**DevOps**

**SPLUNK->Logs Monitoring Tool:-**

* **Enterprise Monitoring tool**
* **Cost-involved**
* **Master and Slave Method – Pull and push based mechanism**
* **Monitors logs**
* **60-days free-trial is available for the learing & Development** 
  + **Splunk is Google for your machine data.**
  + **It’s a software/Engine which can be used for searching,visualizing,Monitoring,reporting etc of your enterprise data.**
* **Splunk takes valuable machine data and turns it into powerful "Operational Intelligence" by providing realtime insight to your data through charts, alerts, reports etc  
  Effective Monitoring and avoids unwanted wastages of the times**

1. **Purpose:** 
   * **Proactive Monitoring + Dashboard Generation + Alerting**
   * **Monitors Entire Application Logs**
   * **Troubleshooting, Auditing and Operational risk etc**
   * **During End of Day Batch Run and Close of Business**
   * **To understand the complex logs.**
   * **For better look and feel.**
   * **Splunk can store and process large amounts of data, data analysts.**
   * **Dashboards meant for Great visualization.**
   * **If you have a machine which is generating data continuously and you want to analyze the machine state in real time.**

1. **Metrics:** 
   * **Application, Logs, Disk, Network, Database, Security, Server etc**
   * **Log path and Logs as follows,**

**File system path: /opt/eRAMS/logs/SystemErr.log**

**File system path: /opt/eRAMS/logs/SystemApp.log**

**File system path: /opt/eRAMS/logs/SystemQuery.log**

**File system path: /opt/eRAMS/logs/Systemgeneric.log**

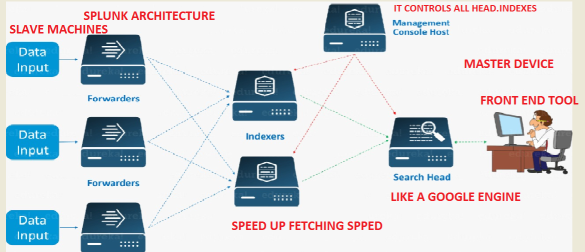
**File system path: /opt/eRAMS/logs/Systemmiddleware.log etc**

1. **Scope of the Developer**

* **Define FS path for logs**
* **What kind of logs need to be captured?**
* **How frequently Logs streamlining process could runs**

**Architecture and Functionality:**

* **Splunk Server Monitors Multiple Applications logs on the servers**
* **Deticated Server Each slaves need one Forwarder**
* **Master Server**

****

**Components of splunk:**

**=====================**

**1) Search head – provides GUI for searching**

**2) Indexer – indexes machine data**

**3) Forwarder - Forwards logs to Indexer**

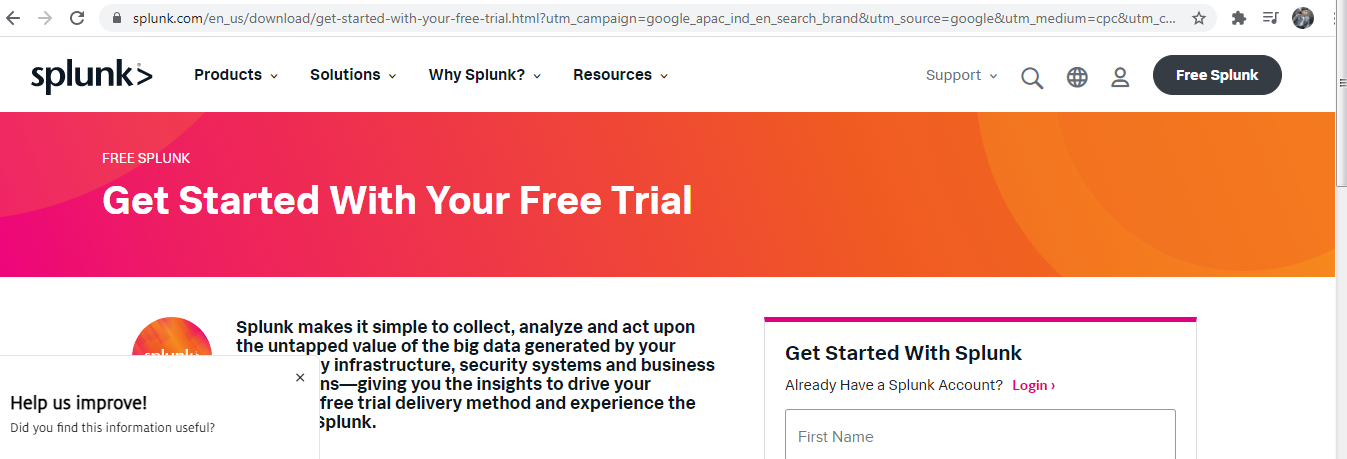
**4) Deployment server - Manages splunk components in distributed environment**

**Search head, Indexer and Management Console could have been kept in Master.**

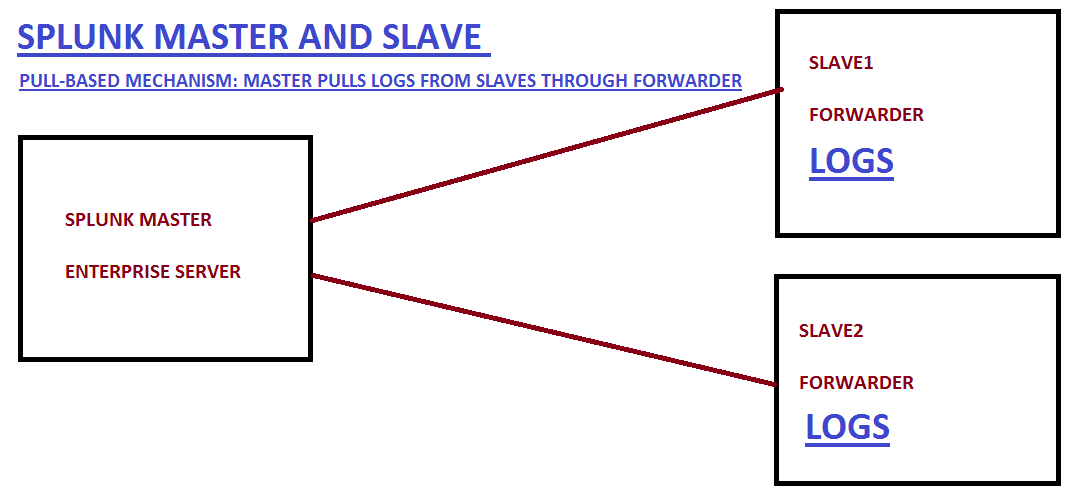
**In slave the Forwarder packagage has been installed.**

1. **Login portal:** [**https://www.splunk.com/**](https://www.splunk.com/)

**Create an sign up**

****

1. **Practicle:- PUSH AND PULL**

****

1. **Practicle: CREATE AN COUPLE OF EC2 SERVERS:**

**Splunk Master and Forwarder Set-Up:** As of now only with these o/s we can set-up the **Important Note:**

* **1 Master to Many Slaves Integration & automation of Logs Monitoring is possible.**
* **Make Sure Both Master and Slaves should be in the same Version always.**
  1. **Goto :** [**https://www.splunk.com/**](https://www.splunk.com/)
     + **Under PLATFORM and Click on** [**Free Trials & Downloads**](https://www.splunk.com/en_us/download.html)
     + **Choose Splunk Enterprise**
     + **And Download Free 60-Days Trial**
     + [**https://www.splunk.com/en\_us/download/splunk-enterprise.html**](https://www.splunk.com/en_us/download/splunk-enterprise.html)

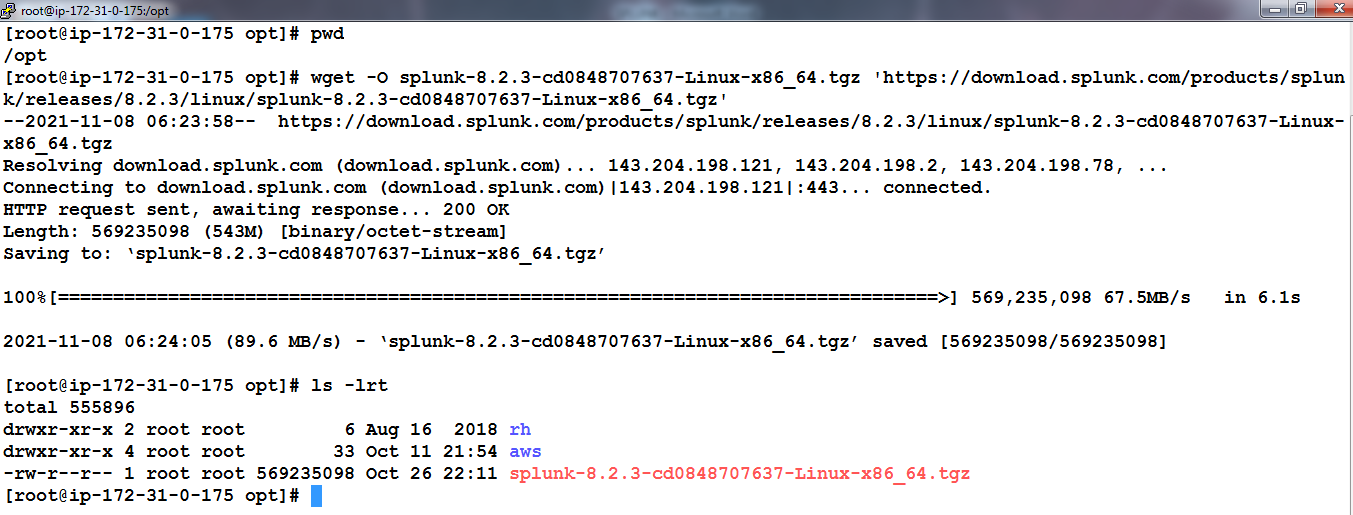
#### Choose Your Installation Package as a “Linux”

* 1. **Splunk Master Set-Up** [**https://www.splunk.com/en\_us/download/splunk-enterprise/thank-you-enterprise.html**](https://www.splunk.com/en_us/download/splunk-enterprise/thank-you-enterprise.html)

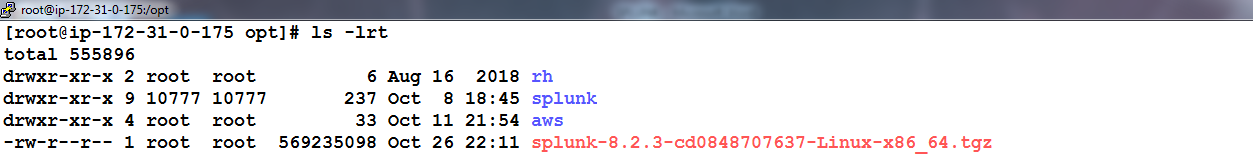
**Operating Systems Supports: Windows/Linux/Mac OS; We have choosen Linux for the demo**

**Login with Master Server, become a root user and navigate into cd /opt**

**wget -O splunk-8.2.3-cd0848707637-Linux-x86\_64.tgz 'https://download.splunk.com/products/splunk/releases/8.2.3/linux/splunk-8.2.3-cd0848707637-Linux-x86\_64.tgz'**

****

**tar -xvzf splunk-8.2.3-cd0848707637-Linux-x86\_64.tgz**

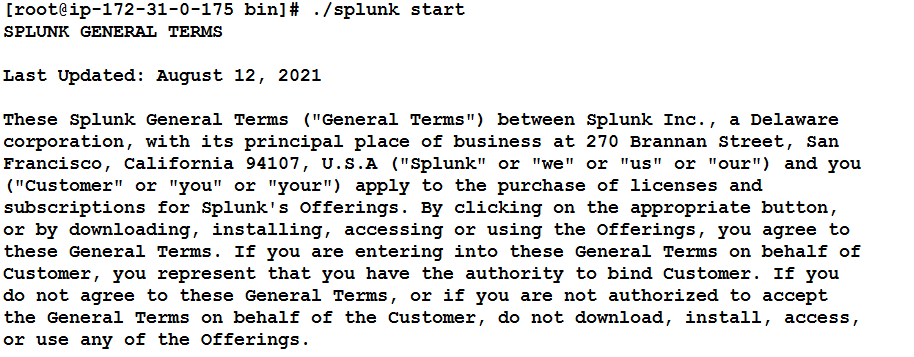
****

**Navigate to the Splunk Directory**

****

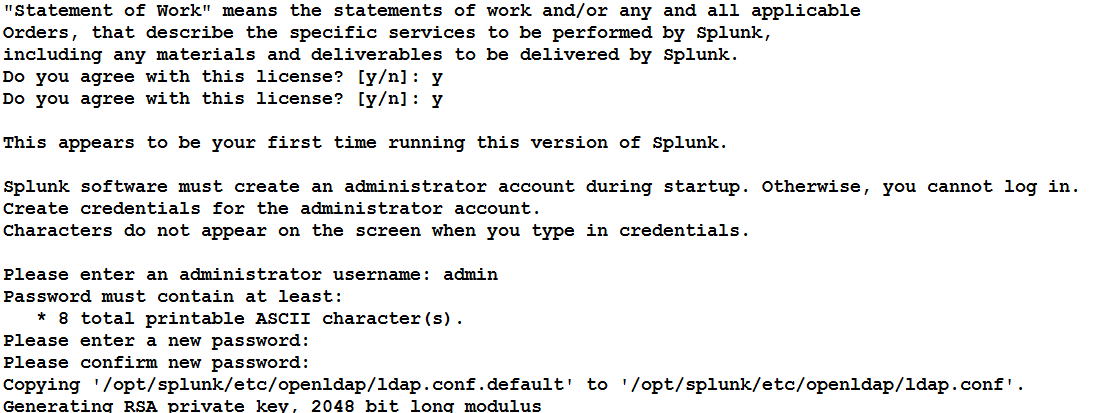
**Goto bin and start Splunk using command: ./splunk start**

**Keep enter Space bar until we reach 100% read and enables to ask options y/n.**



**Set your user-defined User name and password:**

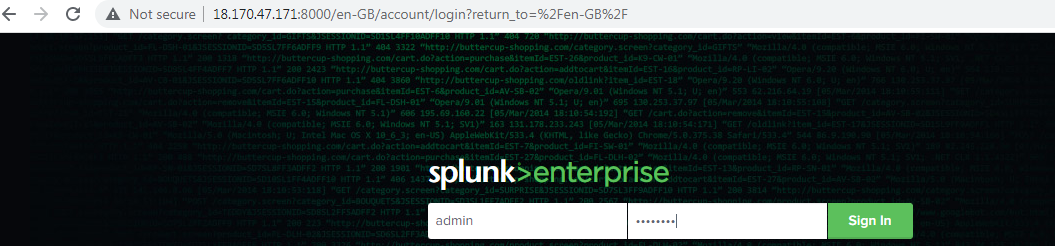
**My choice: admin and admin123**



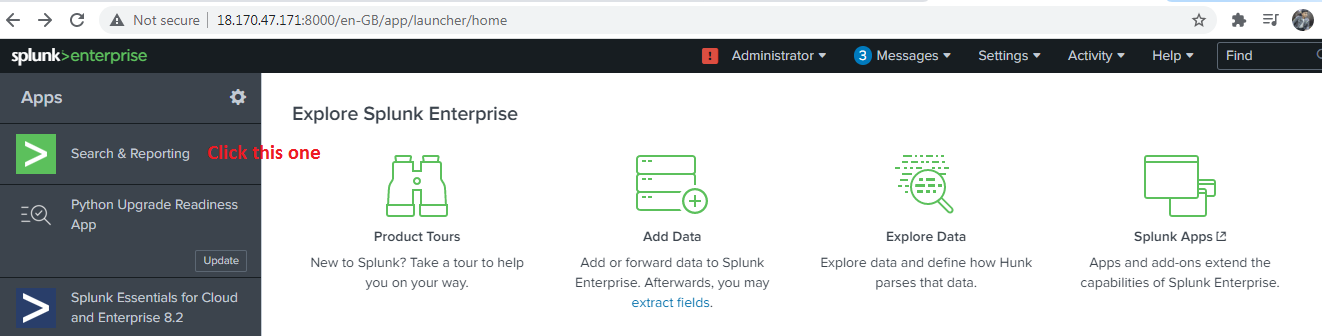
**The Port Number for the Splunk is : 8000, Successfully started.**



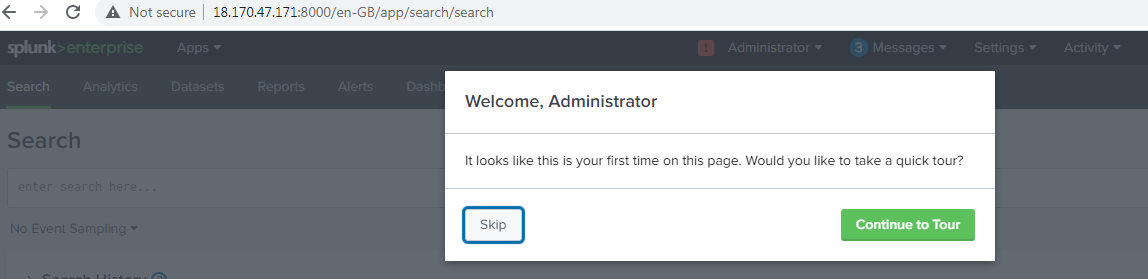
**Verify the Splunk Master using Public Ip and Port Number and Login with credentials we set.**

****

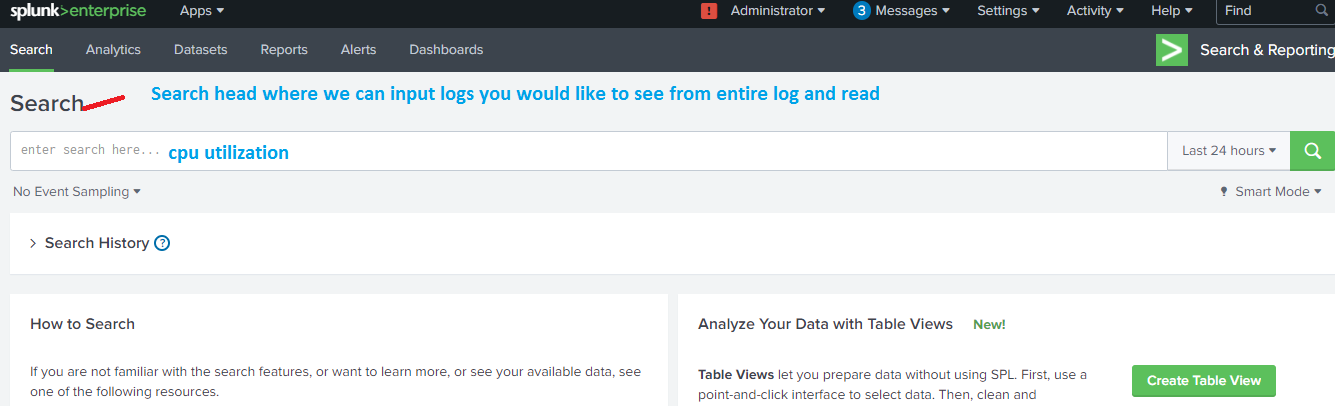
**Goto Search & Reporting**

****

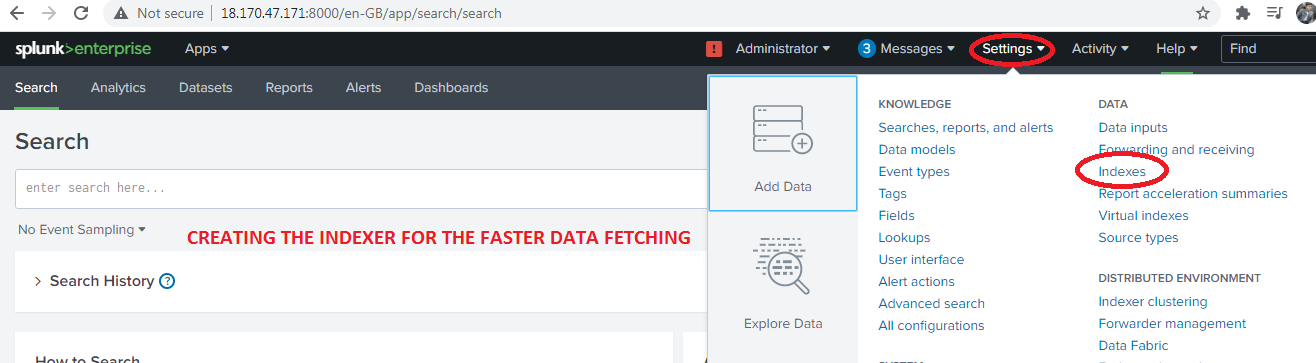
**Click on Continue to Tour**

****

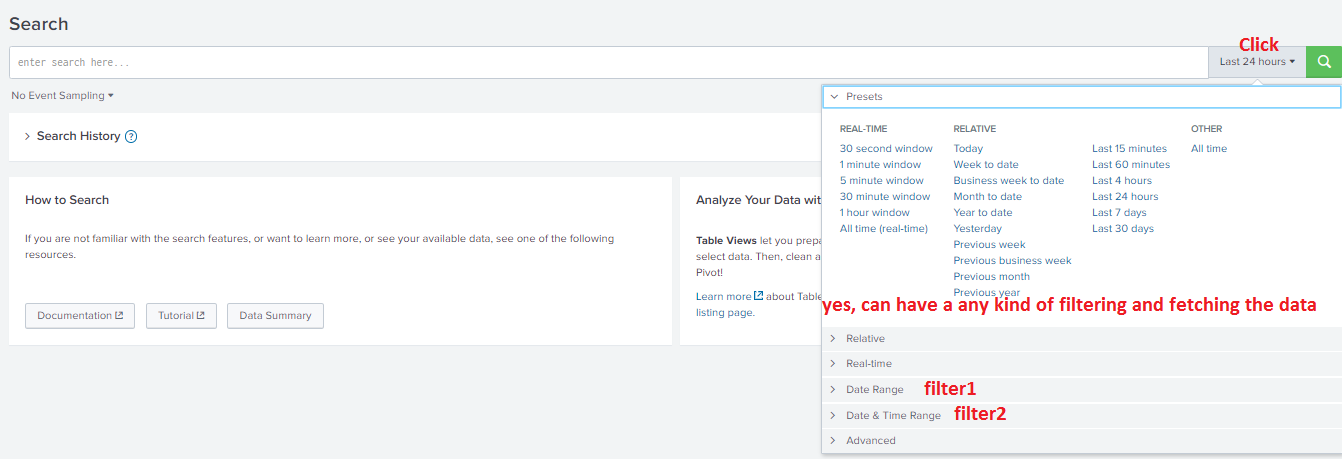
**Input Log need to be watched in the search engine and perform searching…..**

****

**Way to Create an Indexer for Quick Log fetching and report generation.**

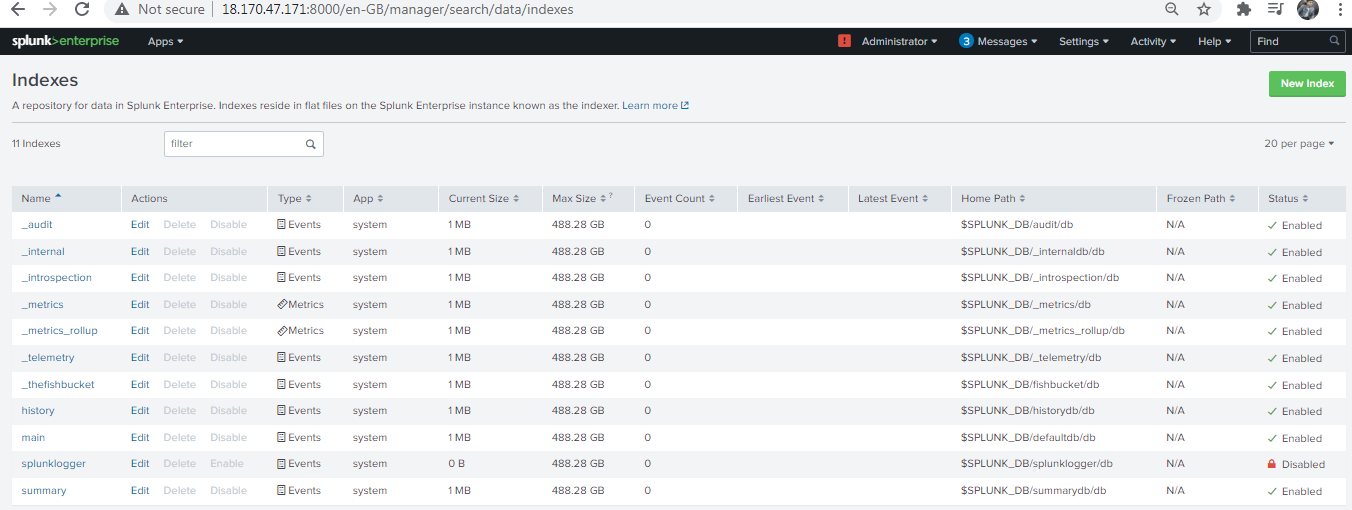


**Filtering the Logs as per ,the need using options available here**



**System generates and Normal files:**

**The file starts with \_ is nothing but system generated one. We could also creates our own index**

****

**Task:**

**Create a new indexer and map to logs**

**Change the Port Number from 8000 to 10000**

**Note: We will make the main indexer for the practical purpose**

* 1. **Splunk Forwarder Set-Up:**[**https://www.splunk.com/en\_us/download/universal-forwarder.html**](https://www.splunk.com/en_us/download/universal-forwarder.html)

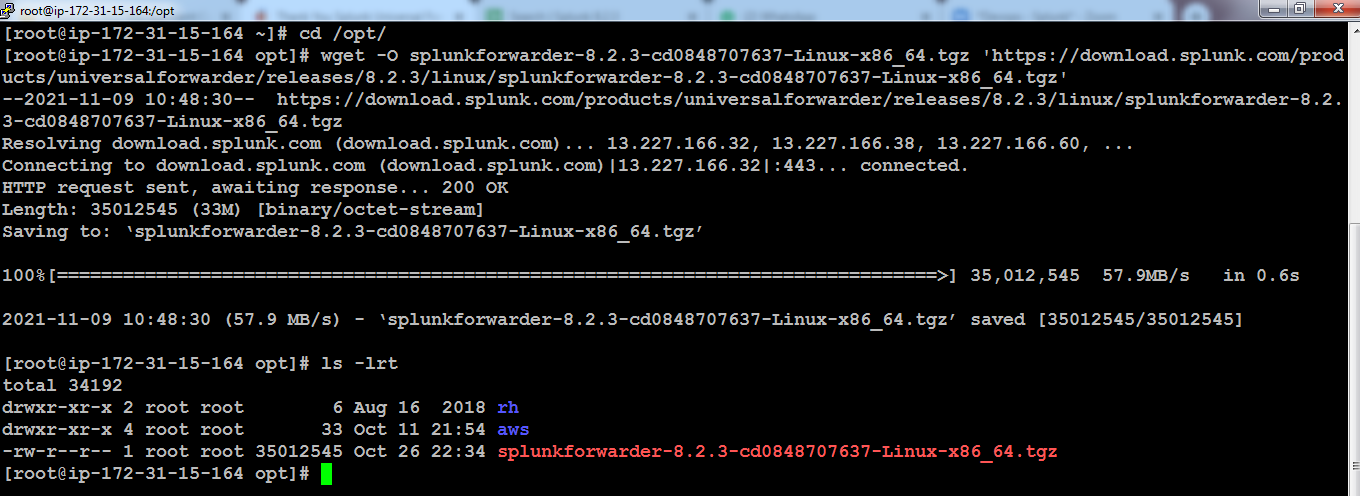
**Operating Systems: Windows; Linux; Mac OS; Free BSD; Solaris and AIX – App may runs in any platform and hence Forwarder cannot be restricted with any Platform.**

**Login with default user – Become as a root user – navigate to /opt FS path**

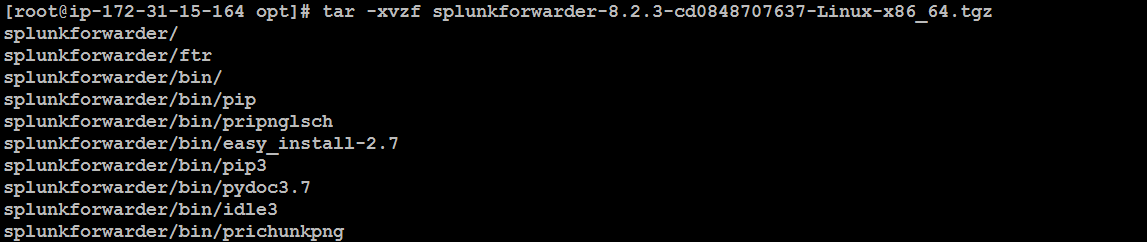
**Both Master and Slave should be the same versions.**

[**https://www.splunk.com/en\_us/download/universal-forwarder/thank-you-universalforwarder.html**](https://www.splunk.com/en_us/download/universal-forwarder/thank-you-universalforwarder.html)

**wget -O splunkforwarder-8.2.3-cd0848707637-Linux-x86\_64.tgz 'https://download.splunk.com/products/universalforwarder/releases/8.2.3/linux/splunkforwarder-8.2.3-cd0848707637-Linux-x86\_64.tgz'**

****

**tar -xvzf splunkforwarder-8.2.3-cd0848707637-Linux-x86\_64.tgz**

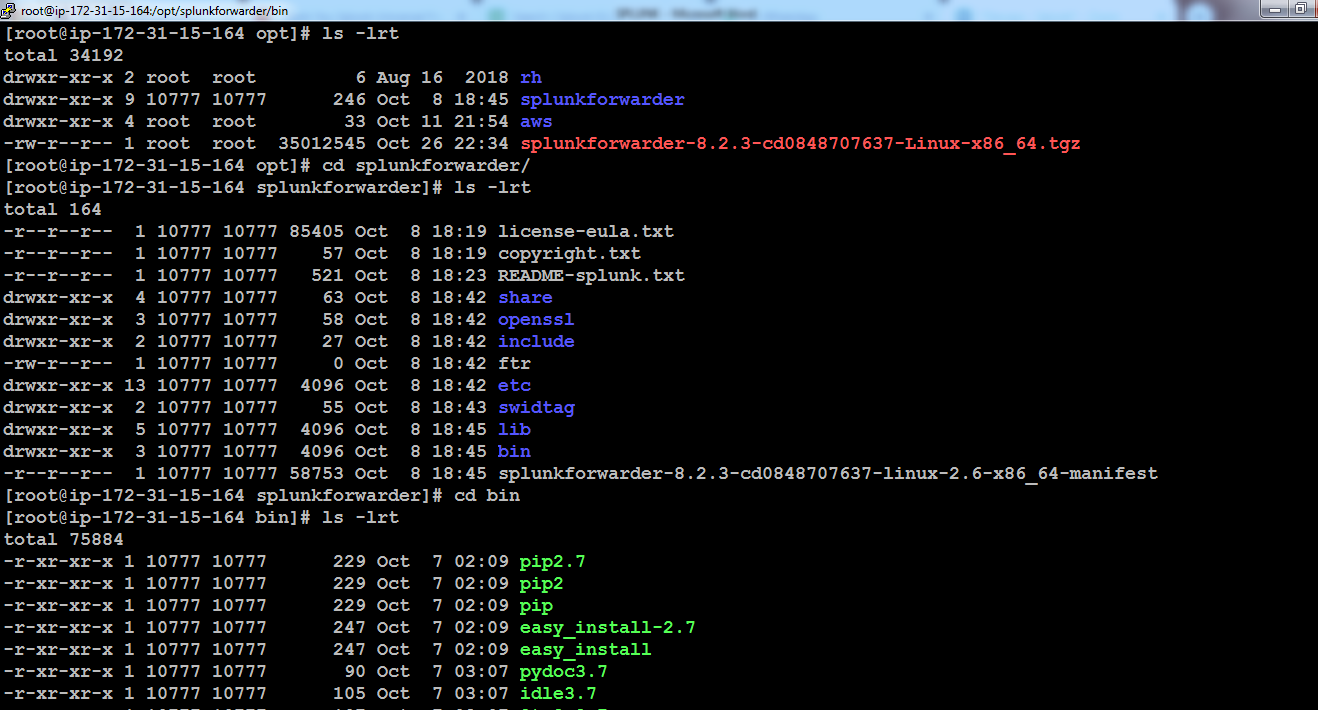
****

**Navigate into Splunkforwarder using an command: cd splunkforwarder/**

**List using the command: ls –lrt**

**Navigate to : cd /bin**

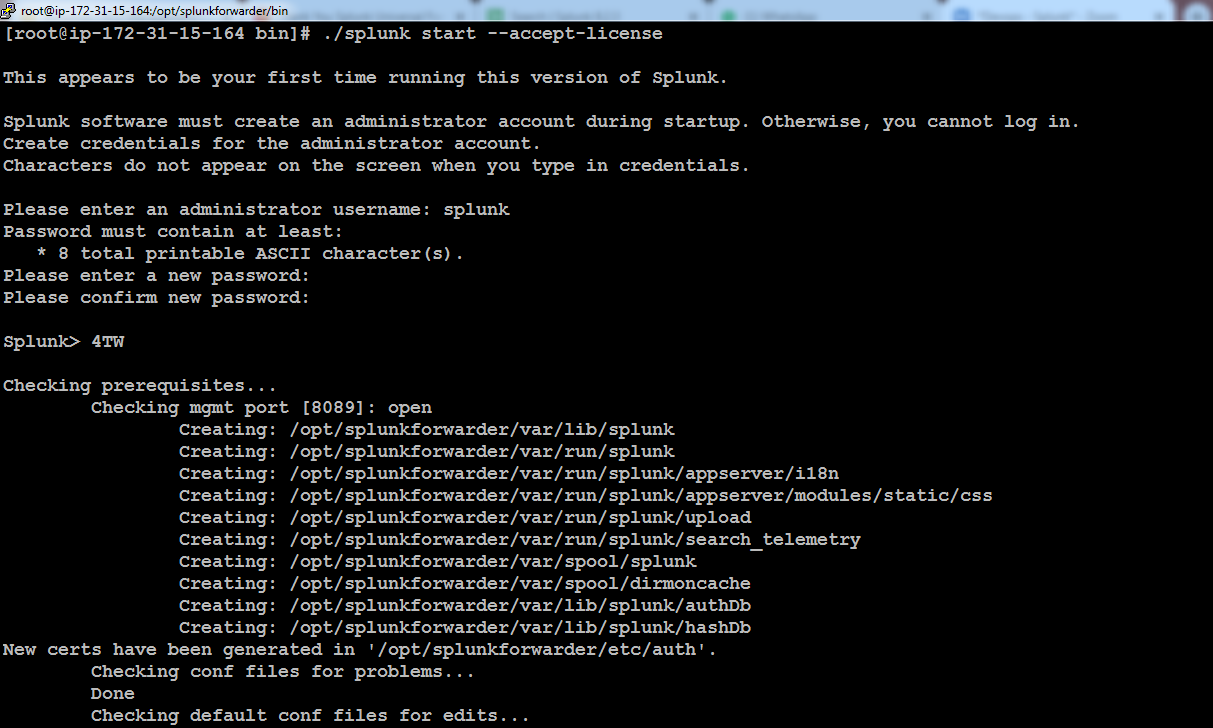
**Then list bin directort: ls -lrt**

****

`

**./splunk start --accept-license**

**Set the userid and password … Mostly set the same credentials we had been updated for master**



**Note: We have been completed <Master and Slave set-up and also started both the processes>**

**MASTER AND SLAVE INTEGRATION AND TESTING:**

1. **Port Number : Default Port where forwarder can push the logs to Master is : 9997**
2. **Master Public IP 13.233.184.13**
3. **Sample Logs Upload through winscp**

**FROM SPLUNK FORWARDER FOLLOW THE BELOW STEPS:**

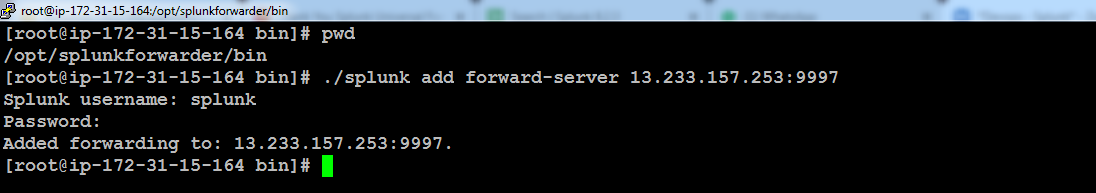
**Navigate to /opt/splunkforwarder/bin**

**./splunk add forward-server Master’s Pub IP:9997**

**./splunk add forward-server 13.233.184.13:9997**

**Supply user name and password created to the Slave machine here,**

**Example: splunk and splunk123**



**Testing**

* **Download the sample log file:**

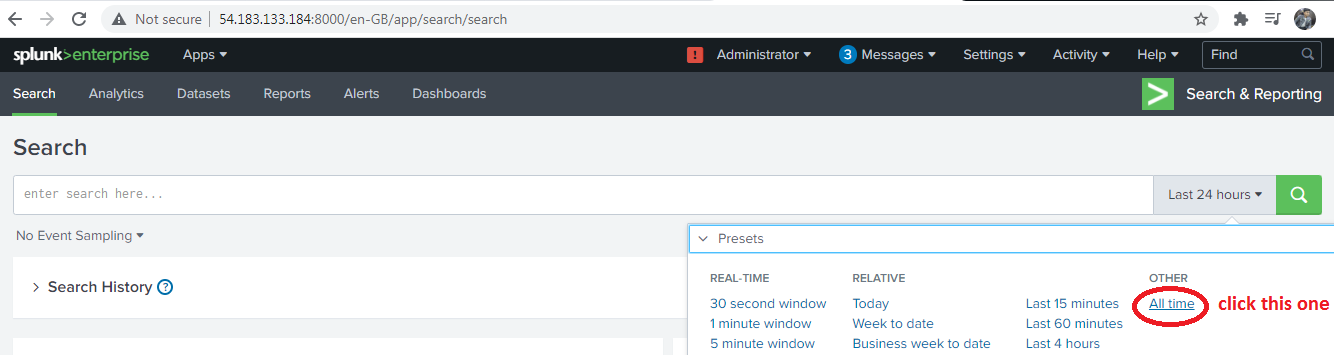
[**https://github.com/elastic/examples/blob/master/Common%20Data%20Formats/apache\_logs/apache\_logs**](https://github.com/elastic/examples/blob/master/Common%20Data%20Formats/apache_logs/apache_logs)

* **Place the Log file either in the universal log path called : /var/log/**

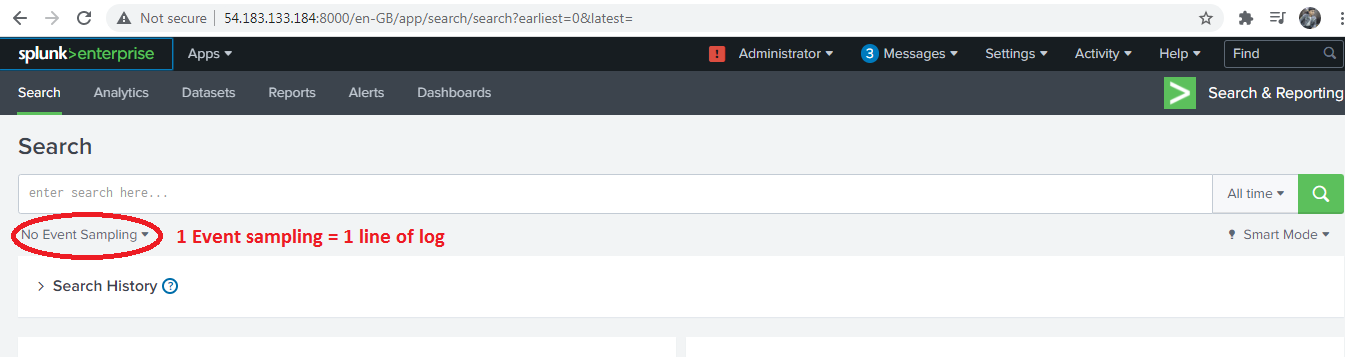
**Customizable log path:**

`

* **Navigate to All time option:**



* **1 Event Sampling is Equal to 1 line of log:**



* **Connect the Slave Machine Using winscp protocol:**

**Upload the sample syslogs to : /home/ec2-user**

**cd /var/log**

**cp /home/ec2-user/syslog .**

**inside bin**

**./splunk add monitor /var/log/syslog –index main**

**./splunk add monitor /var/log/applog –index main**

**./splunk add monitor /var/log/syslog -index new**

**index=”new”**

**index=”main” “dummy”**

**index=”main” host=”ip-172-31-1-21.ap-south-1.compute.internal” source=”/var/log/applog” sourcetype=applog presentations**

* **Connect the Slave Machine Using winscp protocol:**

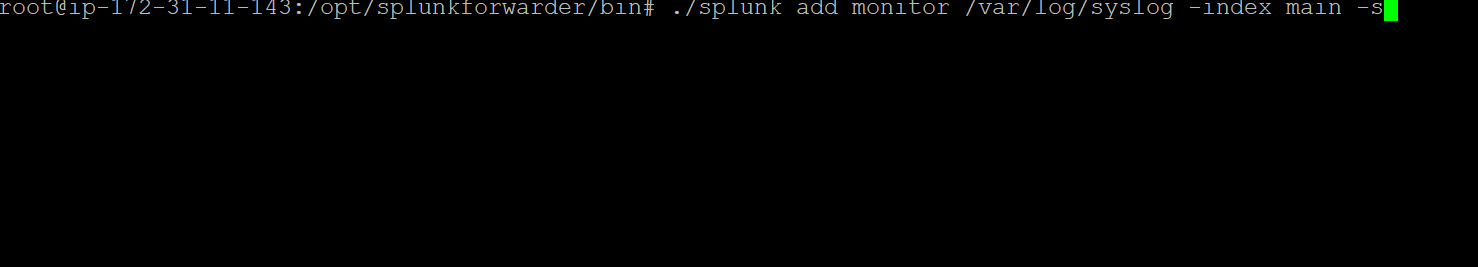
**Upload the sample syslogs to : /home/ec2-user**

**cd /var/log**

**cp /home/ec2-user/syslog .**

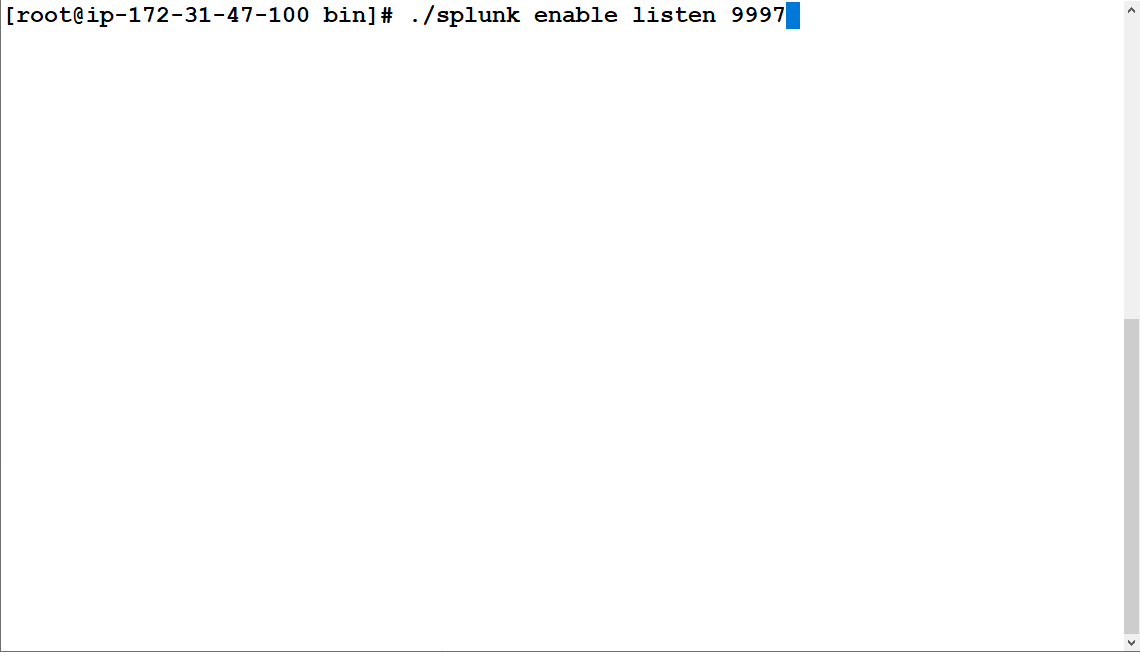
**inside bin**

**./splunk add monitor /var/log/syslog -index main -sourcetype slave1logs**



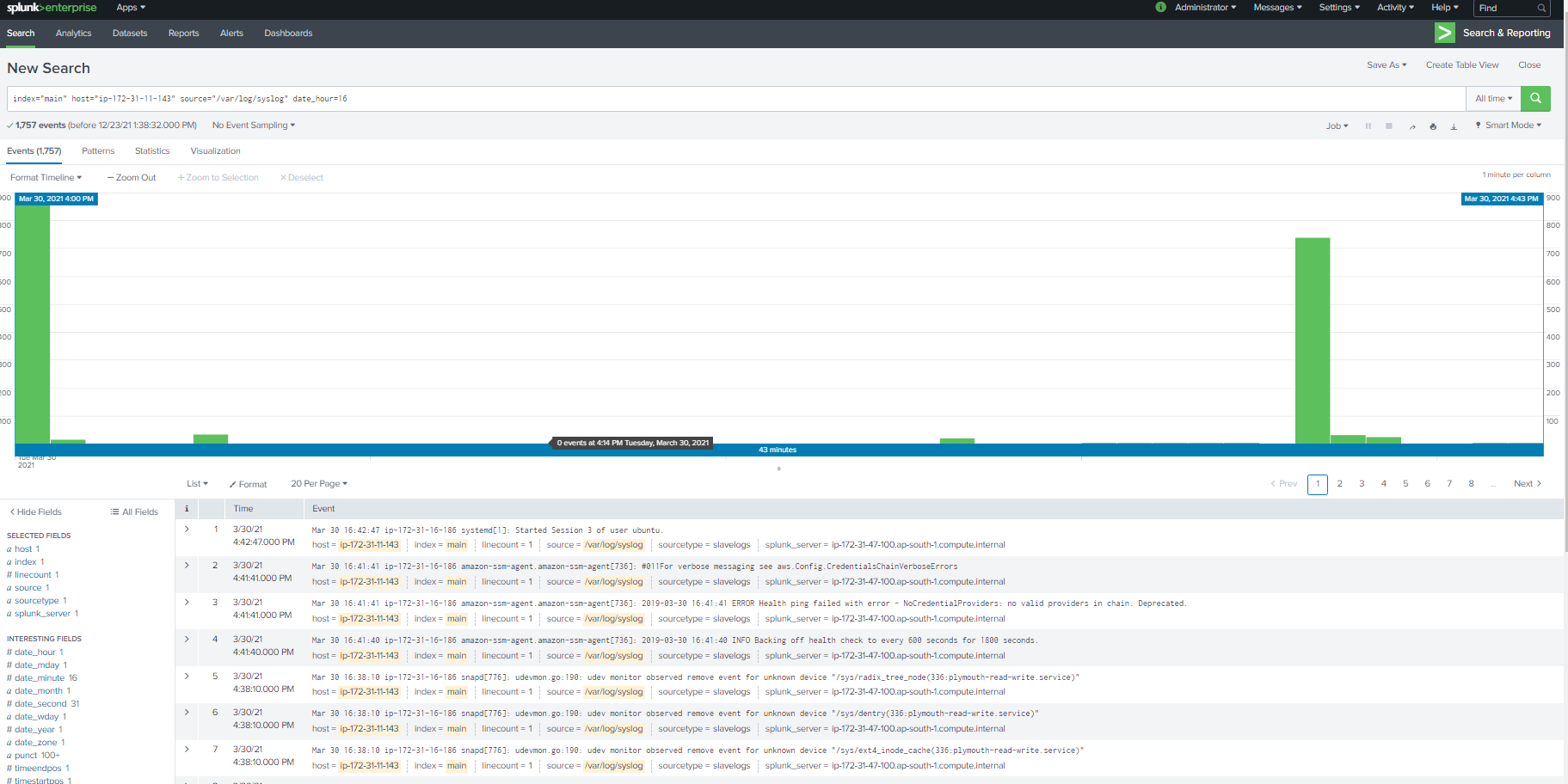
**In master Splunk**

**./splunk enable listen 9997**

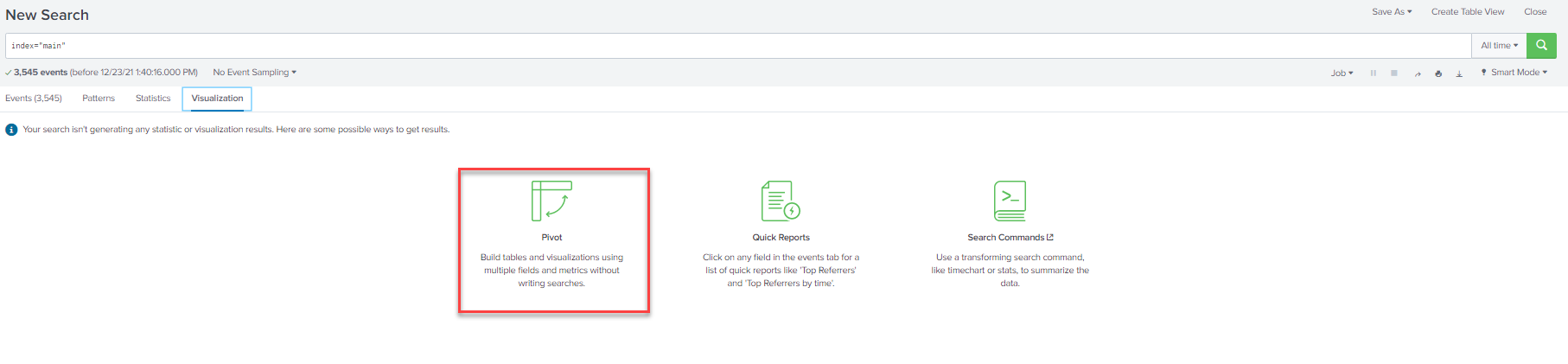


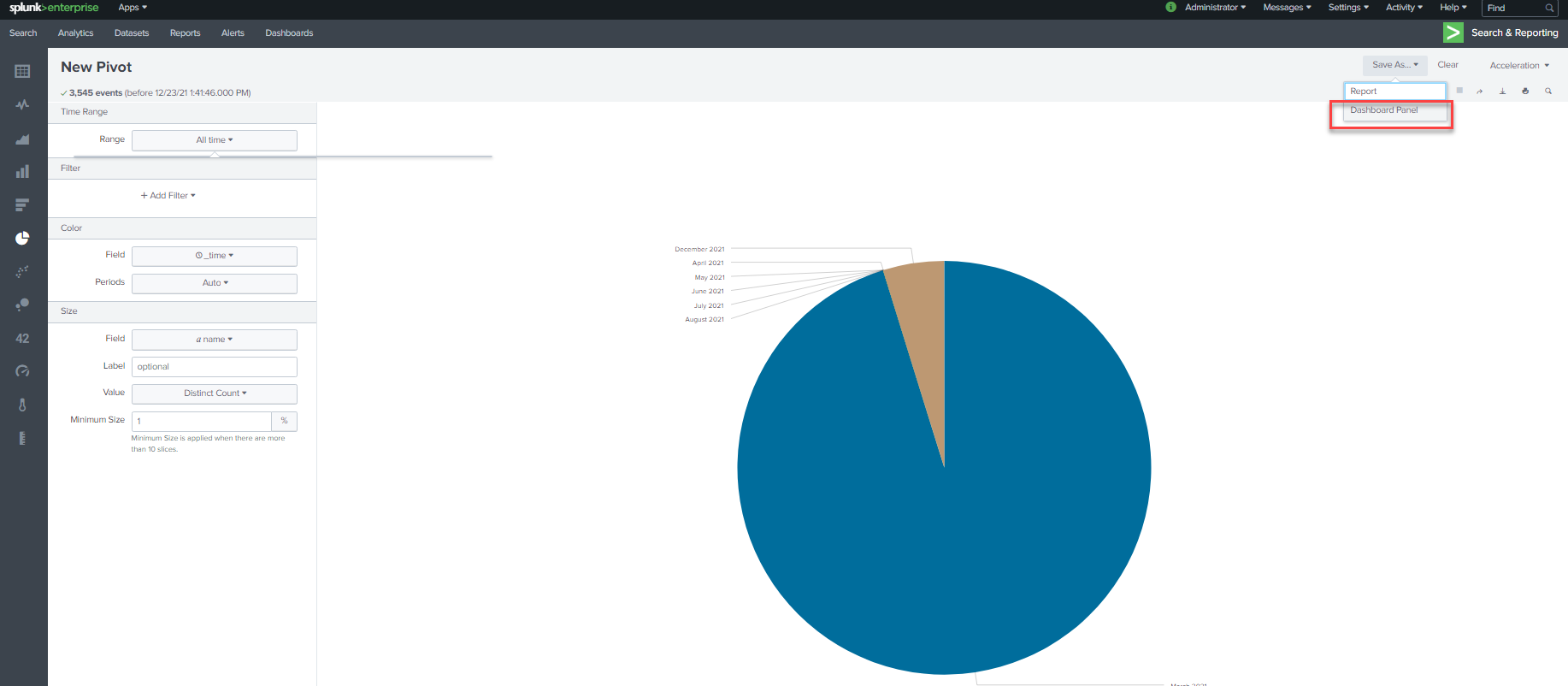
**Task:**

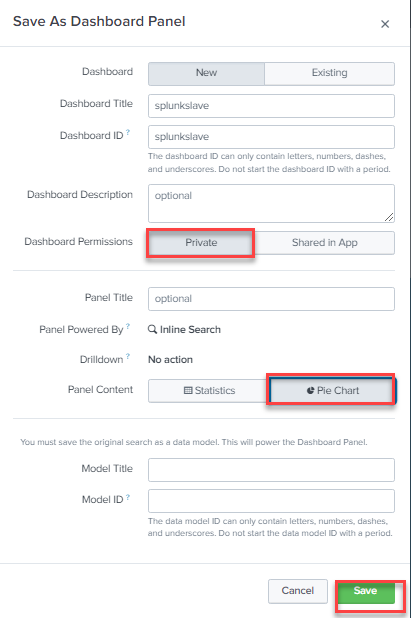
**index="main" host="ip-172-31-11-143" source="/var/log/syslog" date\_hour=16**



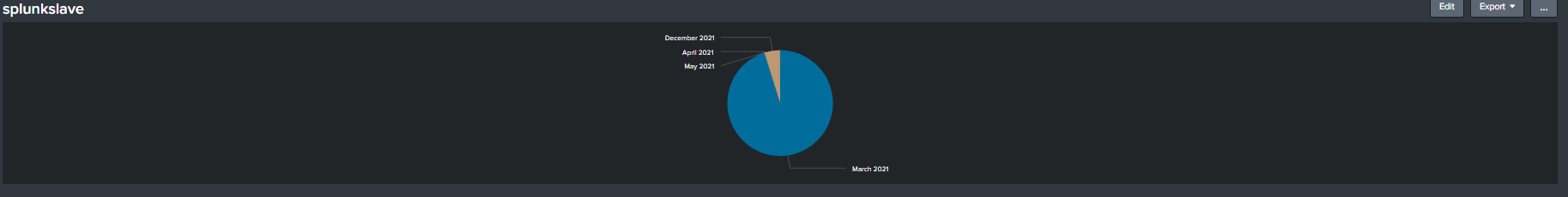
**Dashboard Creation:**







**Final output:**



**Troubleshooting for the error (The minimum free disk space (5000MB) error splunk)**

Follow the below youtube link : <https://www.youtube.com/watch?v=qg1dDczRl7I>