Index Page

|  |  |  |  |
| --- | --- | --- | --- |
| Name Of POC | Author | Date& Version | Tools used in POC |
| Splunk | Akshay Algeri | 17/03/2017 | Splunk |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Monitoring Tools**

Monitoring toolsare used to continuously keep track of the system status in order to have the earliest warning of failures, defects or problems and to improve them.

**Features or characteristics of monitoring tools are:**

* To identify the problems and send an alert message
* To log real-time information
* To monitor the number of users on a network
* To monitor network traffic

**SPLUNK**

Splunk is a software platform to search, analyze and visualize the machine generated data gathered from applications, network services and website logs. Splunk works on push mechanism.

Splunk is used to analyze the machine data. Machine data is nothing but the logs generated. Machine generated data is [information](https://en.wikipedia.org/wiki/Information) automatically generated by a [computer process](https://en.wikipedia.org/wiki/Computer_process), [application](https://en.wikipedia.org/wiki/Computer_application), or other mechanism without the active intervention of a human. Analyzing this large amount of data is very difficult manually because the data generated are unstructured. These data can be any data generated by network devices or websites logs.

These data are unstructured and very difficult to understand, here splunk does the work of analyzing this data.

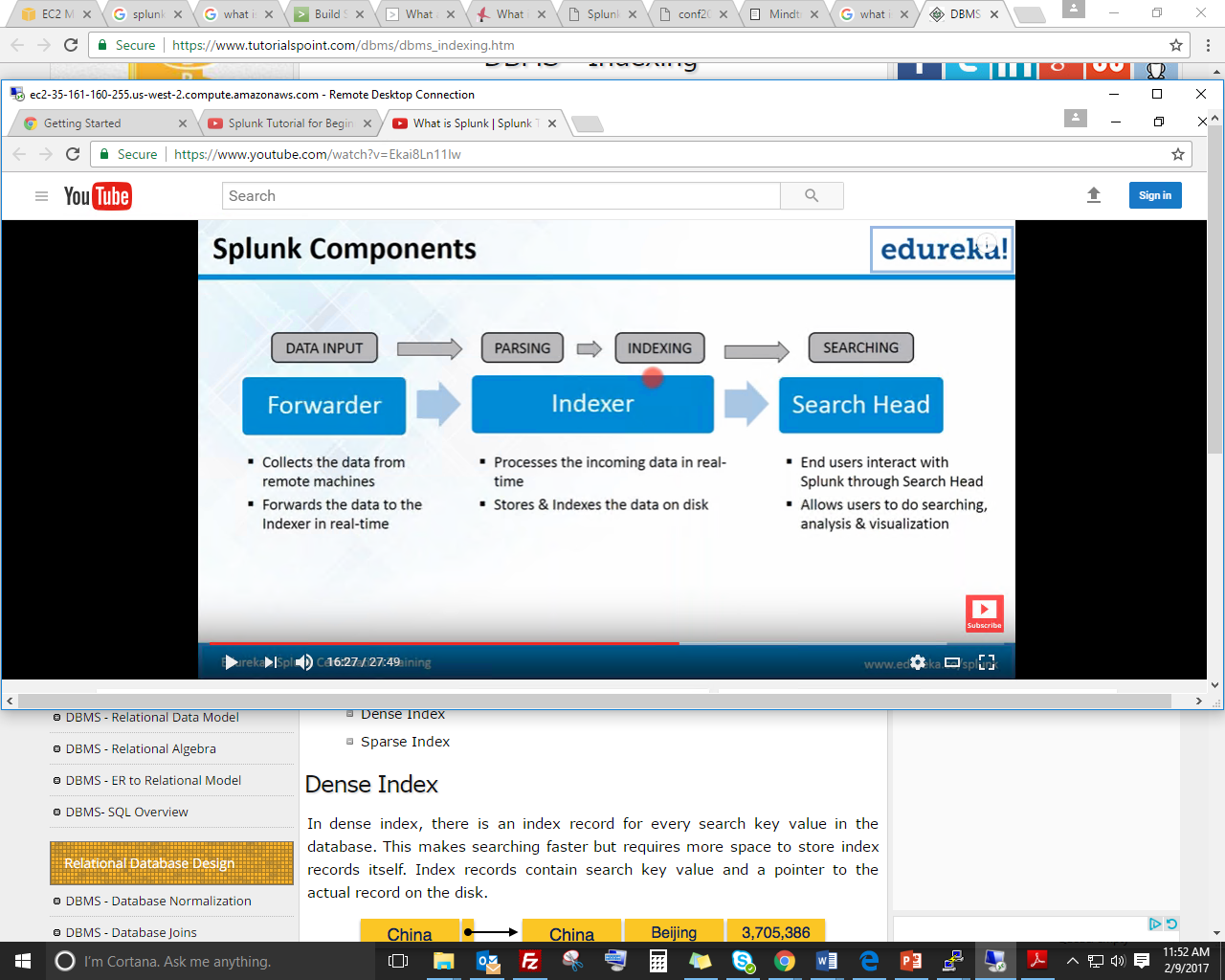
The data generated by the devices are fed to splunk it processes the data and extracts only the relevant information using which we can understand what the problems were. Using this data we can overcome the failure and we can create dashboards to visualize and analyze results. We can even store data for later use.

**ADVANATAGES:**

1. Splunk can collect data in real time from different machines
2. It can accept any datatype like .csv, or logfiles.
3. Splunk gives alerts notification.
4. Has large number of plugins for integration.
5. Splunk lite/ enterprise can be used for on premise setup
6. Splunk cloud can be used as SaaS setup.

Splunk clous is SaaS based setup which allows us to store, search, analyze machine-generated data collected from the websites, applications and so on. Splunk Cloud offers many of the features of Splunk Enterprise as a cloud service. You can use Splunk Cloud alone or with Splunk Enterprise on-premises software as a hybrid solution. Splunk Cloud deployments are continuously monitored and managed by the Splunk Cloud Operations team.

**Working of splunk**



**It consists of 3 components:**

1. **Forwarder**: It collects data from different sorces. We need to install forwarders on different machines which generates machine and then we can forward this data to splunk server for analyzing.
   * *There are two types of splunk forwarder*   
            a) universal forwarder(UF) -Splunk  agent installed on non-Splunk system to gather data locally, can’t parse or index  data  
            b) Heavy weight forwarder(HWF) - full instance of splunk with advance functionality as below.Generally works as a remote collector, intermediate forwarder, and possible data filter because they parse data, they  are not recommended for production systems
2. **Indexer**: This performs the task of indexing the data. Once the data is collected processes the data and removes the irrelevant or junk data and indexes the required data.

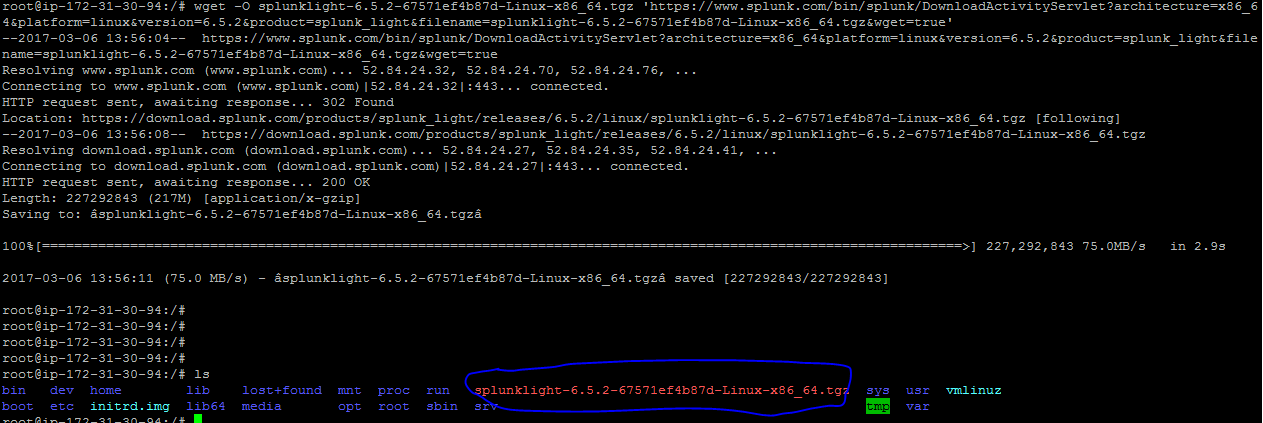
When you add data to Splunk, Splunk processes it, breaking the data into individual events, timestamps the events, and stores them in an index so that the data can be searched and analyzed later. By default, data you feed to Splunk is stored in the main index, but you can create and specify other indexes for Splunk to use for different data inputs.

1. **Search Head**: It provides visualization to search the data. In a distributed search environment, search head is the Splunk instance that directs search requests to a set of search peers and merges the results back to the user.

**Splunk Installation on Linux:**

**Step 1**: Download splunklight (targz file) using wget

wget -O splunklight-6.5.2-67571ef4b87d-Linux-x86\_64.tgz 'https://www.splunk.com/bin/splunk/DownloadActivityServlet?architecture=x86\_64&platform=linux&version=6.5.2&product=splunk\_light&filename=splunklight-6.5.2-67571ef4b87d-Linux-x86\_64.tgz&wget=true'



**Step 2**: Untar the file and install it under required directory

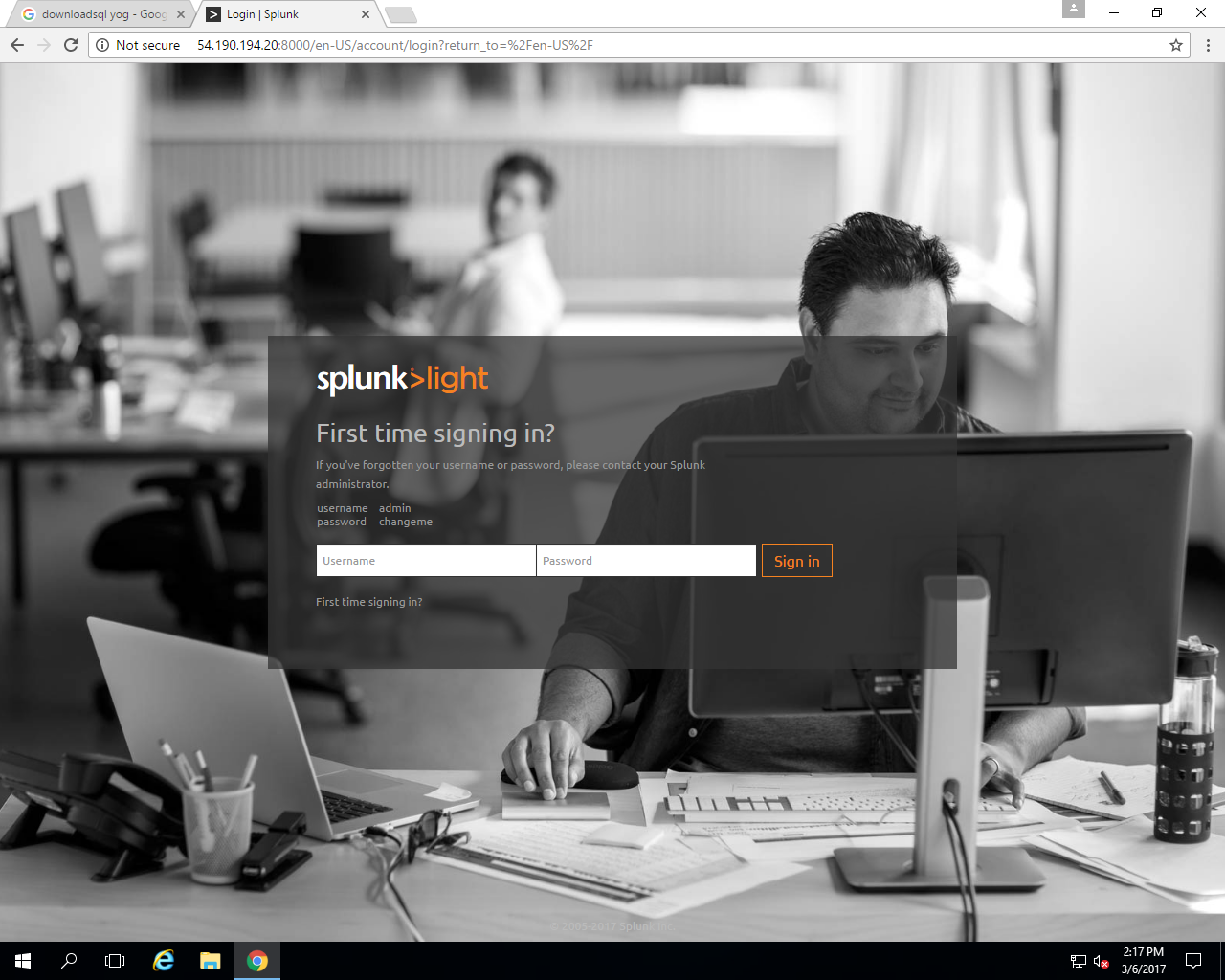
**Step 3**: start the splunk light

Goto bin directory and start the splunk by using command ./splunk start



**Step 4**: open the splunk web interface with *ip:8000* as port number

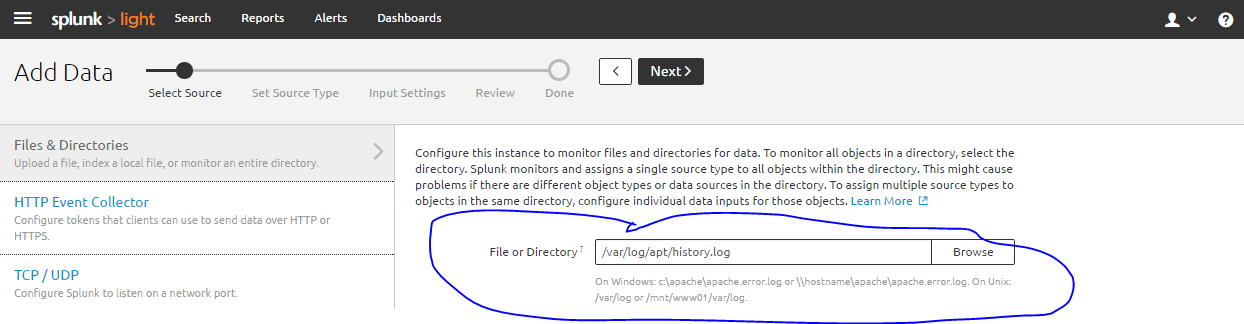
*Login by entering the default credentials*.



**Adding data to splunk from the local system(machine on which splunk is installed)**

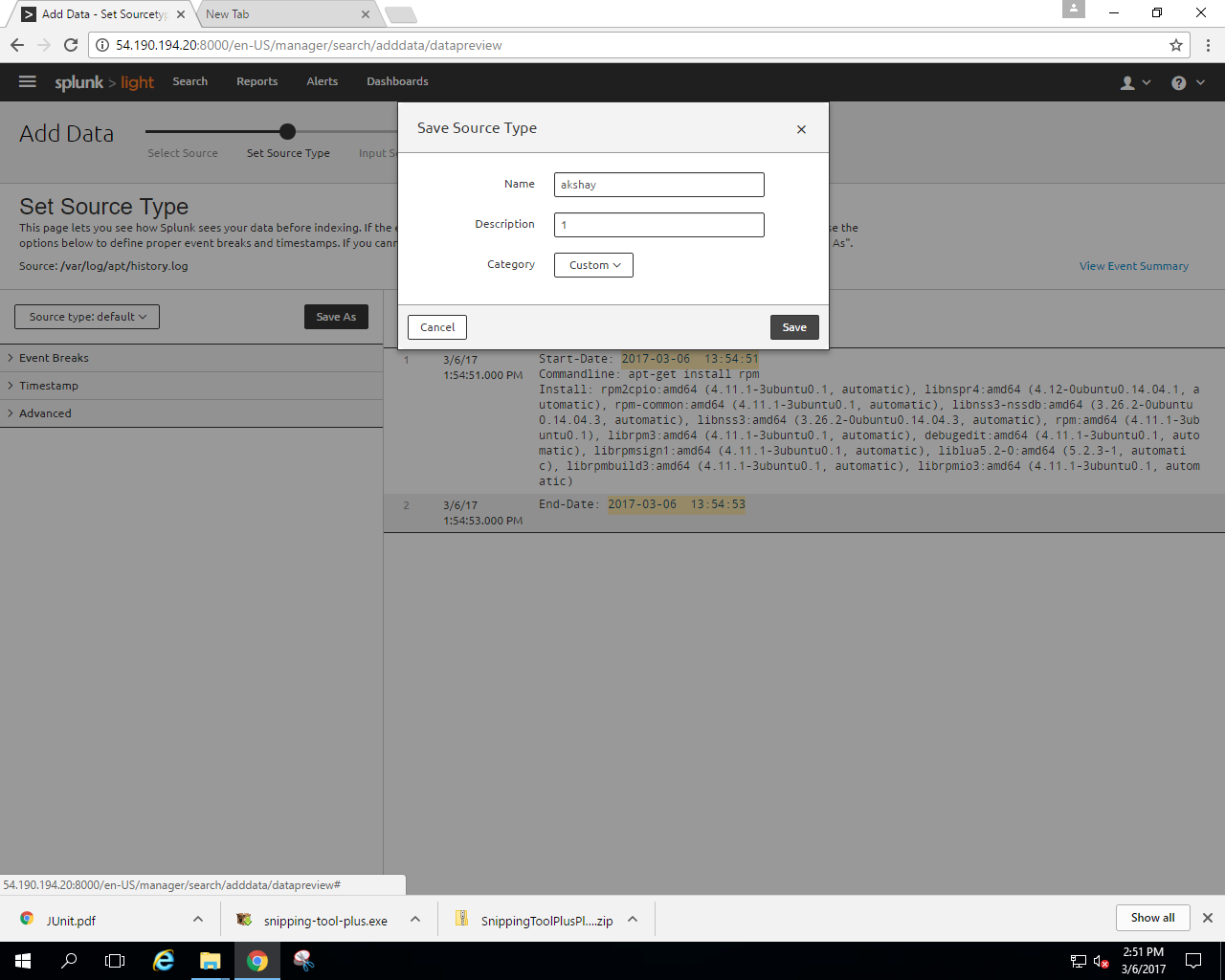
* We can add log files from our instance to splunk for monitoring purpose.

Goto add data-> and select the appropriate file from the directory



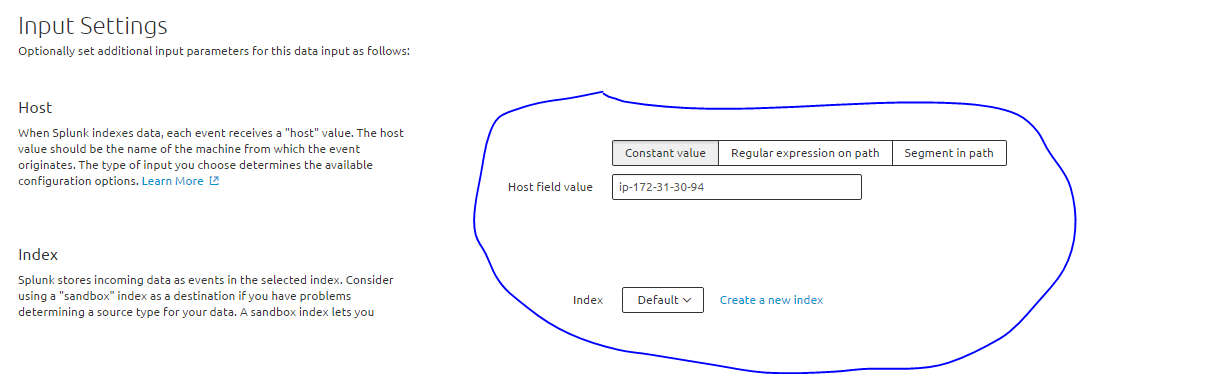
* Select the sourcetype:

Source is name of the file, directory or other input from which a particular log originates.

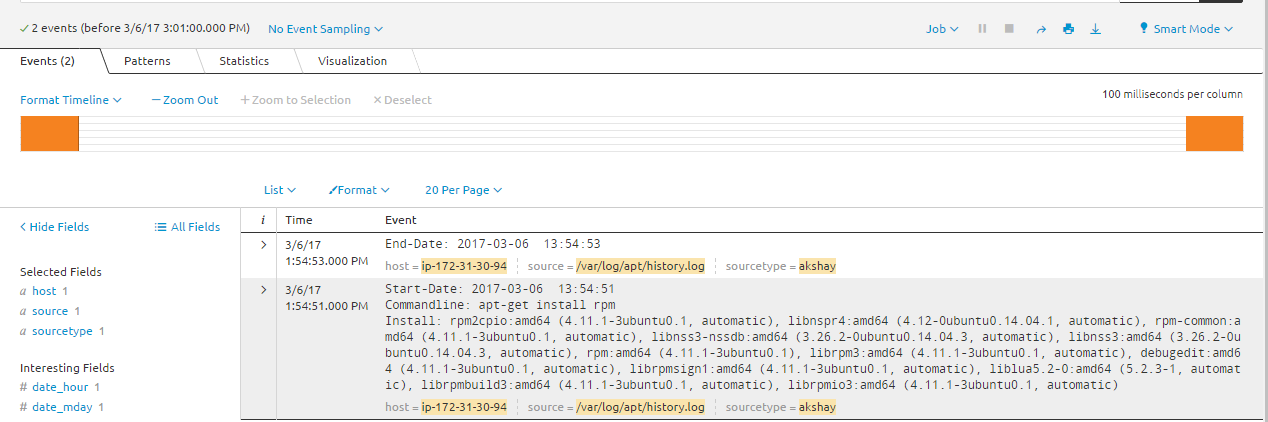


We can even create our own sourcetype,

* Next we need to set the index so that the data that is given as input will be stored under that index. By default there will be 3 index created. We can even create our own index.
* A host is the name of the physical device where an event originates. The host field provides an easy way to find all data originating from a specific device.



* Finally we can preview our logs

we can even observe the graphical representation of logs.

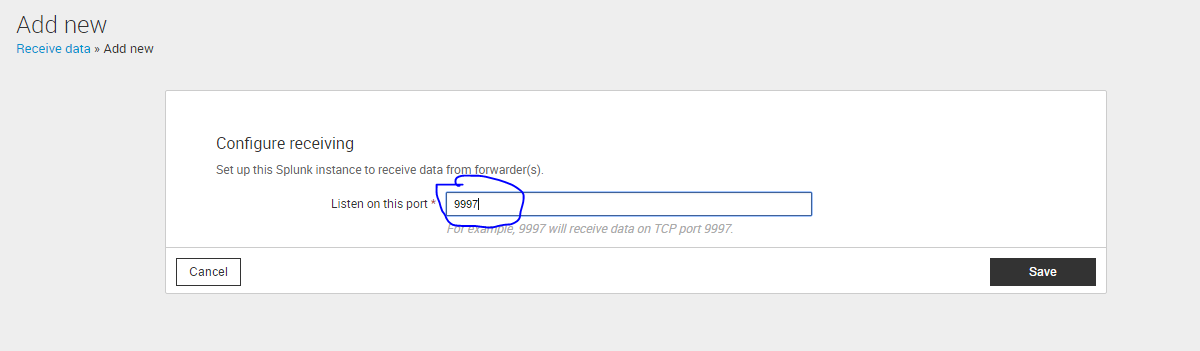
**Adding data to splunk from the remote system(using universal forwarder)**

In order to collect data logs from other system we need to install splunk universal forwarder forwarder on the system from which the data needs to be collected. Splunk forwarder helps to collect the data from the system and send it to splunk server for analyzing. The universal forwarder is a separate Splunk software which needs to be installed and configured to collect data from a remote system.

**Steps followed to get data into Splunk Light:**

**Step 1:** First we need to configure splunk light server so that it can accept data from forwarders. For this we need to use add port 9997 on server

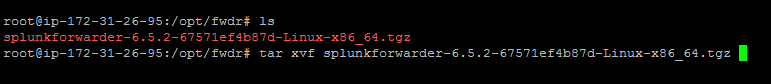
* Goto menu->data receiving-> configure receiving

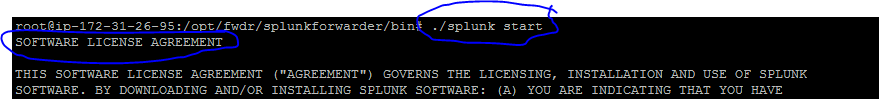


* Add port number 9997 and save it.

**Step 2:** Download and install splunk forwarder on the remote instance.

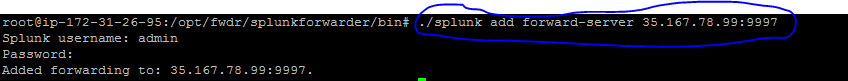
wget -O splunkforwarder-6.5.2-67571ef4b87d-Linux-x86\_64.tgz 'https://www.splunk.com/bin/splunk/DownloadActivityServlet?architecture=x86\_64&platform=linux&version=6.5.2&product=universalforwarder&filename=splunkforwarder-6.5.2-67571ef4b87d-Linux-x86\_64.tgz&wget=true'

**Step 3:** untar the tar file

* Goto bin directory under splunkforwarder and start the splunk using. /*splunk start* moving forward it will ask to accept the licence.

**Step 4:** Configure splunk forwarder to send data to splunk light.

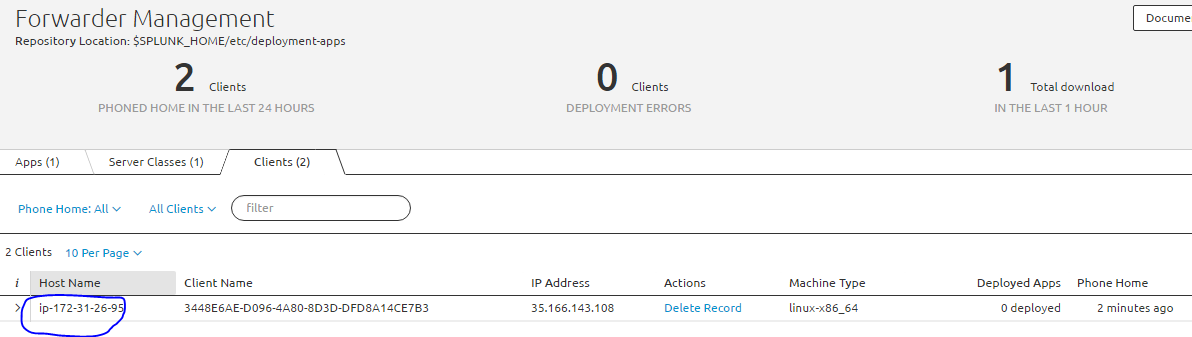
* Goto bin directory under splunkforwarder
* ./splunk add forward-server hostname:9997
* Hostname =ip address of splunk server

(by default password:changeme)

**Step 5:** Configure forwarder as deployment client.

* **.**/splunk set deploy-poll *ip(server):*8089
* Restart splunk using *./splunk restart*

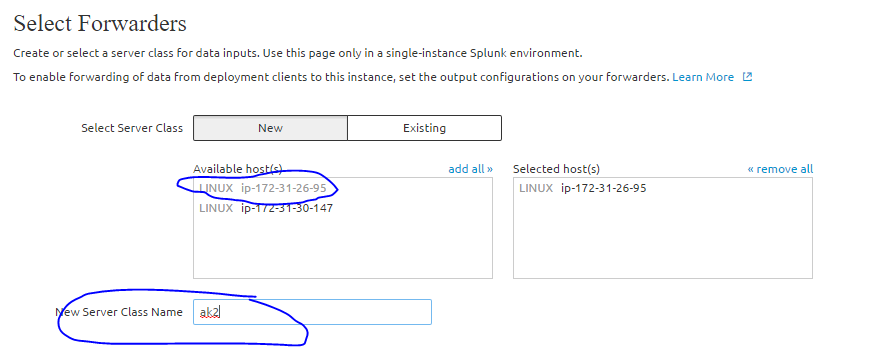
**Step 6:** Check whether client has been configured properly or not.

* Goto forwarder management in splunk server UI, check whether the forwarder installed on client is visible or not.

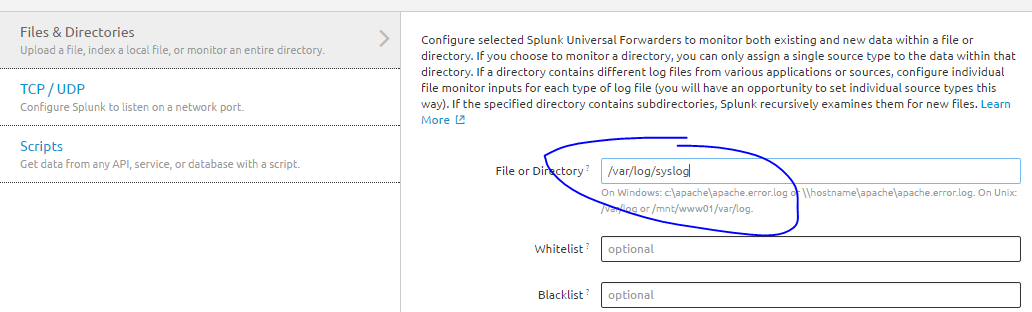
**Step 7:**  Add data to server from client

* 1. Click search on menu bar then you will find add data button, click on it.
  2. Select the the option as forwarding.
  3. Select the host from which you need to collect data.
  4. Create a server class when asked.

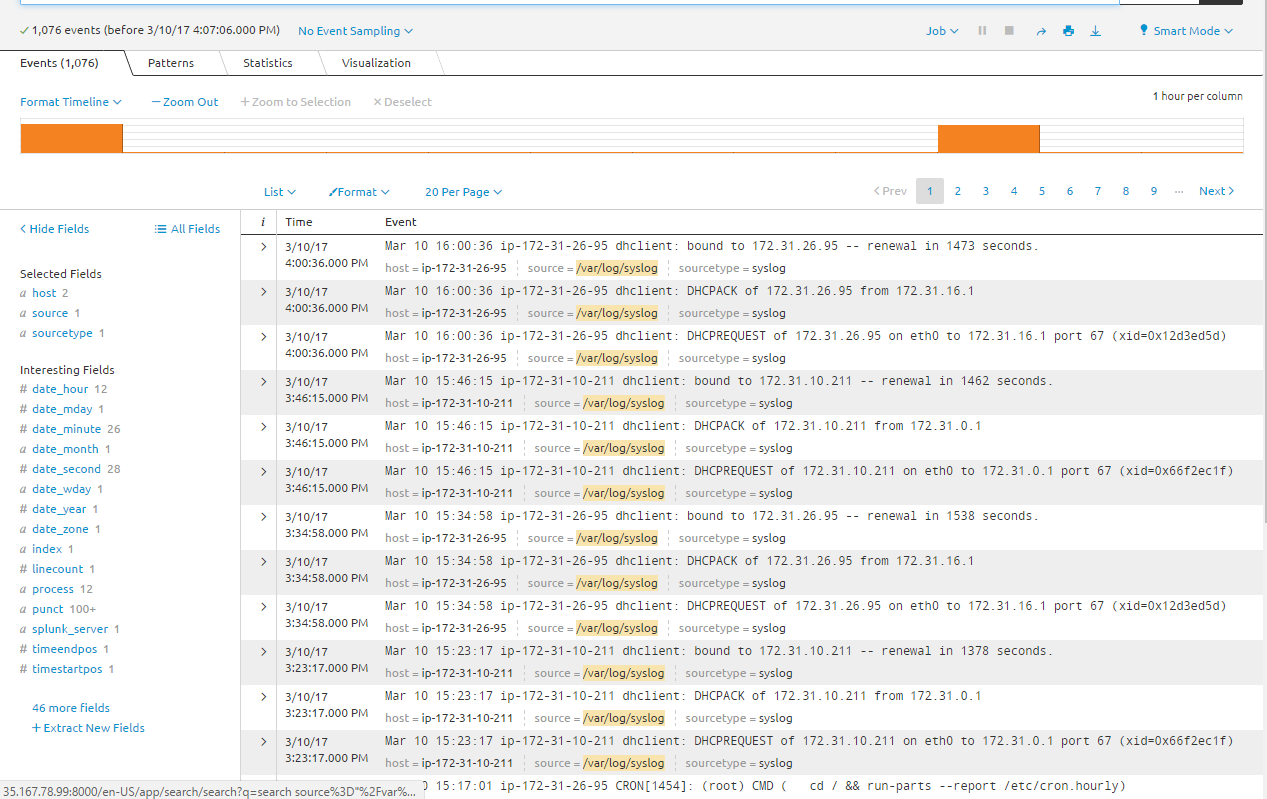
(Deployment clients can be grouped together into one or more server classes)



* 1. Enter the path for the log file and click next.



* 1. Select the index in which you want to index the data or create your new index.
  2. Review your data



We can even store the data to dashboard where we can view the logs.

Goto save option under that select dashboard option. Create a new dashboard if required..

