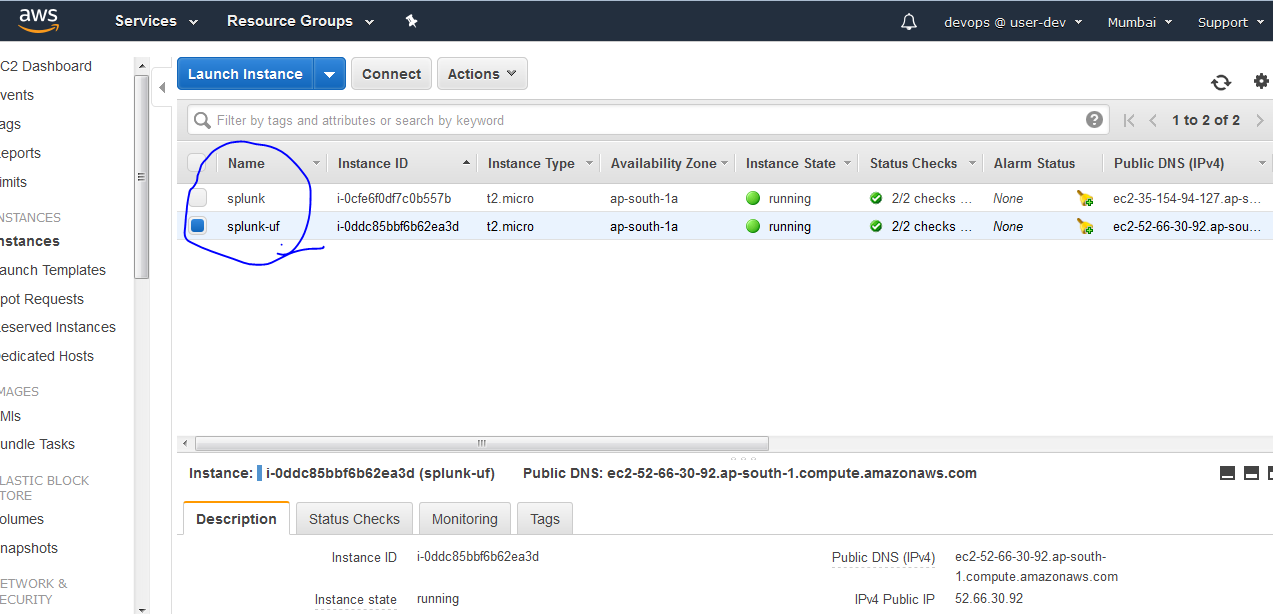
--- launch two instances

1.splunk-cluster master,sg:ssh-22-anywhere,tcp-9997,tcp-8000

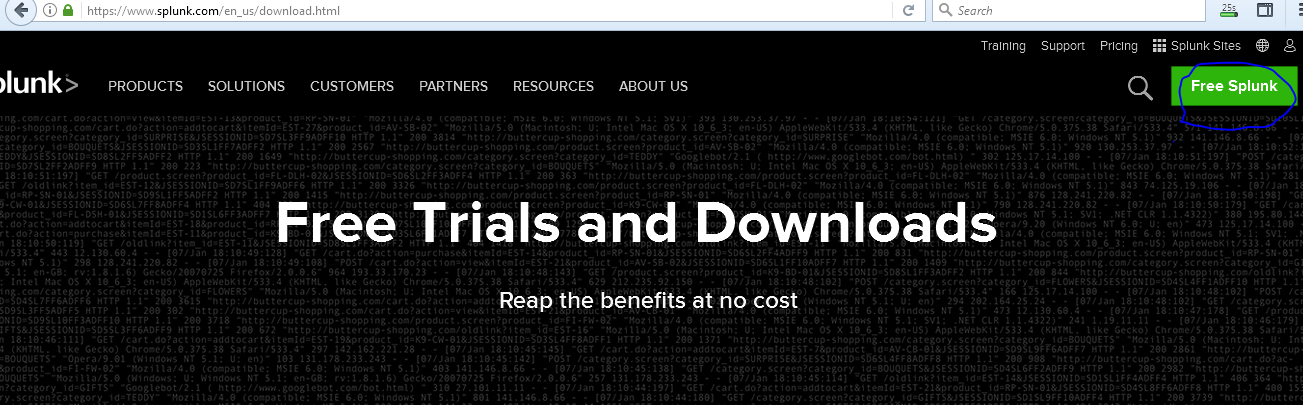
2. universal forwarder sg:ssh-22-anywhere,tcp-9997,tcp-8000

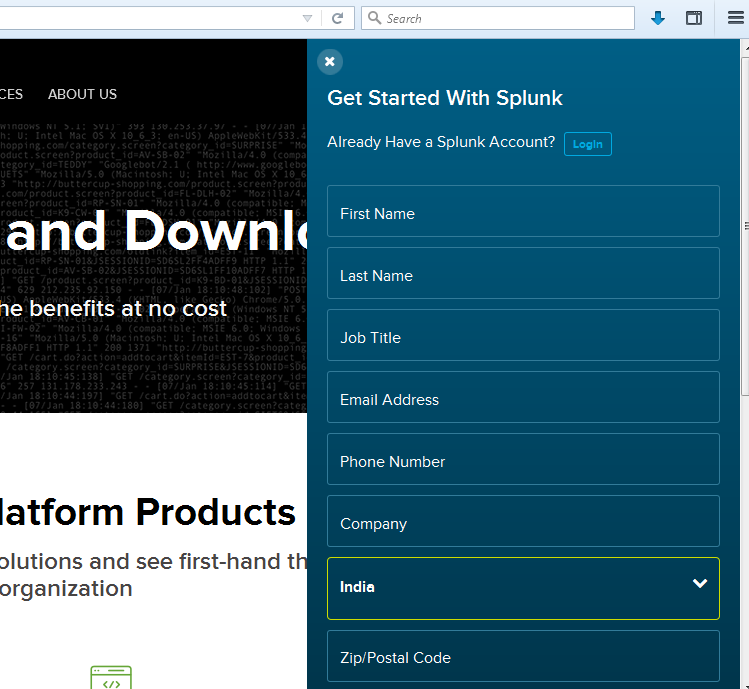


--- **1.splunk-cluster master instance**

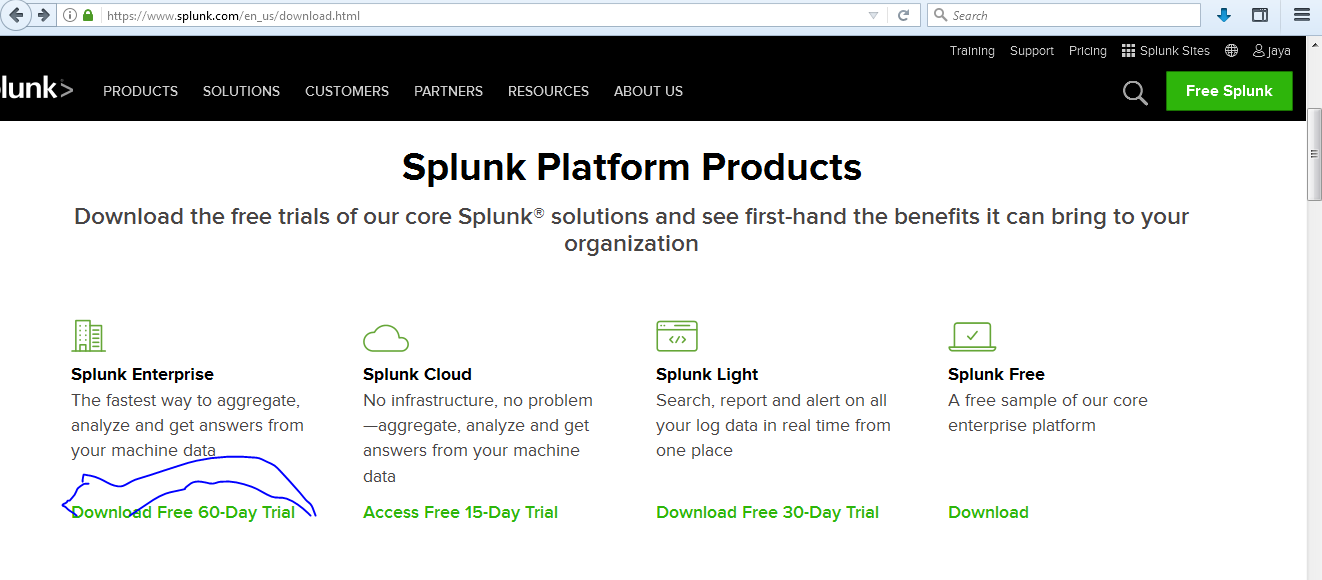
**Sign in to splunk free**

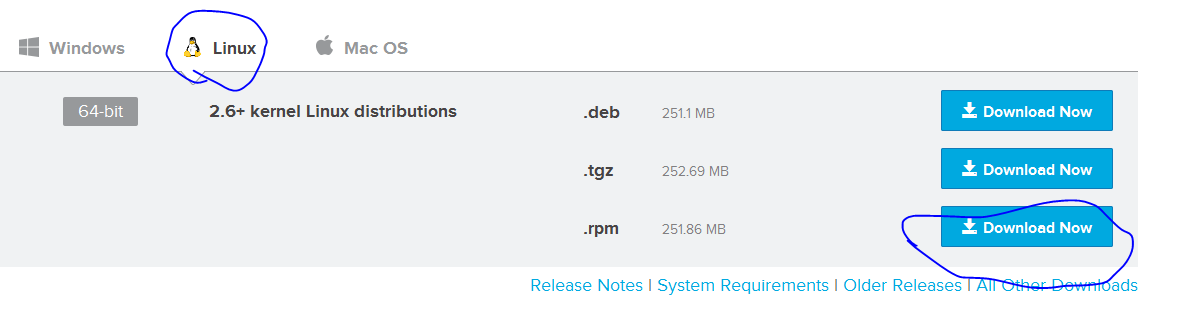
<https://www.splunk.com/en_us/download/splunk-enterprise.html>

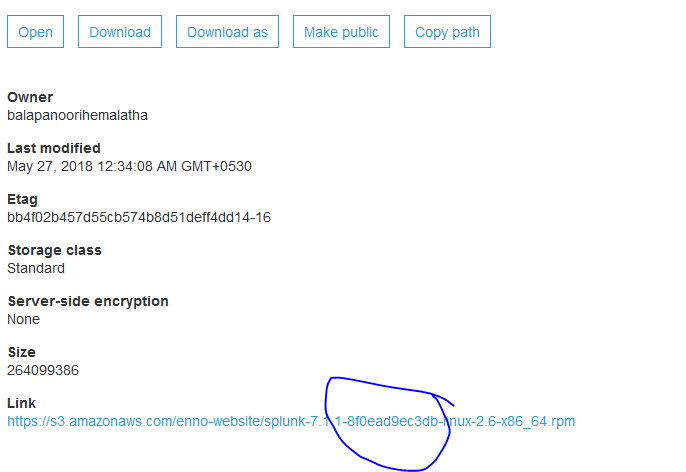




Login and verify your email….after





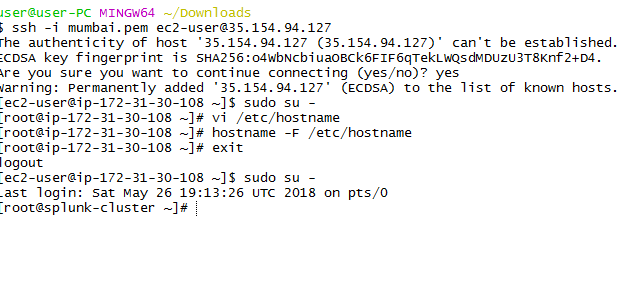
Download and upload into s3 and copy it in splunk-cluster server any where but It extract default path is /opt/splunk

<https://s3.amazonaws.com/enno-website/splunk-7.1.1-8f0ead9ec3db-linux-2.6-x86_64.rpm>

Copy this link and extract in splunk-cluster server

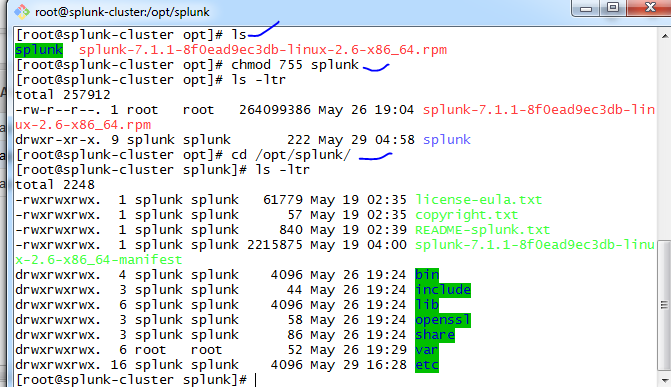
Splunk default path is /opt/splunk. Go to /opt/splunk/

→Login into splunk-cluster and change it hostname to splunk-cluster



1> download splunk rpm package for linux and extract it

2> give 777 permissions to the extract file ("chmod -R 777 splunk")



3> start the splunk instance --> cd /splunk/bin --> "./splunk start --accept-license"

[root@splunk-cluster bin]# ./splunk start --accept-license

This appears to be your first time running this version of Splunk.

An Admin password must be set before installation proceeds.

Password must contain at least:

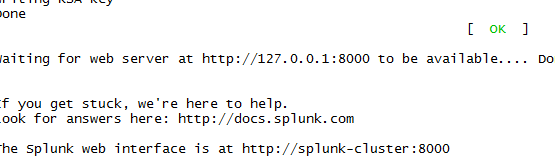
\* 8 total printable ASCII character(s).

Please enter a new password:

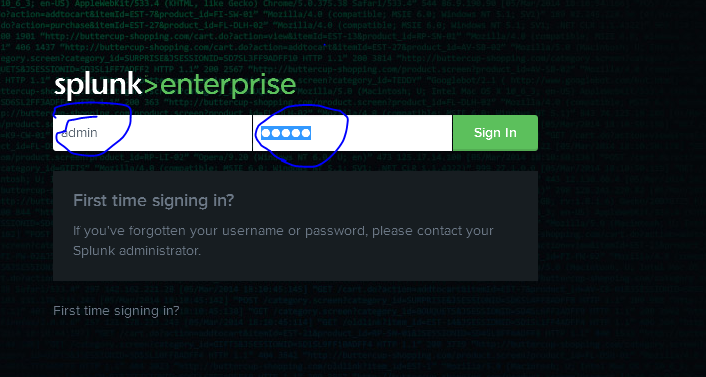
Please confirm new password:

Copying '/opt/splunk/etc/openldap/ldap.conf.default' to '/opt/splunk/etc/openldap/ldap.conf'.

Generating RSA private key, 2048 bit long modulus

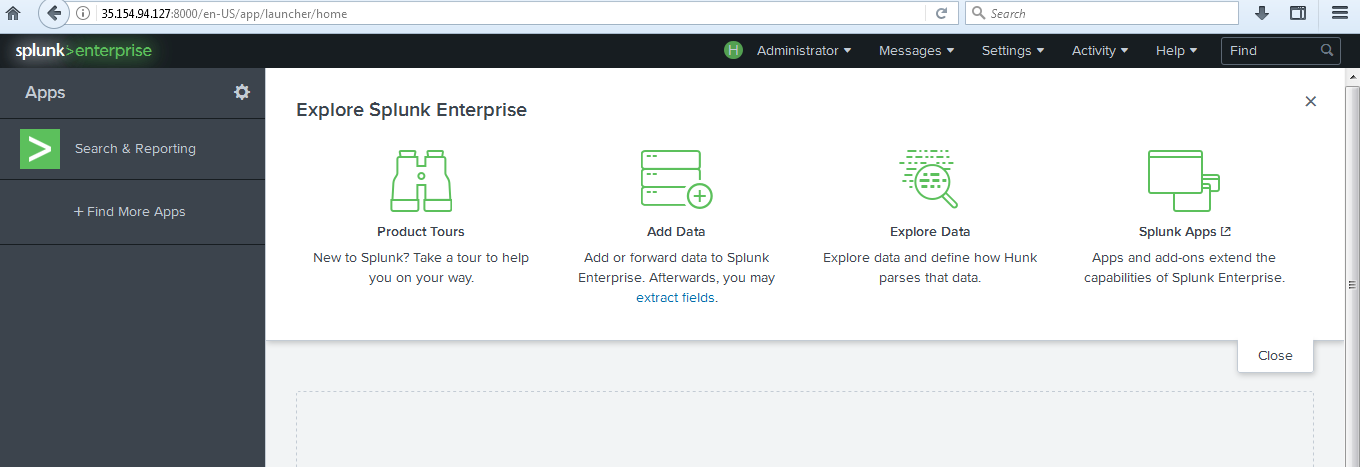


4> now check in the browser with the public ip --> "<ip>:8000"



→Enable security group with tcp 8000 from anywhere and tcp 9997 from anywhere

5> login and with password then it will redirect to splunk page

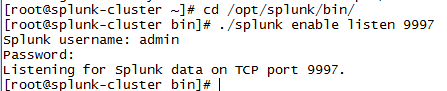


6> click on "search & reporting" on left hand side

7> now search index="main" . By default it will not show any searches bcoz we didn't set any logs to that instance. so now go to universalforwader instance and follow from step 3 to step 7.

8> cd /opt/splunk/bin --> "./splunk enable listen 9997 "

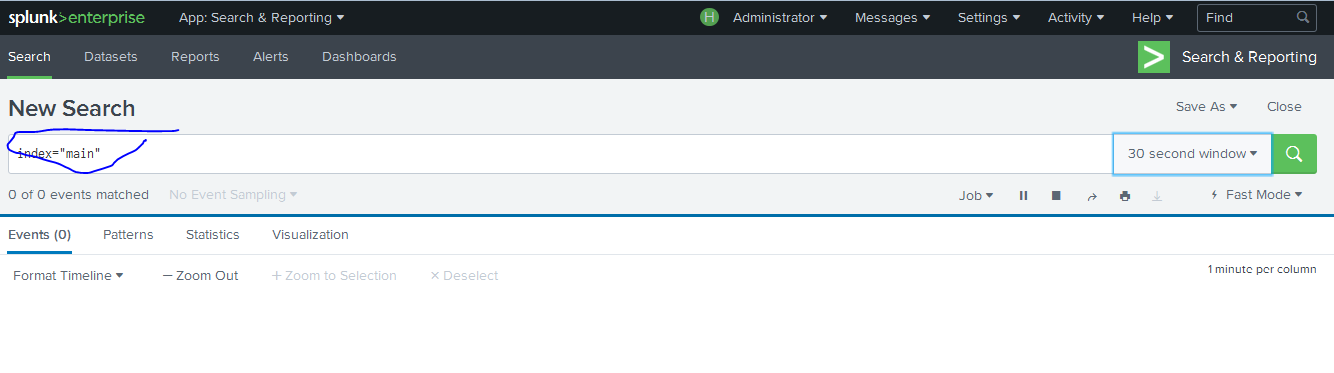
9> now it will ask username:"admin" and password:"admin" (note: here you have to enter the changed password)



and it will show msg like this "Listening for Splunk data on TCP port 9997."

10> now go to browser and check the cluster master splunk page and then go to search page and observe "what to search" section.... it will show how many events are there and latest events timings.

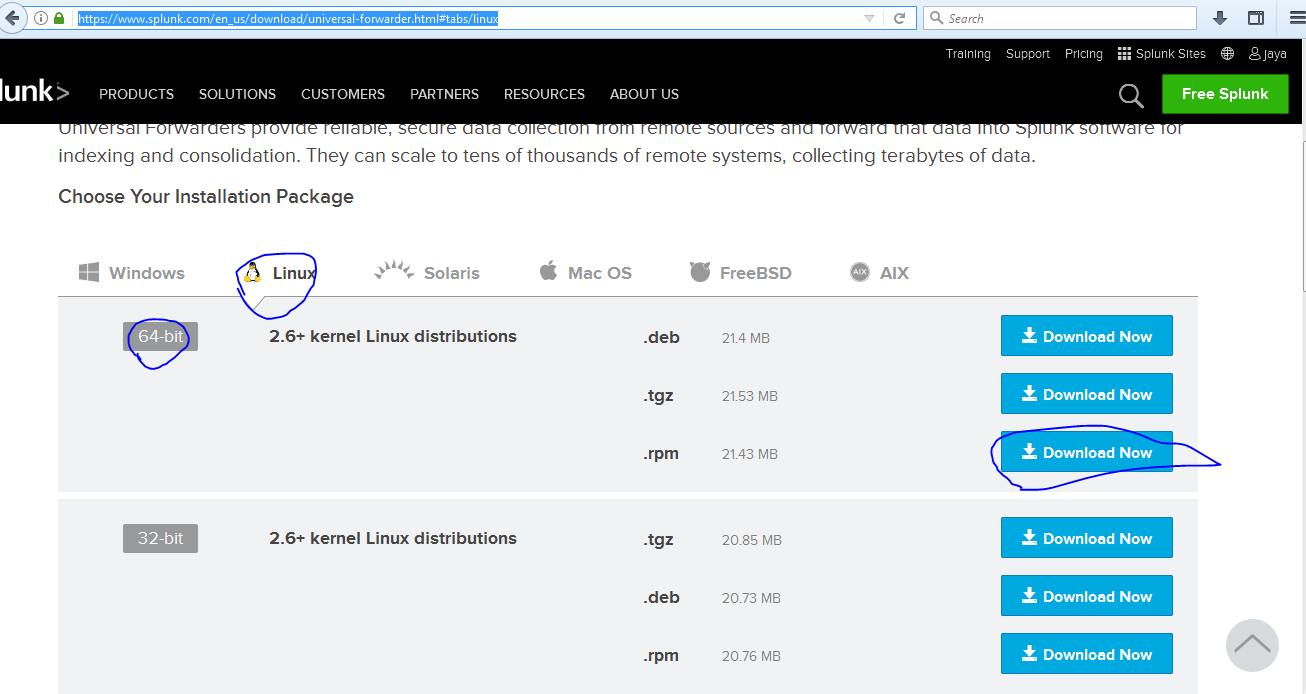
11> now search index="main" and it will show the logs.



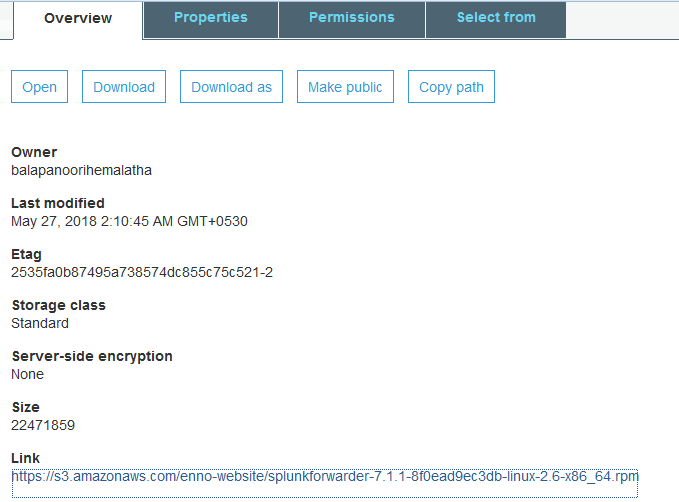
--- **2.universal forwarder instance**

1. download universal forwader rpm package for linux and extract it

<https://www.splunk.com/en_us/download/universal-forwarder.html#tabs/linux>

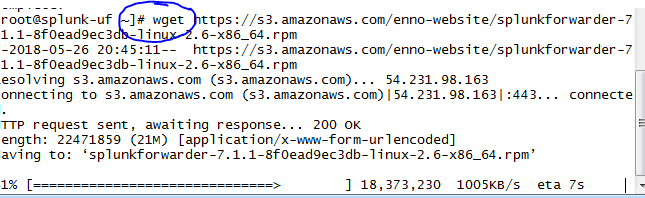


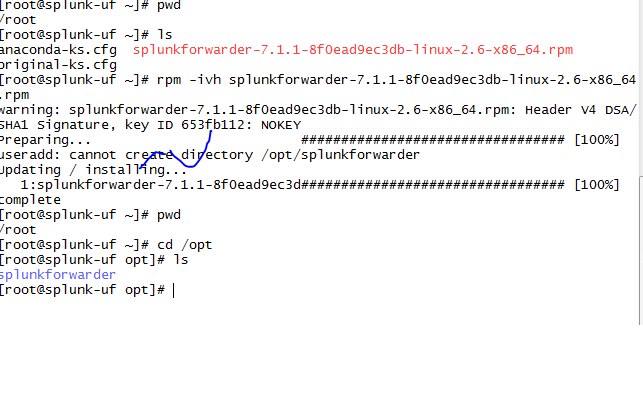
Download and copy to s3 from se to copy in splunk-universal forwarde server

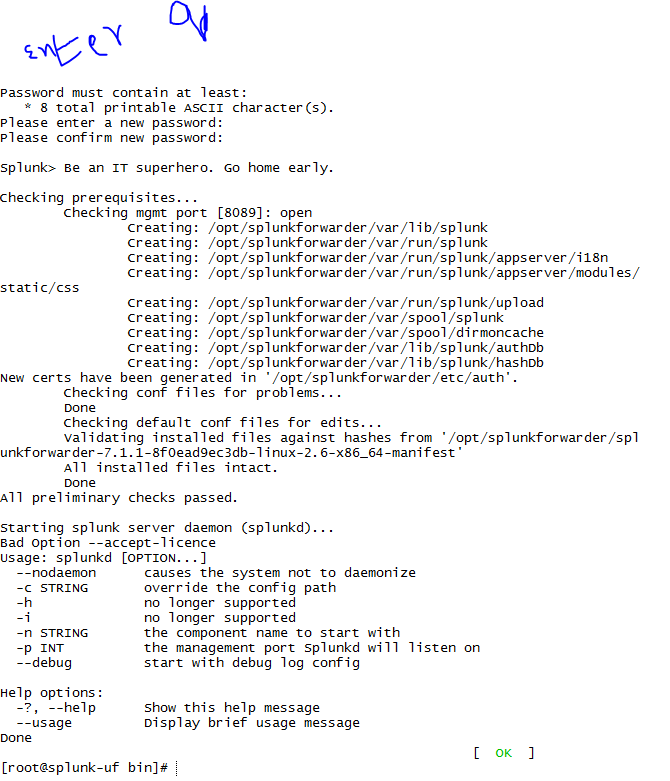


<https://s3.amazonaws.com/enno-website/splunkforwarder-7.1.1-8f0ead9ec3db-linux-2.6-x86_64.rpm>

take this link directly…wget



splunk default path is /opt/splunkforwarder

1. give 777 permissions to the extract file ("chmod -R 777 splunkforwader")
2. cd /opt/splunkforwader/bin --> "./splunk start --accept-license"
3. cd /var/ --> cd log/ --> ls --> there is a file called messages. now go to

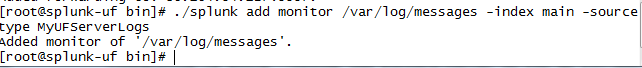
cd /opt/splunkforwader/bin --> "./splunk add forward-server <ipaddress of clustermaster instance>:9997",



**in splunk and for receiving data the default port number there are so many port numbers available is 9997.**

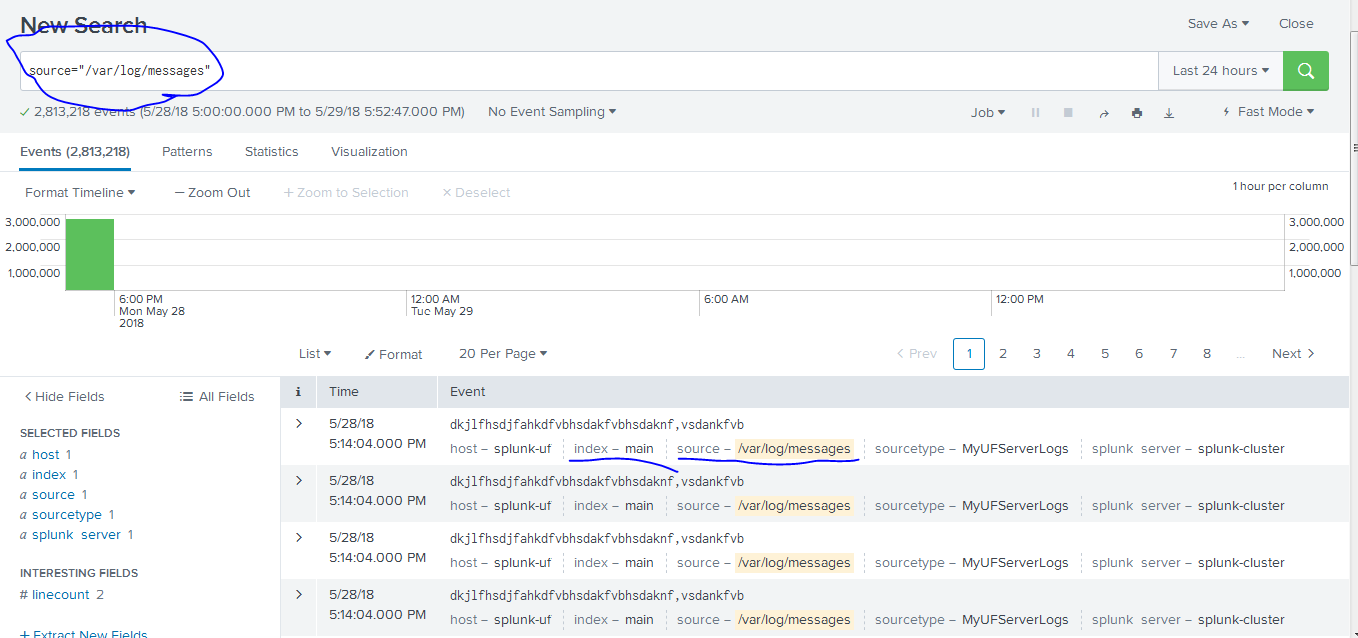
6> after entering the details it will show the msg like this "Added forwarding to: 34.207.109.166:9997."

7> By this the data forwading pipeline is ready but we didn't mention which file it has to forward. so for that --> "./splunk add monitor /var/log/messages -index main -sourcetype MyUFServerLogs" and press enter. now it will show msg like this --> "Added monitor of '/var/log/messages'."



./splunk add monitor /var/log/messages -index main -sourcetype MyUFServerLog./splunk add monitor /var/log/messages -index main -sourcetype MyUFServerLognote: sourcetype is used to identify what type of data is coming in.

8> now goto clustermaster instance and enable 9997 port number to accept data from this instance by like this --> go to step 8 to step 11.

./splunk add monitor /var/log/messages -index main -sourcetype MyUFServerLog

/var/log/httpd

How to remove logs…to splunk-cluster

1. cd /opt/splunkforwarder/bin
2. 215 ./splunk add monitor /var/log/messages -index main -sourcetype MyUFServerLogs
3. 216 ./splunk remove monitor /var/log/messages -index main -sourcetype MyUFServerLogs
4. 217 ./splunk add monitor /var/log/messages -index main -sourcetype MyUFServerLogs
5. 218 ./splunk remove monitor /var/log/httpd/access\_log -index main -sourcetype MyUFServerLogs
6. 219 ./splunk remove monitor /var/log/httpd/error\_log -index main -sourcetype MyUFServerLogs
7. 220 ./splunk remove monitor /var/log/secure -index main -sourcetype MyUFServerLogs
8. 221 clear
9. 222 ./splunk remove monitor /var/log/test -index main -sourcetype MyUFServerLogs

Forwarding tomcat logs to splunk:

Take one tomcat server and install splunk-uf in this server

[devopsadmin@tomcatserver ~]$ pwd

/home/devopsadmin

[devopsadmin@tomcatserver ~]$ wget https://s3.amazonaws.com/enno-website/splunkforwarder-7.1.1-8f0ead9ec3db-linux-2.6-x86\_64.rpm

[devopsadmin@tomcatserver ~]$ ll

total 21948

-rw-rw-r--. 1 devopsadmin devopsadmin 22471859 May 26 20:40 splunkforwarder-7.1.1-8f0ead9ec3db-linux-2.6-x86\_64.rpm

[devopsadmin@tomcatserver ~]$sudo rpm -ivh splunkforwarder-7.1.1-8f0ead9ec3db-linux-2.6-x86\_64.rpm

[devopsadmin@tomcatserver ~]$ cd /opt

[devopsadmin@tomcatserver opt]$ ls

apache-tomcat-8.5.31-windows-x64.zip splunkforwarder

jdk-8u151-linux-x64.rpm tomcat

[devopsadmin@tomcatserver opt]$ sudo chmod -R 755 splunkforwarder/

[devopsadmin@tomcatserver opt]$ cd /opt/splunkforwarder/

[devopsadmin@tomcatserver splunkforwarder]$ ls -ltr

total 128

-rwxr-xr-x. 1 splunk splunk 61779 May 19 02:35 license-eula.txt

-rwxr-xr-x. 1 splunk splunk 57 May 19 02:35 copyright.txt

-rwxr-xr-x. 1 splunk splunk 840 May 19 02:39 README-splunk.txt

-rwxr-xr-x. 1 splunk splunk 37921 May 19 04:00 splunkforwarder-7.1.1-8f0ead9ec3db-linux-2.6-x86\_64-manifest

drwxr-xr-x. 3 splunk splunk 4096 May 29 18:02 bin

drwxr-xr-x. 2 splunk splunk 27 May 29 18:02 include

drwxr-xr-x. 4 splunk splunk 4096 May 29 18:02 lib

drwxr-xr-x. 3 splunk splunk 58 May 29 18:02 openssl

drwxr-xr-x. 3 splunk splunk 41 May 29 18:02 share

drwxr-xr-x. 13 splunk splunk 4096 May 29 18:02 etc

-rwxr-xr-x. 1 splunk splunk 364 May 29 18:02 ftr

[devopsadmin@tomcatserver splunkforwarder]$cd bin

[devopsadmin@tomcatserver splunkforwarder]$ cd bin

[devopsadmin@tomcatserver bin]$sudo ./splunk start --accept-licence

Warning: cannot create "/opt/splunkforwarder/var/log/splunk"

Warning: cannot create "/opt/splunkforwarder/var/log/introspection"

SPLUNK SOFTWARE LICENSE AGREEMENT

THIS SPLUNK SOFTWARE LICENSE AGREEMENT ("AGREEMENT") GOVERNS THE LICENSING,

INSTALLATION AND USE OF SPLUNK SOFTWARE. BY DOWNLOADING AND/OR INSTALLING SPLUNK

SOFTWARE: (A) YOU ARE INDICATING THAT YOU HAVE READ AND UNDERSTAND THIS

AGREEMENT, AND AGREE TO BE LEGALLY BOUND BY IT ON BEHALF OF THE COMPANY,

GOVERNMENT, OR OTHER ENTITY FOR WHICH YOU ARE ACTING (FOR EXAMPLE, AS AN

EMPLOYEE OR GOVERNMENT OFFICIAL) OR, IF THERE IS NO COMPANY, GOVERNMENT OR OTHER

ENTITY FOR WHICH YOU ARE ACTING, ON BEHALF OF YOURSELF AS AN INDIVIDUAL; AND (B)

YOU REPRESENT AND WARRANT THAT YOU HAVE THE AUTHORITY TO ACT ON BEHALF OF AND

BIND SUCH COMPANY, GOVERNMENT OR OTHER ENTITY (IF ANY). WITHOUT LIMITING THE

FOREGOING, YOU (AND YOUR ENTITY, IF ANY) ACKNOWLEDGE THAT BY SUBMITTING AN ORDER

FOR THE SPLUNK SOFTWARE, YOU (AND YOUR ENTITY (IF ANY)) HAVE AGREED TO BE BOUND

BY THIS AGREEMENT. As used in this Agreement, "Splunk," refers to Splunk Inc., a

Delaware corporation, with its principal place of business at 270 Brannan

Street, San Francisco, California 94107, U.S.A.; and "Customer" refers to the

company, government, or other entity on whose behalf you have entered into this

Agreement or, if there is no such entity, you as an individual.

1. DEFINITIONS. Capitalized terms used but not otherwise defined in this

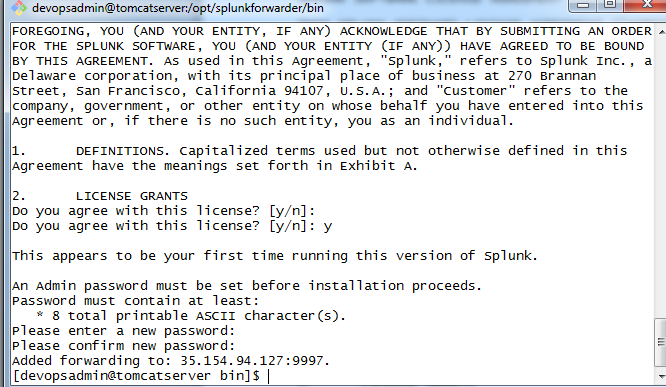
Agreement have the meanings set forth in Exhibit A.

2. LICENSE GRANTS

--More--(2%)

ENTER q here------- and enter y-------

[devopsadmin@tomcatserver bin]$ sudo ./splunk add forward-server 35.154.94.127:9997



**Now restart splunk-universal forwarder and spunk-cluster master**

[devopsadmin@tomcatserver bin]$ sudo ./splunk start

Splunk> Take the sh out of IT.

Checking prerequisites...

Checking mgmt port [8089]: open

Creating: /opt/splunkforwarder/var/run/splunk/appserver/i18n

Creating: /opt/splunkforwarder/var/run/splunk/appserver/modules/ static/css

Creating: /opt/splunkforwarder/var/run/splunk/upload

Creating: /opt/splunkforwarder/var/spool/splunk

Creating: /opt/splunkforwarder/var/spool/dirmoncache

Creating: /opt/splunkforwarder/var/lib/splunk/authDb

Creating: /opt/splunkforwarder/var/lib/splunk/hashDb

New certs have been generated in '/opt/splunkforwarder/etc/auth'.

Checking conf files for problems...

Done

Checking default conf files for edits...

Validating installed files against hashes from '/opt/splunkforwarder/spl unkforwarder-7.1.1-8f0ead9ec3db-linux-2.6-x86\_64-manifest'

All installed files intact.

Done

All preliminary checks passed.

Starting splunk server daemon (splunkd)...

Done

[ OK ]

[devopsadmin@**tomcatserver** bin]$

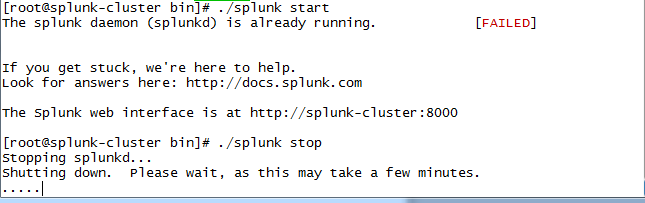
[root@**splunk-cluster** ~]# cd /opt/splunk/bin/

[**devopsadmin@tomcatserver** bin]$ sudo ./splunk add monitor /opt/tomcat/logs/catalina.out -index main -sourcetype MyUFLogs

Added monitor of '/opt/tomcat/logs/catalina.out'.

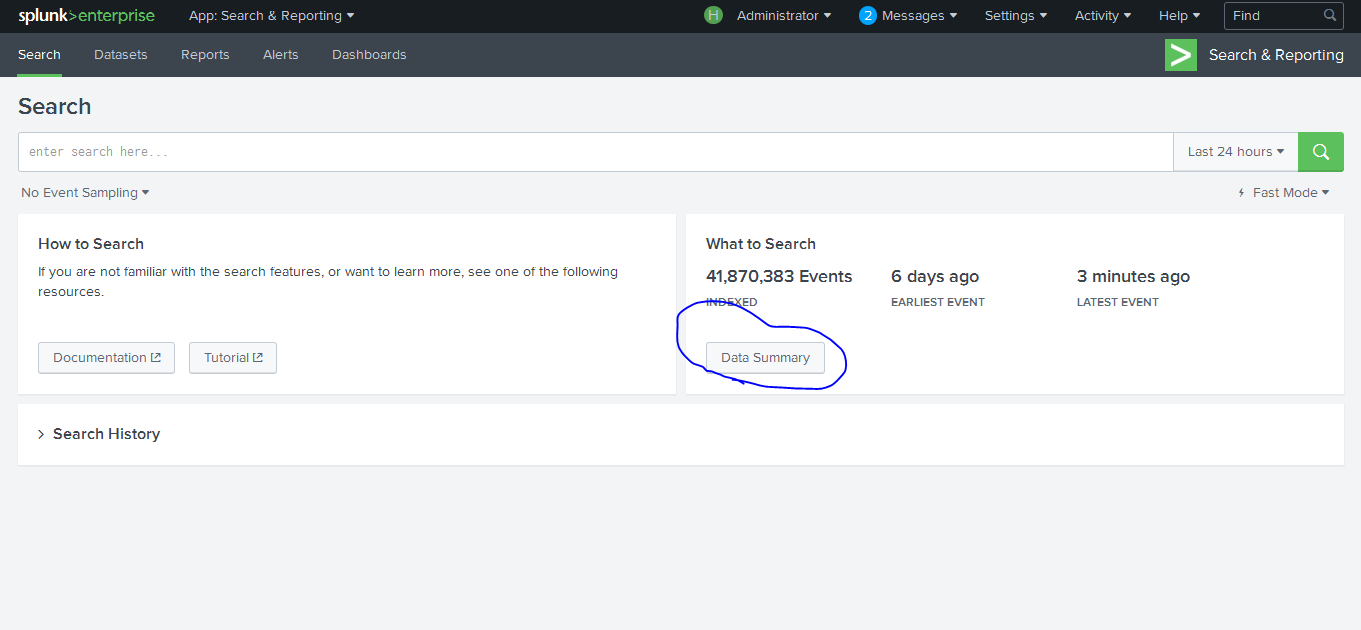
[**devopsadmin@tomcatserver bin]$**

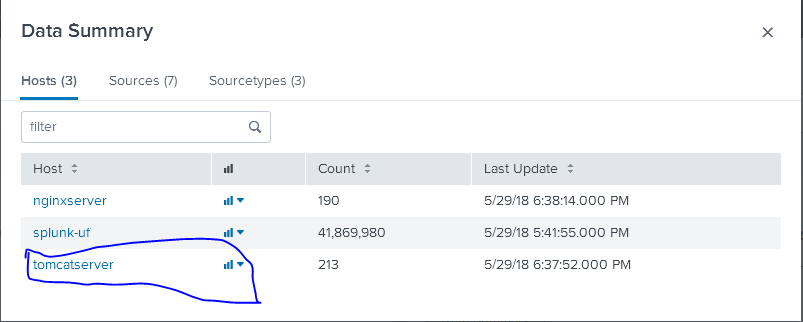
**Now connect to splunk-cluster and restart splunk**

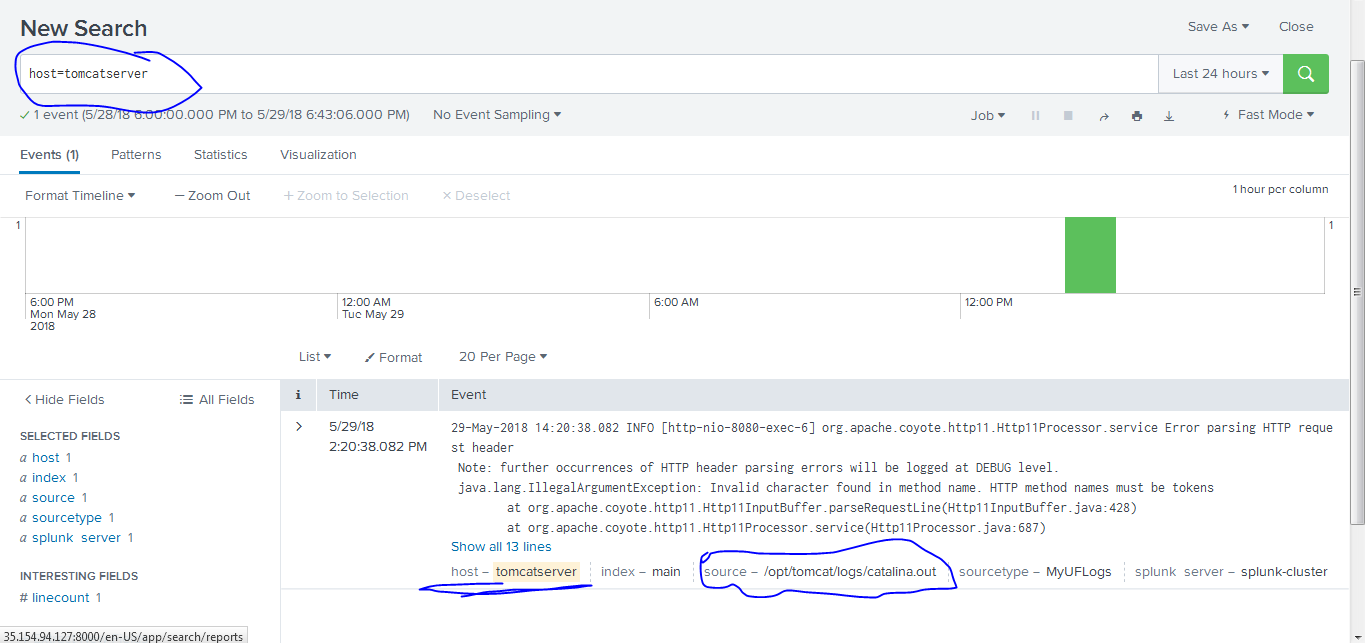


[root@splunk-cluster bin]# ./splunk start

Now go and check splunk-cluster <public ip>:8000







These are tomcat logs in splunk……