**Installation Steps for Splunk**

Below are the steps connection between SplunkIndexer and Splunk forwarder

* I am using Splunk Indexer and Splunk Searchehad as same componenet in
* Download the latest Enterprise tar file which will act as Splunk indexer and searchhead.
* Execute the command below to extract the tar file

[root@d3d855989802 splunk]# tar xvzf splunk-7.1.3-51d9cac7b837-Linux-x86\_64.tgz -C /opt/splunk

* To start splunk in your terminal

splunk/bin/splunk start --accept-license

* To enable splunk at boot time

[root@d3d855989802 splunk]# splunk/bin/splunk enable boot-start

* check the splunk is enable or not

[root@d3d855989802 splunk]# ls -lrt /etc/init.d/splunk

-rwx------. 1 root root 995 Oct 27 00:21 /etc/init.d/splunk

**Installation of Universal forwarder**

* Download the executable for splunk forwarder from splunk site (**Note:** *splunk Enterprise is used for indexer , searchhead, Deployment server, ect. there is different executable for splunk forwarder*)
* Execute the below command in other box for universal forwarder

tar xvzf splunkforwarder-7.2.0-8c86330ac18-Linux-x86\_64.tgz -C /opt/splunk

[root@39aa82e63c03 splunkforwarder]# ls -lrt

total 128

-r--r--r--. 1 10777 10777 63711 Sep 28 17:04 license-eula.txt

-r--r--r--. 1 10777 10777 57 Sep 28 17:04 copyright.txt

-r--r--r--. 1 10777 10777 846 Sep 28 17:07 README-splunk.txt

drwxr-xr-x. 3 10777 10777 41 Sep 28 17:30 share

drwxr-xr-x. 3 10777 10777 58 Sep 28 17:30 openssl

drwxr-xr-x. 2 10777 10777 27 Sep 28 17:30 include

-rw-r--r--. 1 10777 10777 0 Sep 28 17:30 ftr

drwxr-xr-x. 13 10777 10777 4096 Sep 28 17:30 etc

drwxr-xr-x. 5 10777 10777 4096 Sep 28 18:00 lib

drwxr-xr-x. 3 10777 10777 4096 Sep 28 18:00 bin

-r--r--r--. 1 10777 10777 40974 Sep 28 18:00 splunkforwarder-7.2.0-8c86330ac18-linux-2.6-x86\_64-manifest

[root@39aa82e63c03 splunkforwarder]# pwd

/opt/splunk/splunkforwarder

* Accept the lience while starting the splunk forwarder

[root@39aa82e63c03 splunkforwarder]# bin/splunk start --accept-license

* Create a new app . Create the below directory under
* SPLUNK\_HOME/etc/app/
* <testapp>/local/input.conf (This file contains possible settings you can use to configure inputs,distributed inputs such as forwarders, and file system monitoring in inputs.conf.)
* Configure the universal forwarder to connect to a receiving indexer by the below command. BY default it listen to 9777 port. So we can configure with 9777 on it

[root@39aa82e63c03 bin]# ./splunk add forward-server 172.17.0.2:9997

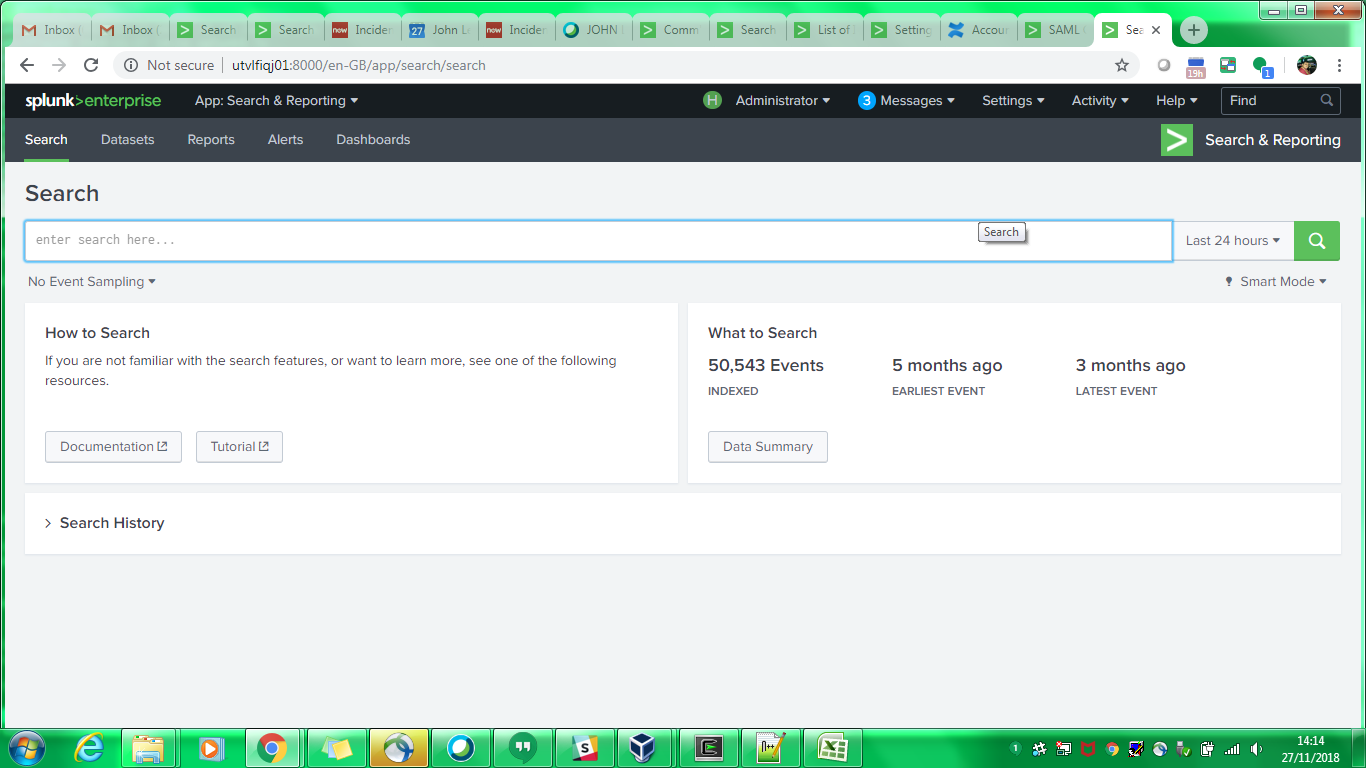
Splunk username: <splunkforwarder\_username>

Password:

Added forwarding to: 172.17.0.2:9997.

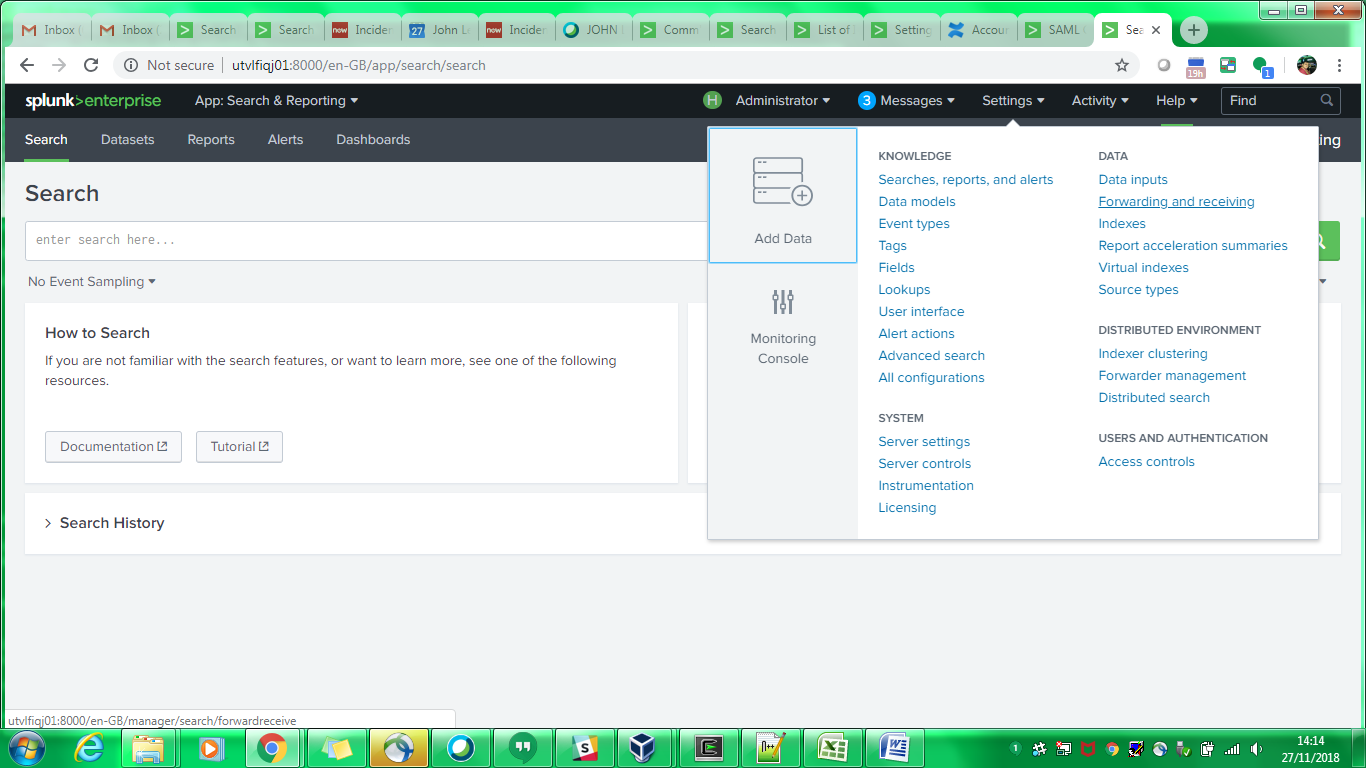
**Configure the port at the Indexer side**

* Configure the port at Splunk Enterprise at Indexer from GUI. Below are the steps
* Open the Splunk Enterprise Dashboard.



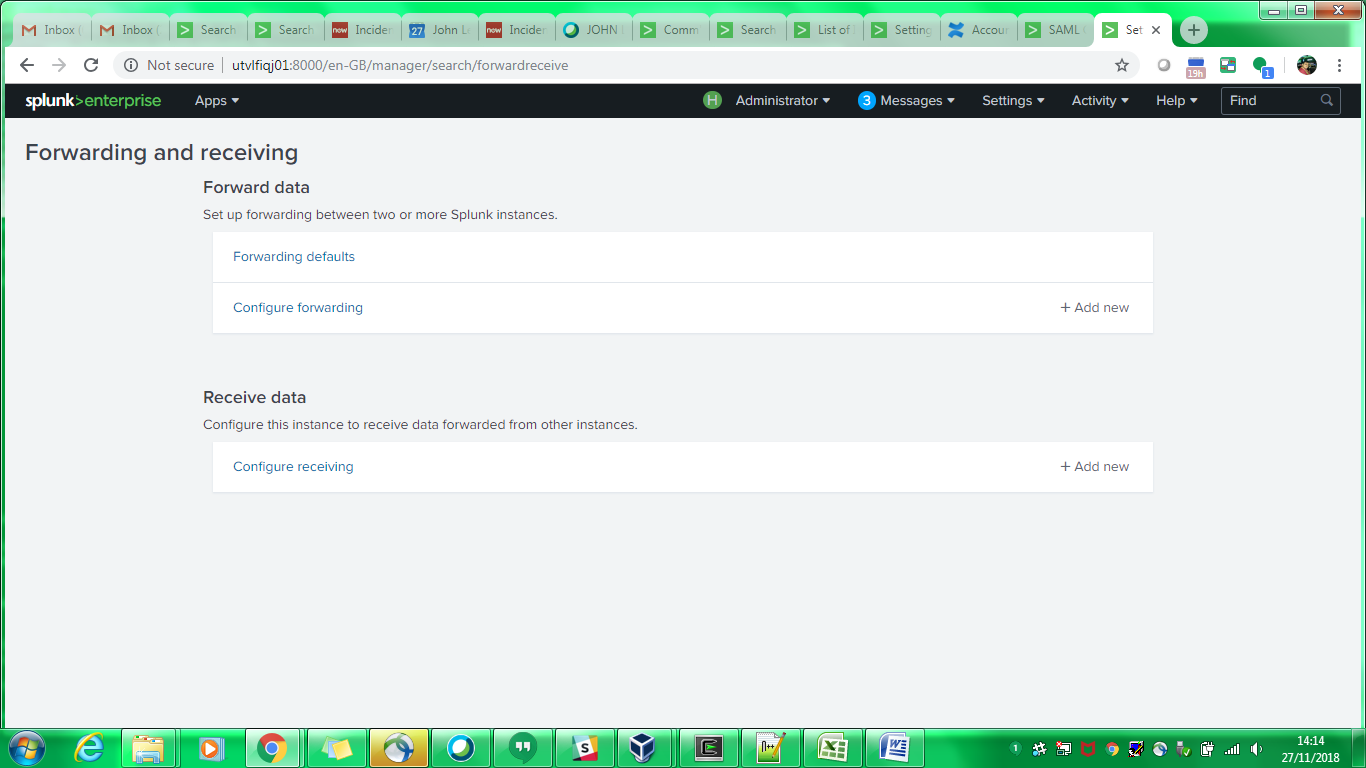
*Fig. 1*

* Click on the “**Setting** > **Forwarding and receiving**” as shown in below Fig.2



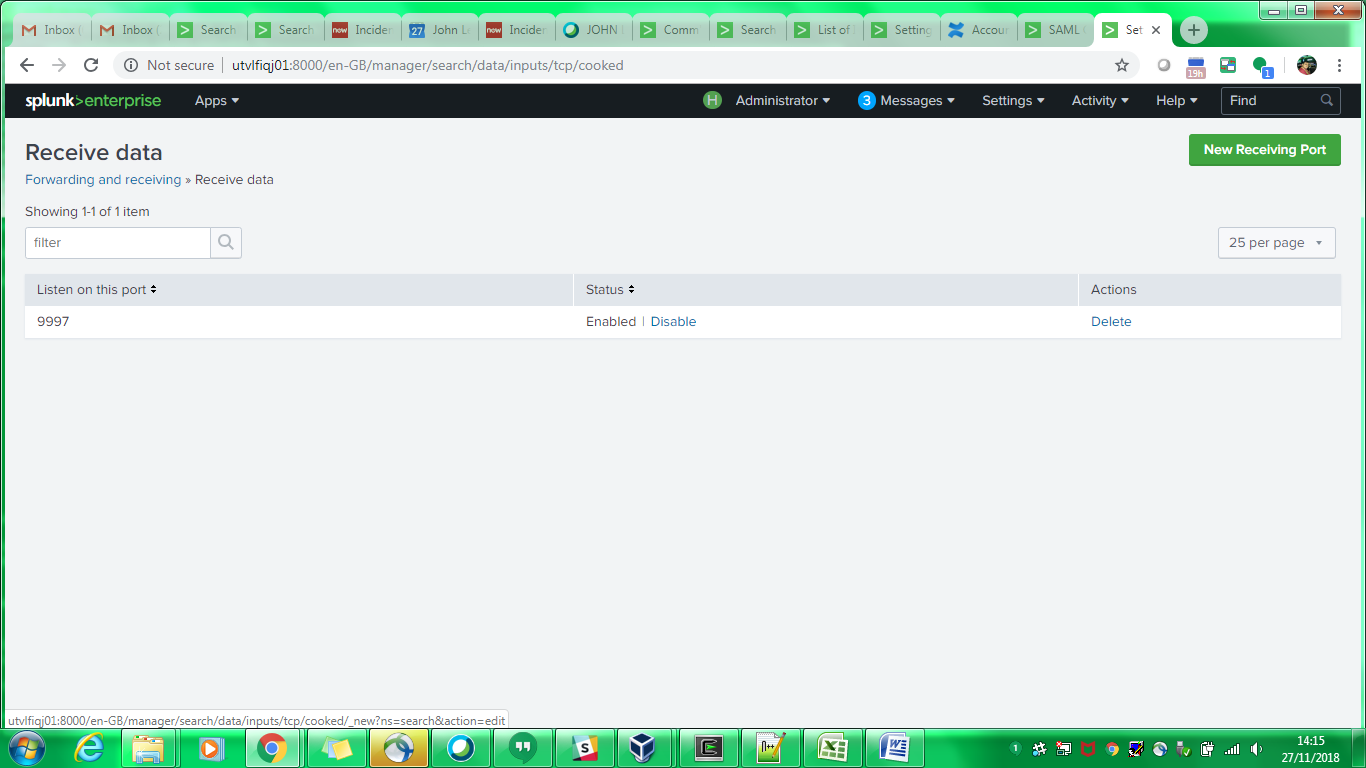
*Fig. 2*

* You will be reverted to Forwarding and receiving page and you have to Click the “**Configure receiving**”

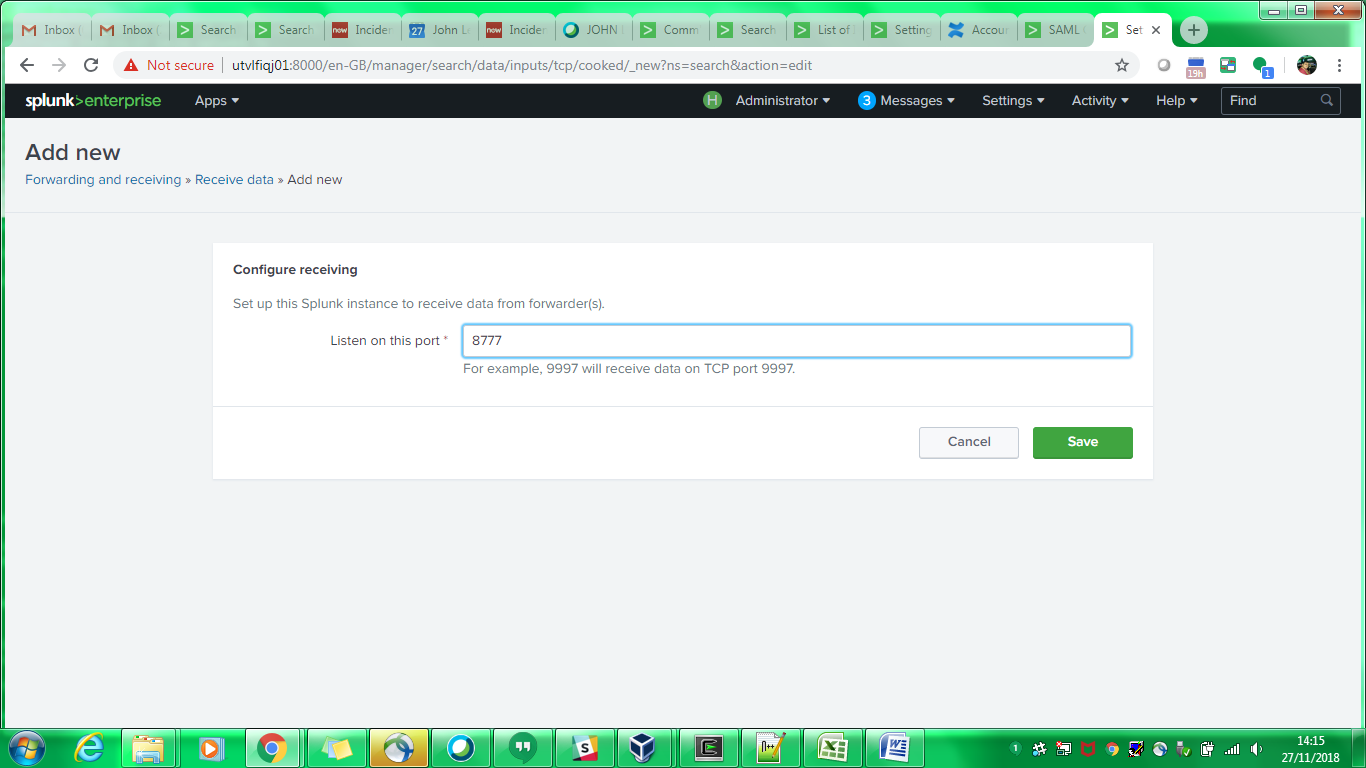


*Fig. 3*

* After Clicking the option you will be landed to below page and Click “**New Receiving Port**” to configure with port that will communicate with Splunk forwarder. Below are Figs that show how to configure the port. (By default 9997 can be configure)



*Fig. 4*



*Fig. 5*

**How to configure the input.conf in Universal forwarder to index the data.**

* As shown above the input.conf is created under the new app. Add the below stanza input.conf to monitor the files.

[root@39aa82e63c03 local]# pwd

/opt/splunk/splunkforwarder/etc/apps/testapp/local

[root@39aa82e63c03 local]# ls -lrt

total 4

-rw-r--r--. 1 root root 486 Oct 31 12:47 inputs.conf

[root@39aa82e63c03 local]#

* Add the stanza in the input.conf file

[root@39aa82e63c03 local]# cat inputs.conf

[monitor:///opt/splunk/logs/test.txt]

disabled = 0

sourcetype = test\_data

index = testdata

[monitor:///opt/splunk/logs/test.txt]

disabled = false

sourcetype = test\_data

index = testdata1

[monitor:///opt/splunk/logs/test.log]

disabled = false

sourcetype = test\_data

index = testdata1

[monitor:///opt/splunk/logs/www1/secure.log]

disabled = false

sourcetype = secure\_log

index = www1

[monitor:///opt/splunk/logs/www3/\*.log]

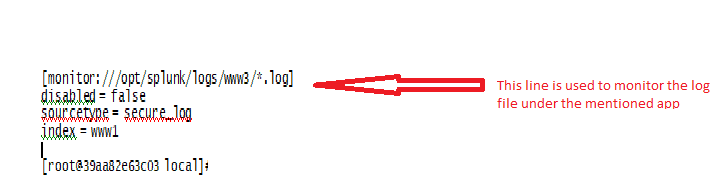
disabled = false

sourcetype = secure\_log

index = www1

[root@39aa82e63c03 local]#

In the above input.conf file is configure the above file



*Fig. 6*

These files paths are configured as of the path in your splunk universal forwarder. Splunk Universal Forwarder will act as application box from where you can point files to monitor which log files you want to monitor.

* You can see the below is the log file path in the same forwarder

[root@39aa82e63c03 logs]# ls -lrt

total 8

-rwxr-xr-x. 1 root root 130 Oct 28 05:13 test.log

drwxr-xr-x. 2 root root 42 Oct 29 07:15 www1

drwxr-xr-x. 2 root root 42 Oct 29 07:15 www3

drwxr-xr-x. 2 root root 30 Oct 29 07:15 vendor\_sales

drwxr-xr-x. 2 root root 42 Oct 29 07:15 www2

drwxr-xr-x. 2 root root 24 Oct 29 07:15 mailsv

-rwxr-xr-x. 1 root root 151 Oct 31 14:45 test.txt

[root@39aa82e63c03 logs]# pwd

/opt/splunk/logs

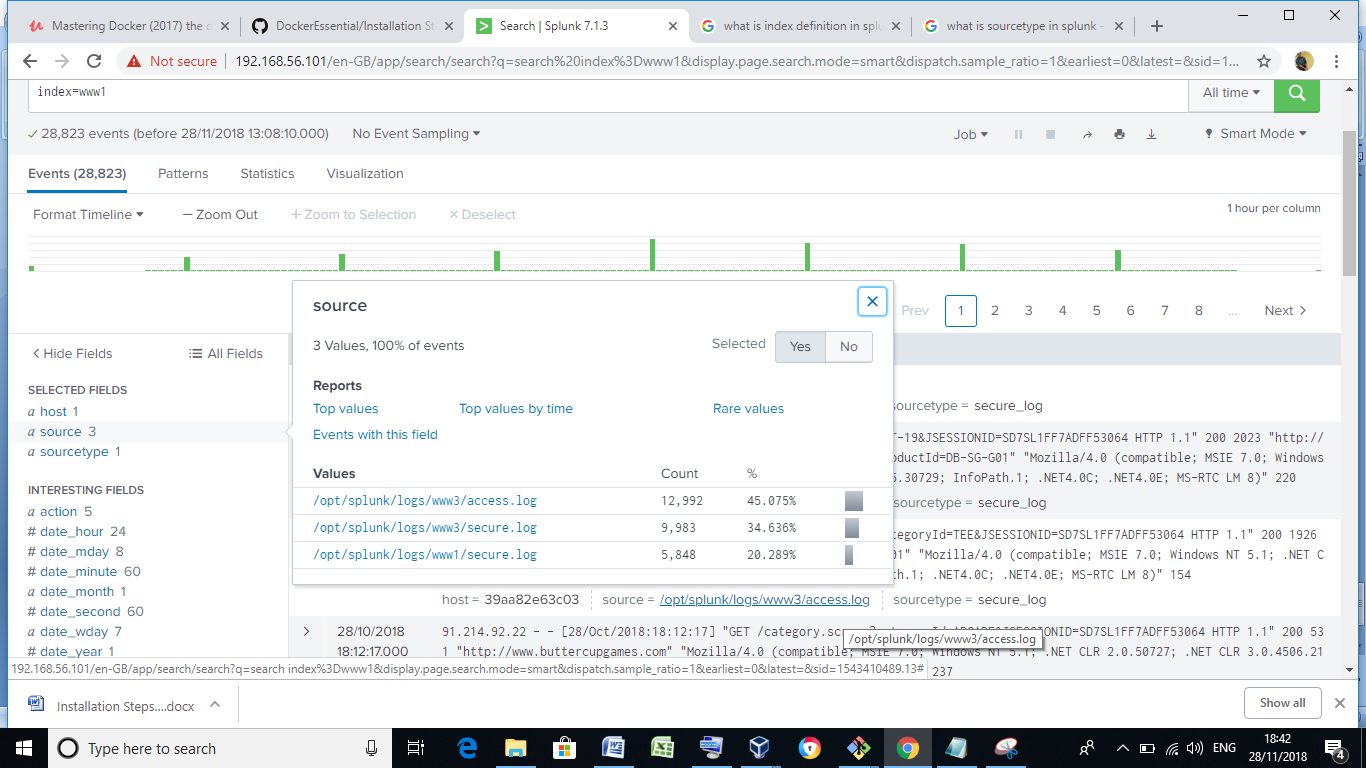
[root@39aa82e63c03 logs]#

* Below are some description about index and sourcetype.

**Index**: *The repository for data. When the Splunk platform indexes raw data, it transforms the data into searchable events. Indexes reside in flat files on the indexer.*

**Sourcetype**: *A default field that identifies the data structure of an event. A source typedetermines how Splunk Enterprise formats the data during the indexing process.The indexer identifies and adds the source type field when it indexes the data. As a result, each indexed event has a sourcetype field.*

See below Fig. 7, how we can see the data for index www1 in our UI.



*Fig.7*

So against index www1 we have 3 log files to be monitor.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

The above are the basic of how to use splunk and how to forward data to searchhead.

This was implantation was mainly done for getting splunk use as a container. I have use splunk in docker container. We can spin up container with splunk install in it from splunk image.

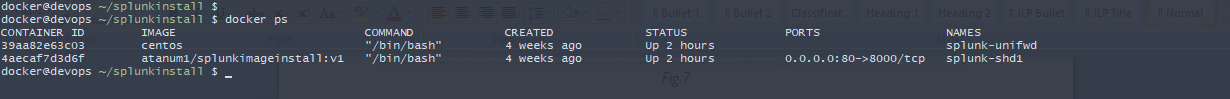
docker@devops ~/splunkinstall $ docker ps

CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES

39aa82e63c03 centos "/bin/bash" 4 weeks ago Up 2 hours splunk-unifwd

4aecaf7d3d6f atanum1/splunkimageinstall:v1 "/bin/bash" 4 weeks ago Up 2 hours 0.0.0.0:80->8000/tcp splunk-shd1

docker@devops ~/splunkinstall $



docker@devops ~/splunkinstall $ docker images

REPOSITORY TAG IMAGE ID CREATED SIZE

demo latest 496083bd3bc9 3 weeks ago 2.05GB

atanum1/splunkinstall v7 8bc0a5f80195 3 weeks ago 2.19GB

atanum1/splunkinstall v6 2f60969862f1 3 weeks ago 2.19GB

atanum1/splunkimageinstall v1 3ff6cd0e3991 4 weeks ago 2.19GB

docker@devops ~/splunkinstall $ ^C