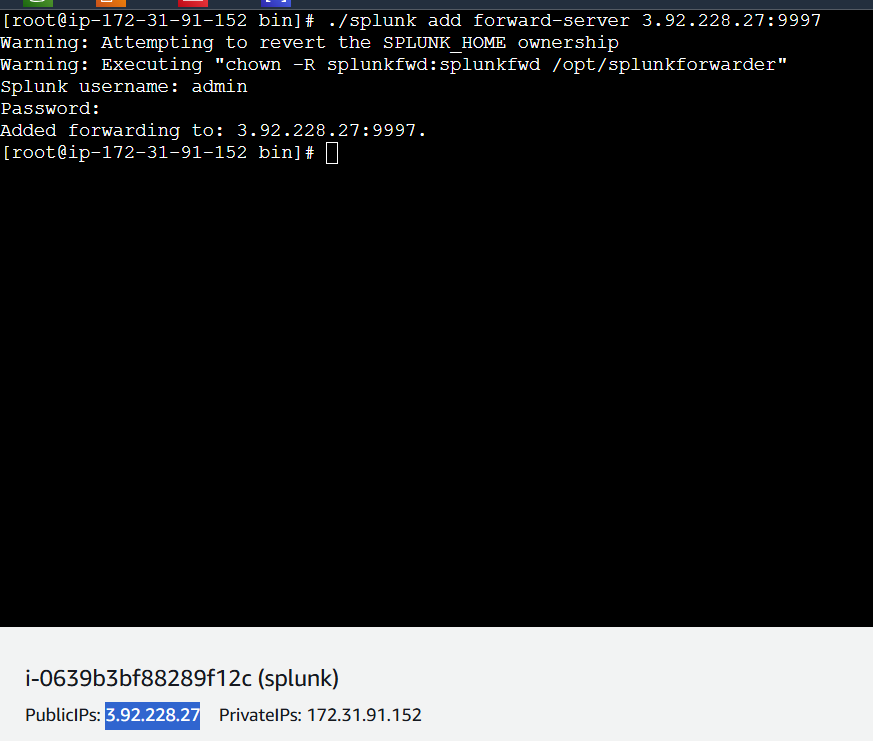


* We need to add forward server
* This splunk forwarder forwared the logs to splunk

./splunk add forward-server <your splunk public-ip>:9997

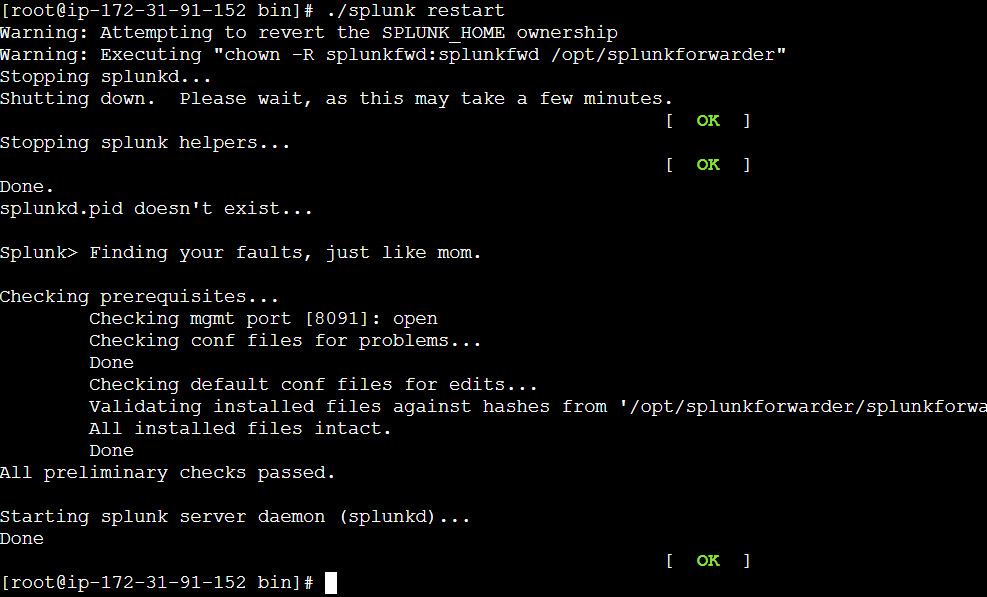
Ex: ./splunk add forward-server 8.253.63.35:9997

* It will ask your splunk user name and password



* After that restart the splunk forwarder

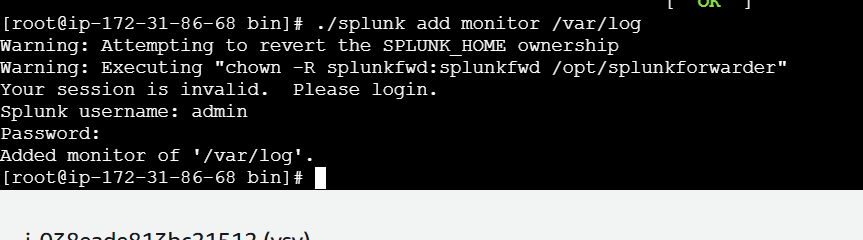
./splunk restart



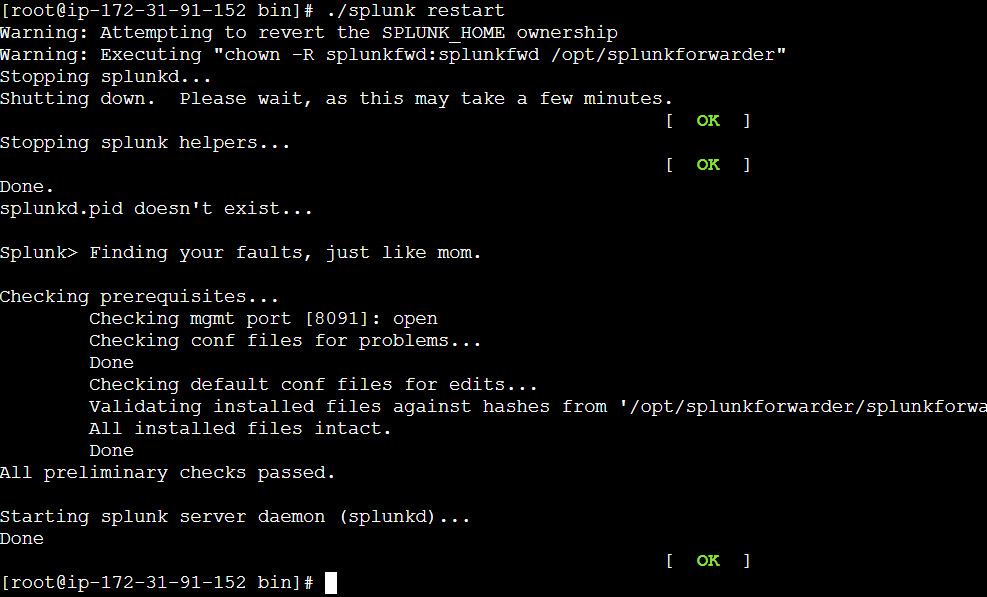
* Now add the log path to splunk forwarder

./splunk add monitor /var/log

* Enter the splunk user name and password

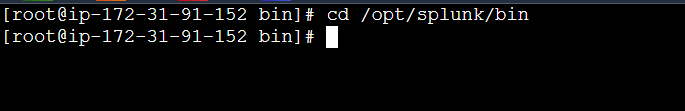


* Now again restart the splunk forwarder
* Restart is mandatory after doing any changes



* Now switch to splunk bin folder

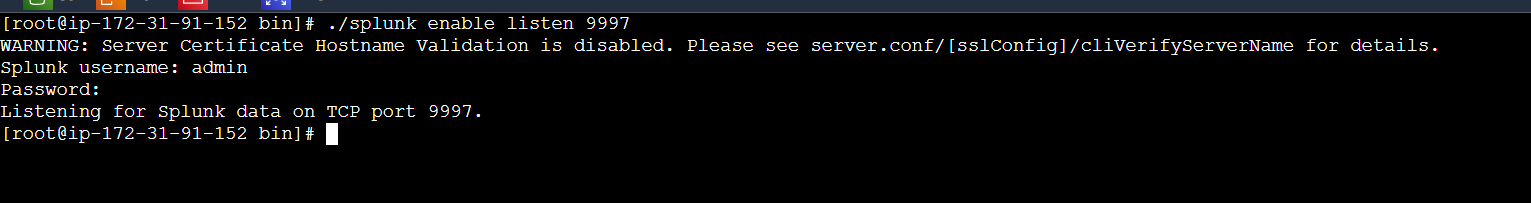
cd /opt/splunk/bin



* Enable the 9997 port requests

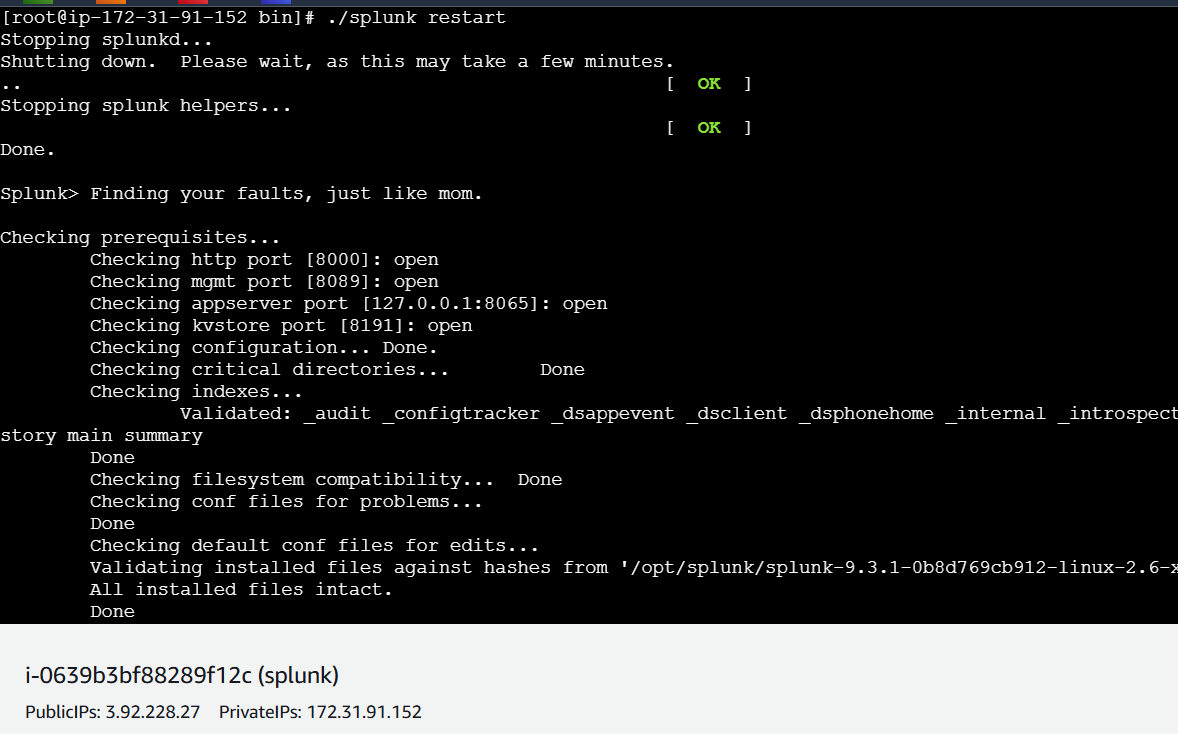
./splunk enable listen 9997

* It will ask the username and password just enter and continue

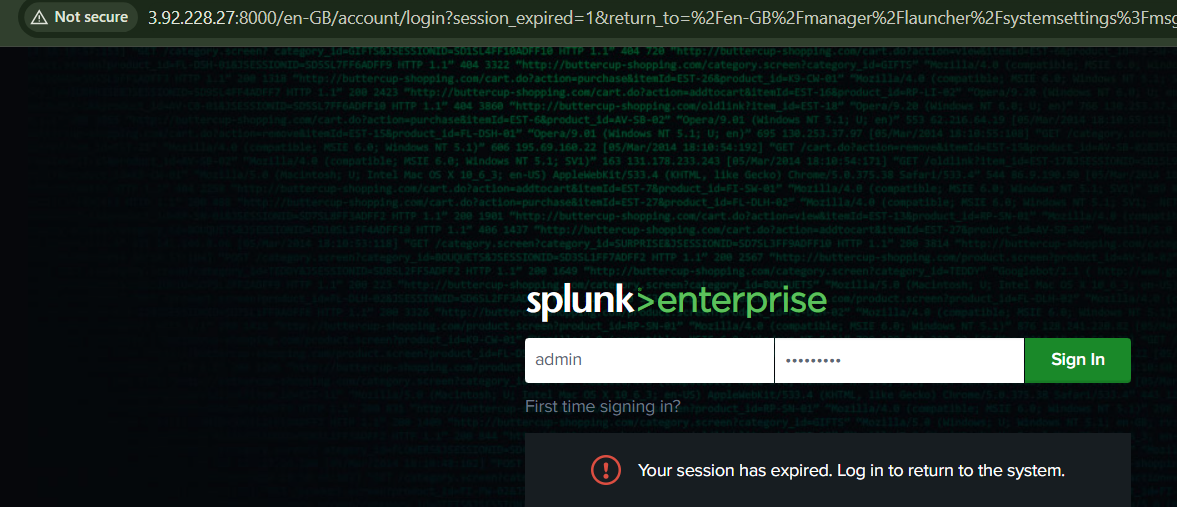


* Restart the splunk

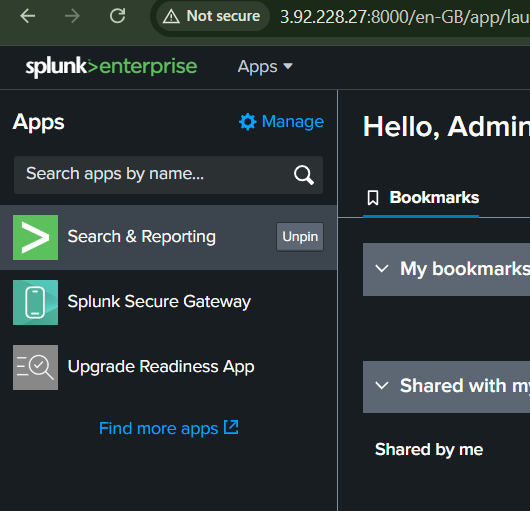
./splunk restart



* Again to the login to the splunk



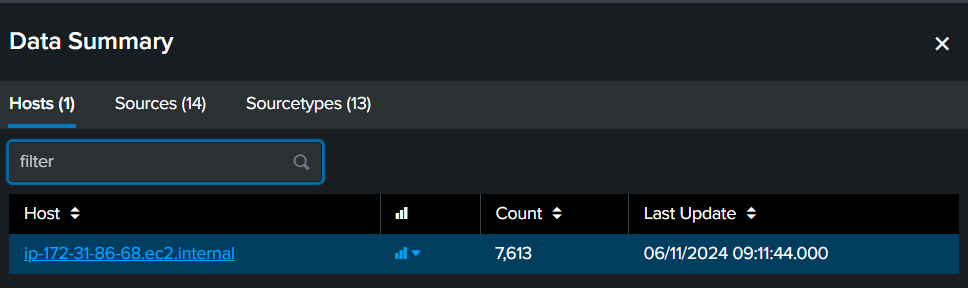
* Click in search and reporting
* If you not find serch and reporting just click on splunk>enterprise



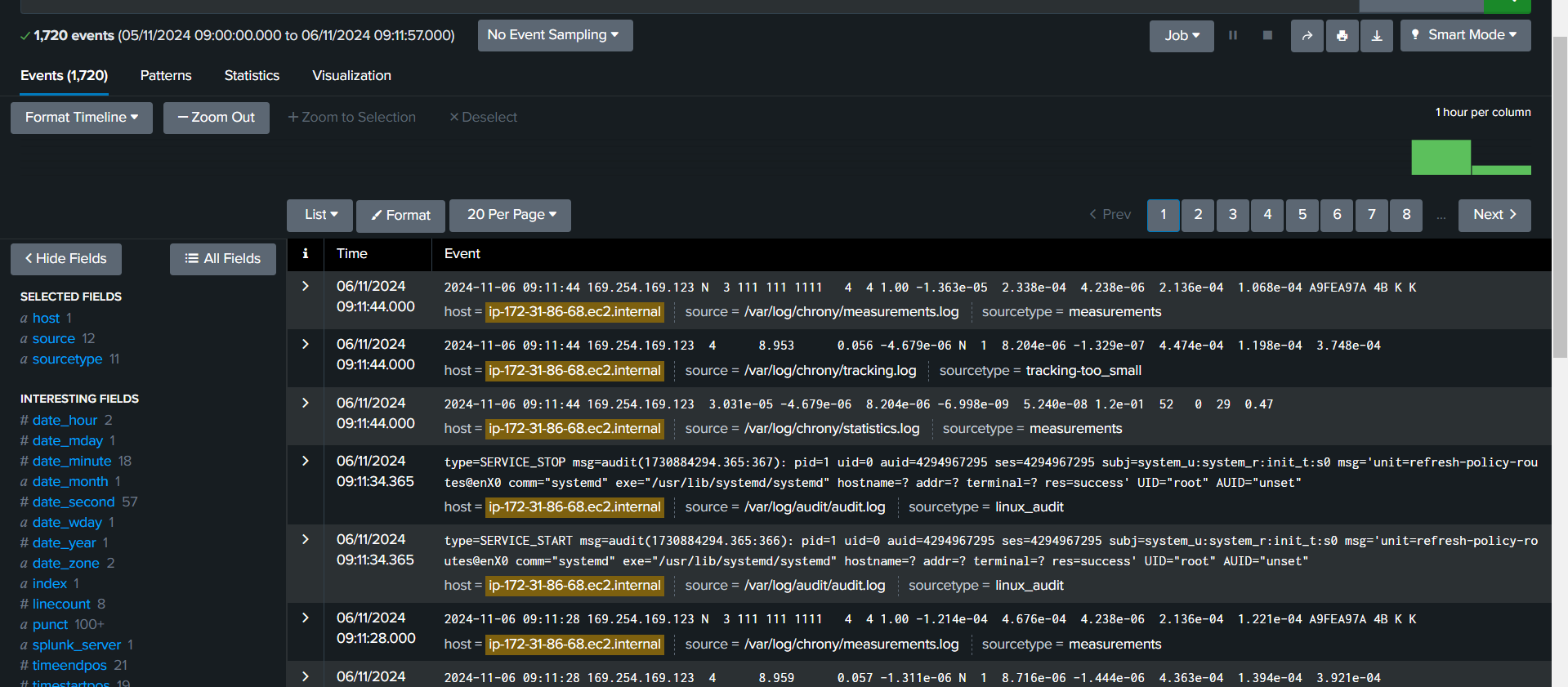
* Click on data summary



* Click on your ip address



* These are your splunk logs



Testing the splunk

Install httpd in splunk server

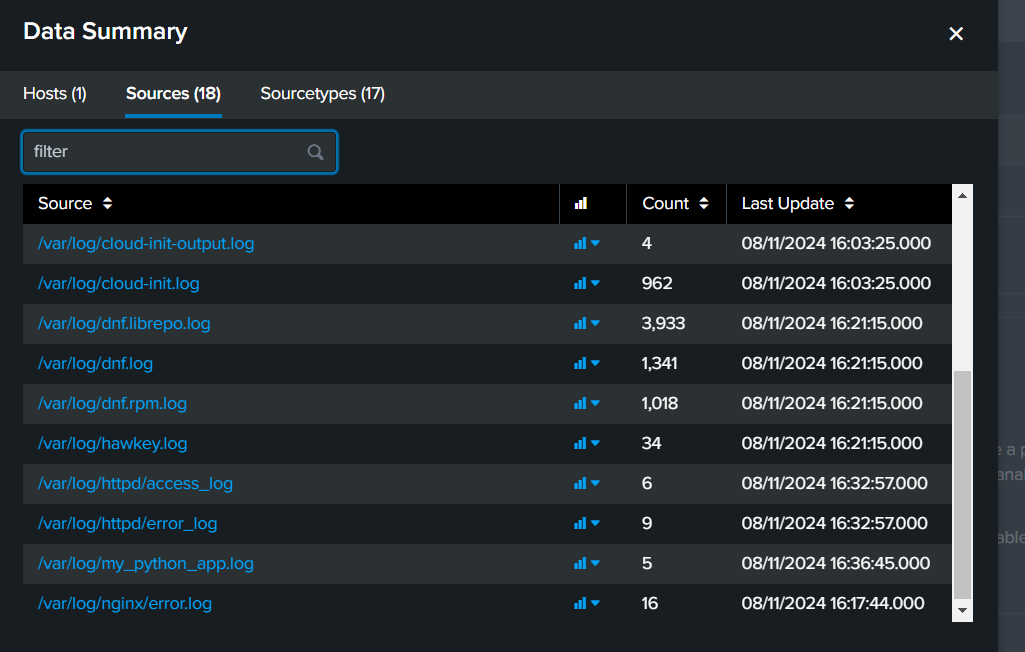
yum install httpd -y

systemctl strat httpd

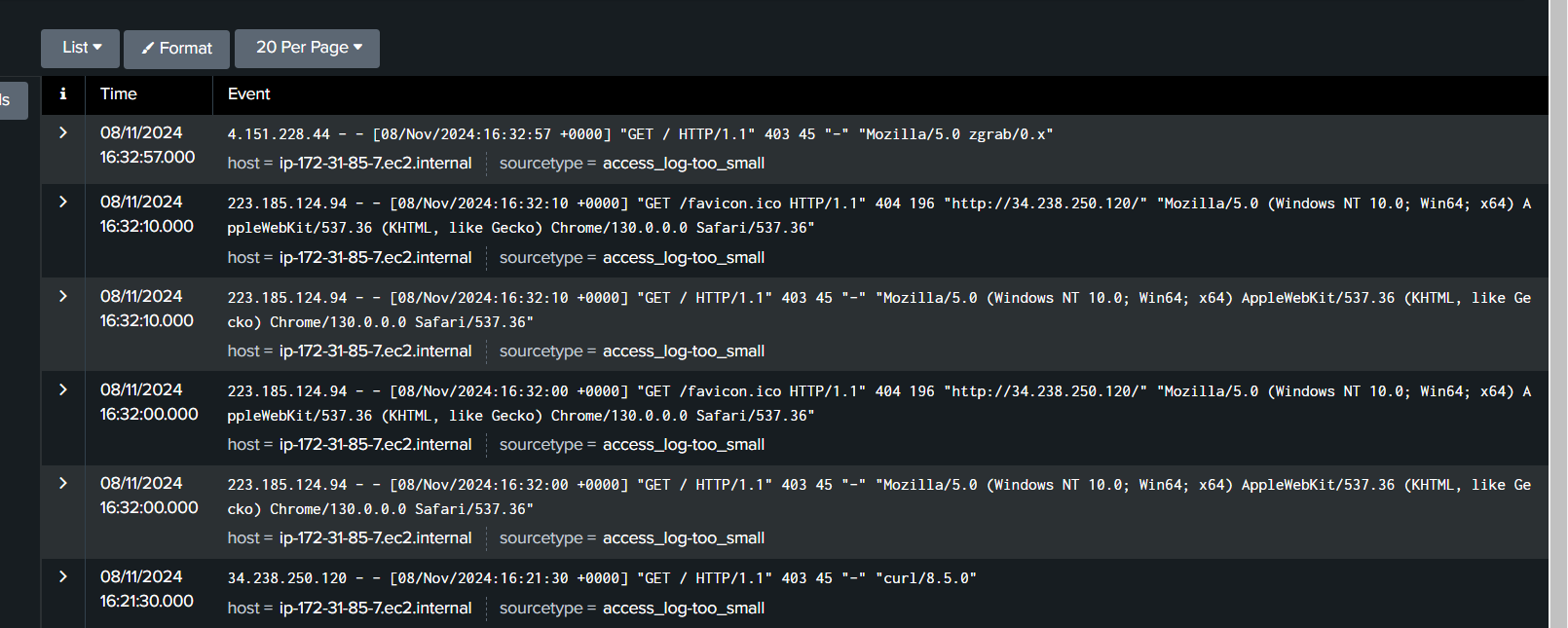
* Then search your public ip in browser

Next go to splunk click on data summery select sources

* Click on httpd/accesslog



* Click on httpd/accesslog ### these are the httpd application access logs



Testing method 2

* Create a test.py file add the bellow script

import logging

# Configure logging settings

logging.basicConfig(

level=logging.INFO,

format='%(asctime)s - %(levelname)s - %(message)s',

handlers=[

logging.FileHandler("/var/log/my\_python\_app.log"), # Change path if needed

logging.StreamHandler()

]

)

# Example usage

logging.info("This is a success log message.")

logging.error("This is an error log message.")

* Create another file app.py enter the below script

import logging

# Configure logging settings

logging.basicConfig(

level=logging.INFO,

format='%(asctime)s - %(levelname)s - %(message)s',

handlers=[

logging.FileHandler("/var/log/my\_python\_app.log"), # Ensure path is writable

logging.StreamHandler()

]

)

# Success log

logging.info("This is a success log message.")

try:

# Intentional error: Divide by zero

result = 10 / 0

except ZeroDivisionError as e:

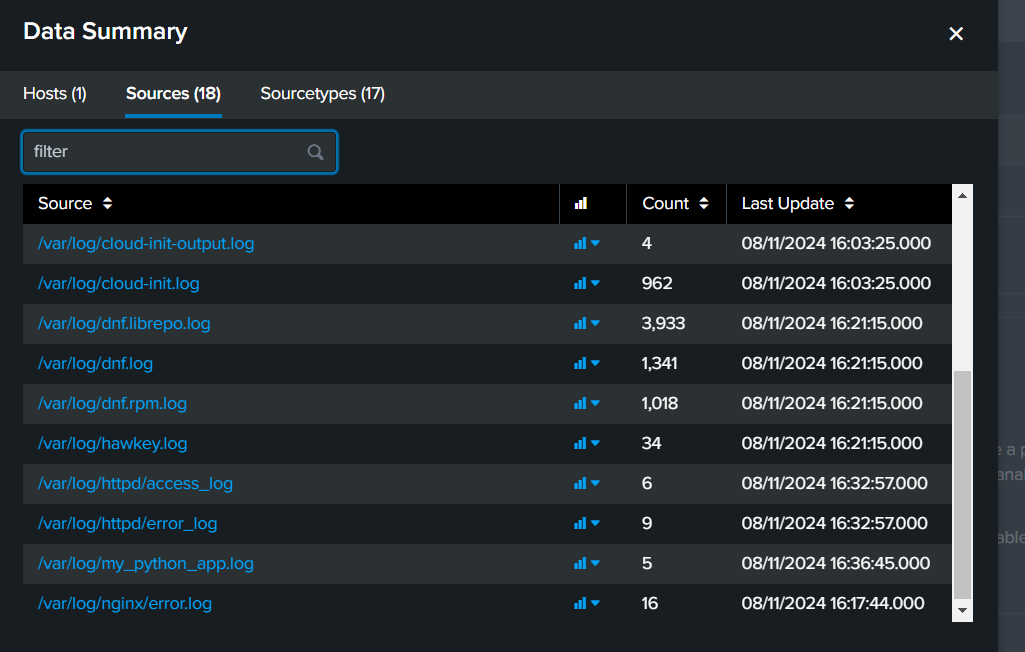
# Log the error with stack trace

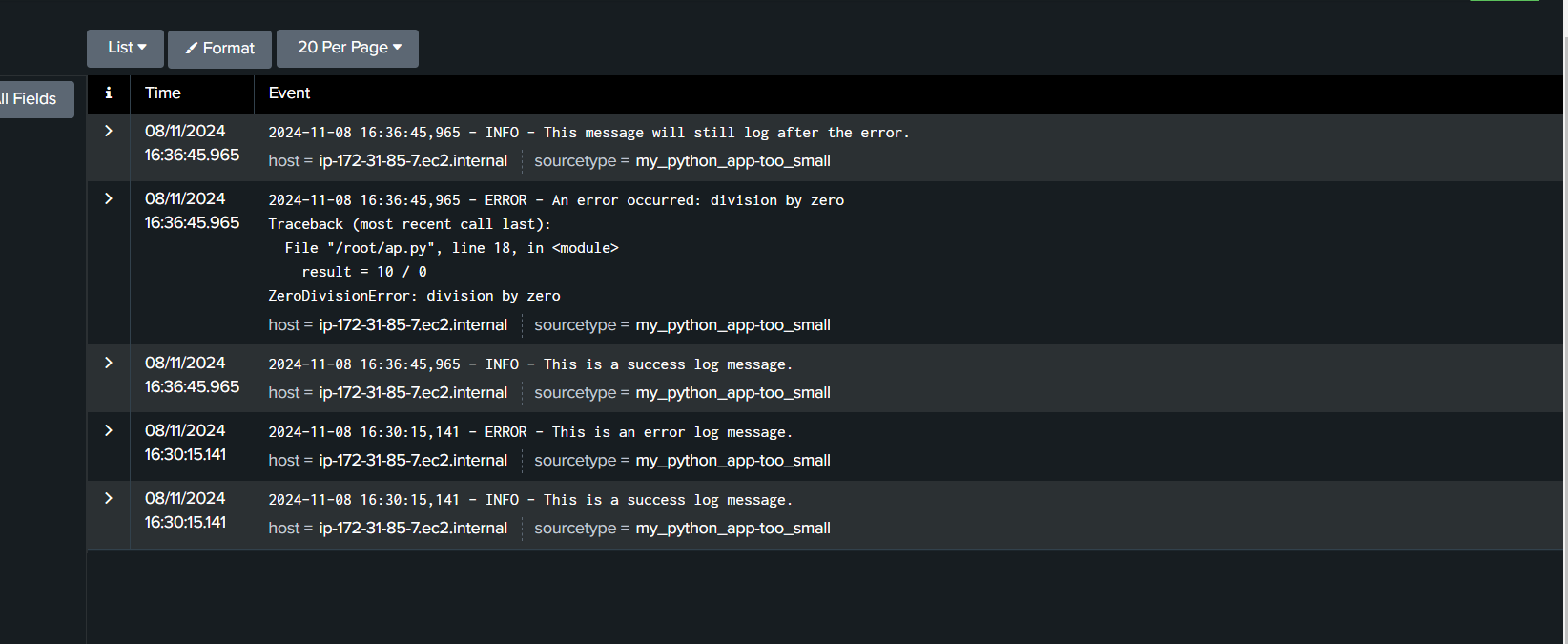
logging.error("An error occurred: %s", e, exc\_info=True)

# Additional success log

logging.info("This message will still log after the error.")

* Then open splunk data summary select sources
* Click on python\_app.log





These are the python application logs