SPLUNK

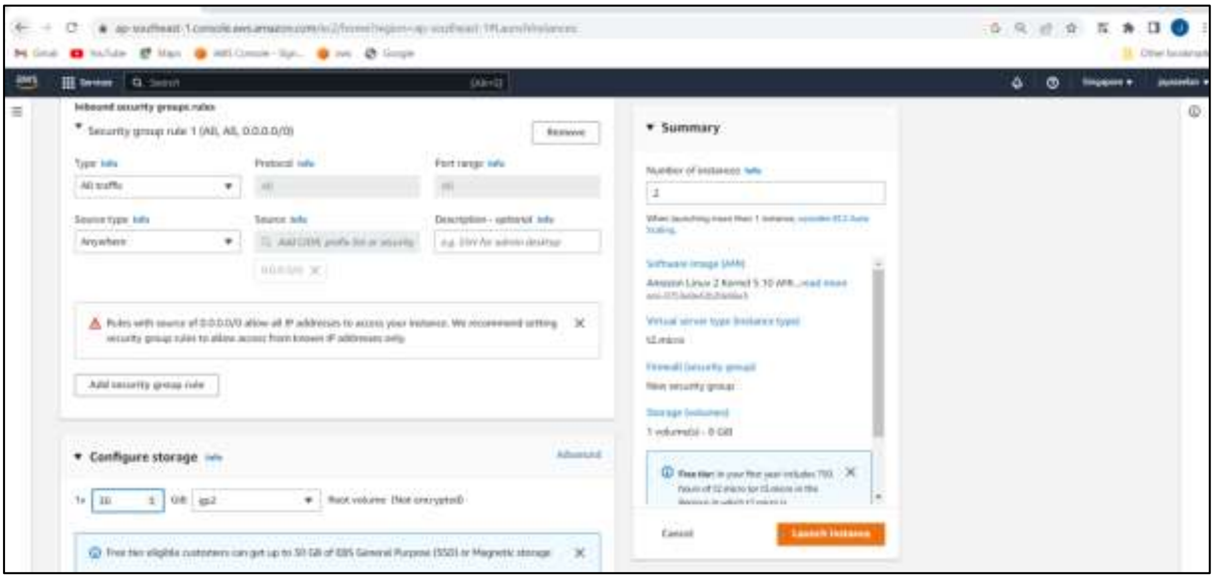
- It is log monitoring tool
- Master slave architecture
- 60 days free trail available
- Splunk is google for your machine data
- It used searching,visualizing,monitoring,reporting your data

purpose

- Proactive monitoring+dashboard generation+alterting
- 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.

Steps to create splunk

Step1:create EC2 server (2)---->1-master server,2-slave server---->security (all traffic)---->storage (30gb)---->launch instance.



Inbound security groups rules

Security group rule 1 (All, All, 0.0.0.0/0)

Type: All traffic

Protocol: All

Port range: All

Source type: Anywhere

Source: 0.0.0.0/0

Description - optional: e.g. SSH for admin desktop

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Configure storage

1x 30 GiB gp2 Root volume (Not encrypted)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

Summary

Number of instances: 2

When launching more than 1 instance, consider EC2 Auto Scaling.

Software Image (AMI)

Amazon Linux 2 Kernel 5.10 AMI...read more

Virtual server type (instance type)

t2.micro

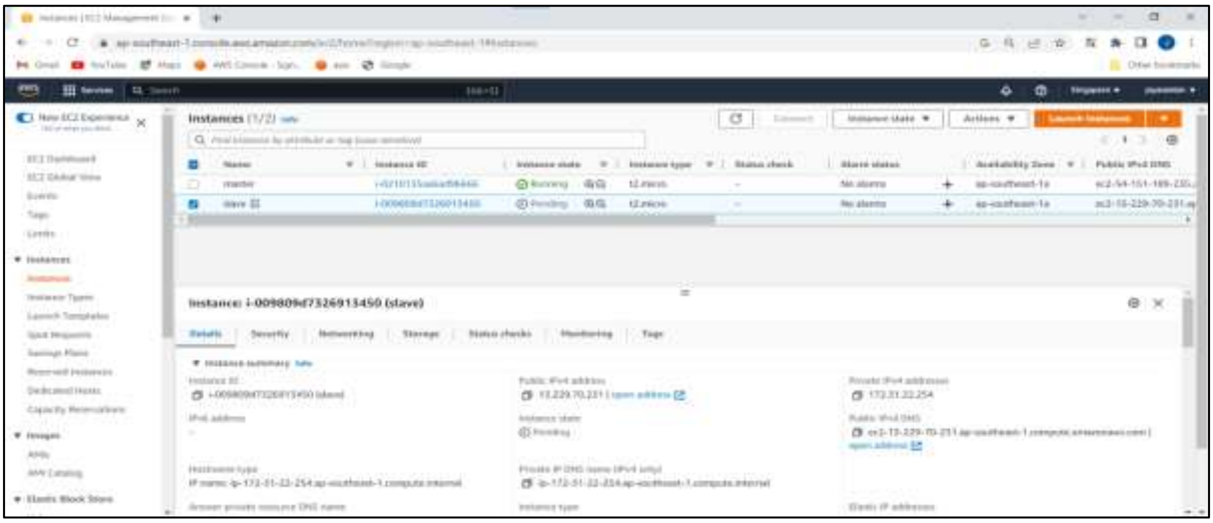
Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is master and slave server created.



Instances (1/2)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
master	[illegible]	Running	t2.micro	-	No alarms	ap-southeast-1a	ec2-54-151-189-235...
slave	i-009809d7326913450	Pending	t2.micro	-	No alarms	ap-southeast-1a	ec2-13-229-70-231...

Instance: i-009809d7326913450 (slave)

Instance summary

Instance ID: i-009809d7326913450 (slave)

Public IPv4 address: 13.229.70.231 | open address

Private IPv4 addresses: 172.31.22.254

IPv6 address: -

Instance state: Pending

Public IPv4 DNS: ec2-13-229-70-231.ap-southeast-1.compute.amazonaws.com | open address

Hostname type: IP name: ip-172-31-22-254.ap-southeast-1.compute.internal

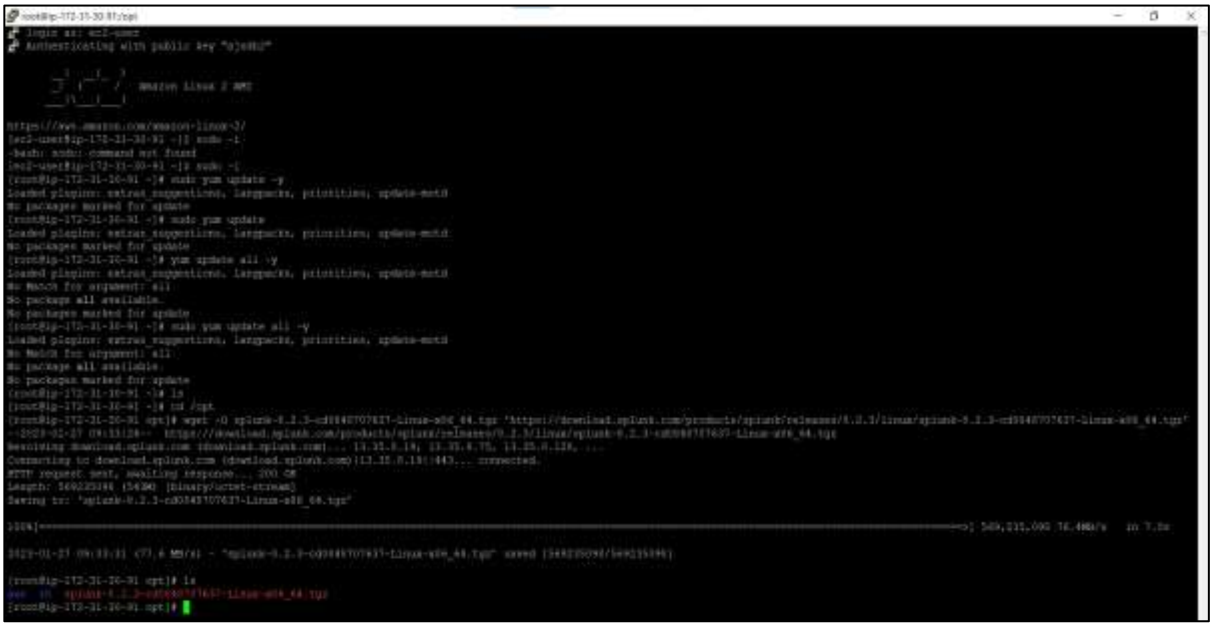
Private IP DNS name (IPv4 only): ip-172-31-22-254.ap-southeast-1.compute.internal

Step2:login master server(**Enterprise Server**)--->sudo –i

----->#sudo yum update –y (or) cd /opt

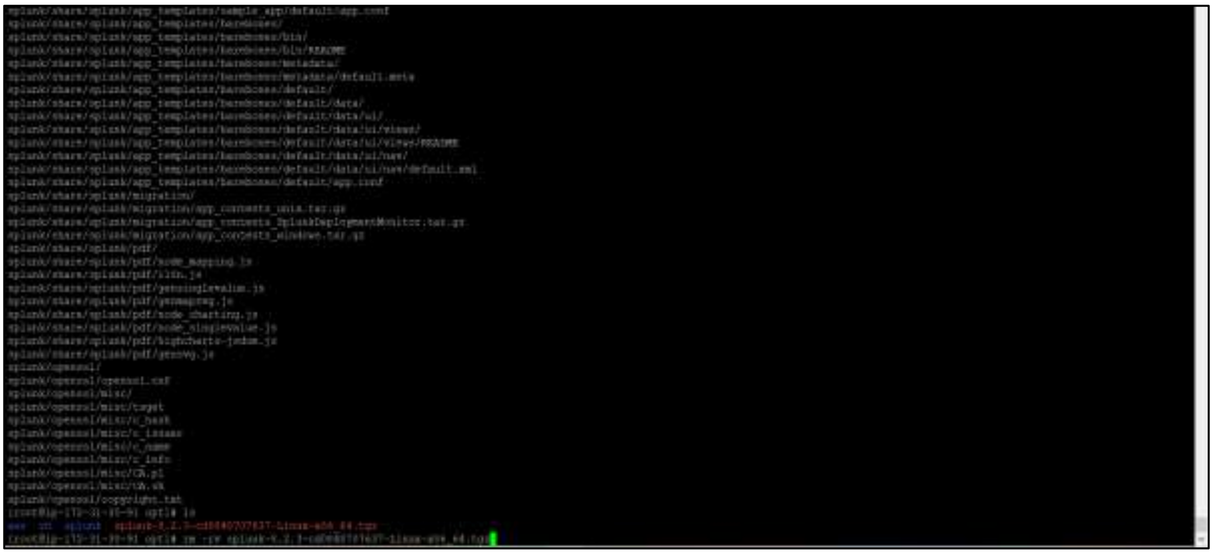
------># wget -O splunk-8.2.3-cd0848707637-Linux-x86_64.tgz 'https://download.splunk.com/products/splunk/releases/8.2.3/linux/splunk-8.2.3-cd0848707637-Linux-x86_64.tgz' ------>(splunk download)

#ls ------>shown splunk file



```
login as: ec2-user
Authenticating with public key "[illegible]"

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-30-91 ~]$ sudo -i
-bash: sudo: command not found
[ec2-user@ip-172-31-30-91 ~]$ sudo -i
[root@ip-172-31-30-91 ~]# sudo yum update -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
No packages marked for update
[root@ip-172-31-30-91 ~]# sudo yum update
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
No packages marked for update
[root@ip-172-31-30-91 ~]# yum update all -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
No Match for argument: all
No package all available.
No packages marked for update
[root@ip-172-31-30-91 ~]# sudo yum update all -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
No Match for argument: all
No package all available.
No packages marked for update
[root@ip-172-31-30-91 ~]# ls
[root@ip-172-31-30-91 ~]# cd /opt
[root@ip-172-31-30-91 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'
--2022-01-27 09:33:28--  https://download.splunk.com/products/splunk/releases/8.2.3/linux/splunk-8.2.3-cd0848707637-Linux-x86_64.tgz
Resolving download.splunk.com (download.splunk.com)... 13.35.8.19, 13.35.8.75, 13.35.8.128, ...
Connecting to download.splunk.com (download.splunk.com)|13.35.8.19|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 569235098 (543M) [binary/octet-stream]
Saving to: 'splunk-8.2.3-cd0848707637-Linux-x86_64.tgz'

100%[==================================================================================>] 569,235,098  76.4MB/s   in 7.0s

2022-01-27 09:33:35 (77.6 MB/s) - 'splunk-8.2.3-cd0848707637-Linux-x86_64.tgz' saved [569235098/569235098]

[root@ip-172-31-30-91 opt]# ls
aws  rh  splunk-8.2.3-cd0848707637-Linux-x86_64.tgz
[root@ip-172-31-30-91 opt]#
```

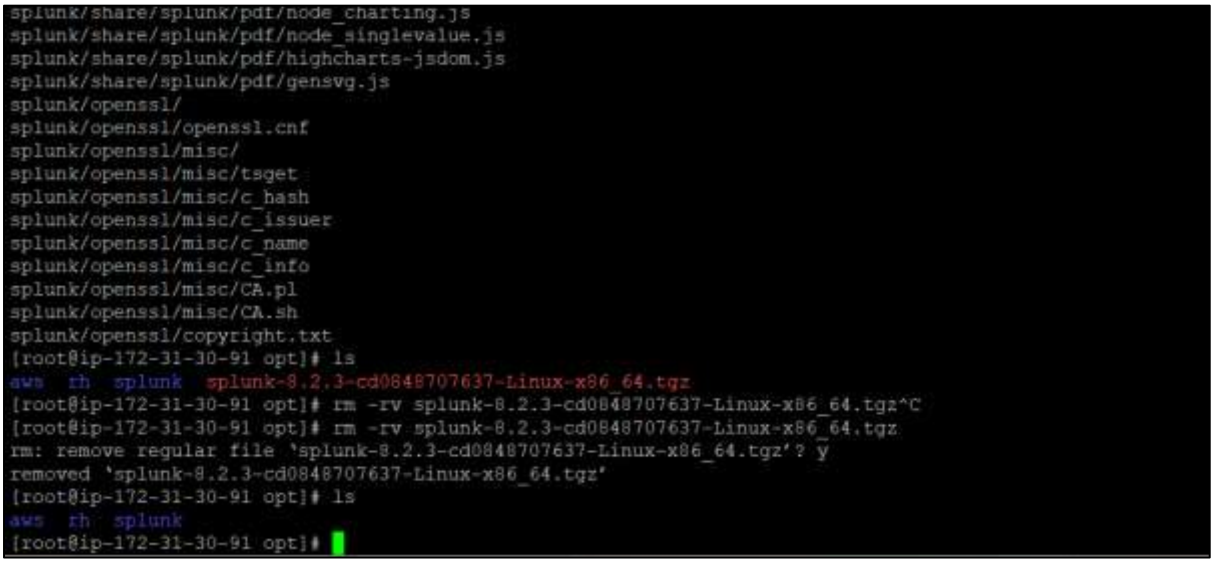
#tar –xvzf splunk-8.2.3-cd0848707637-Linux-x86_64.tgz --->unzip



```
splunk/share/splunk/app_templates/sample_app/default/app.conf
splunk/share/splunk/app_templates/barebones/
splunk/share/splunk/app_templates/barebones/bin/
splunk/share/splunk/app_templates/barebones/bin/README
splunk/share/splunk/app_templates/barebones/metadata/
splunk/share/splunk/app_templates/barebones/metadata/default.meta
splunk/share/splunk/app_templates/barebones/default/
splunk/share/splunk/app_templates/barebones/default/data/
splunk/share/splunk/app_templates/barebones/default/data/ui/
splunk/share/splunk/app_templates/barebones/default/data/ui/views/
splunk/share/splunk/app_templates/barebones/default/data/ui/views/README
splunk/share/splunk/app_templates/barebones/default/data/ui/nav/
splunk/share/splunk/app_templates/barebones/default/data/ui/nav/default.xml
splunk/share/splunk/app_templates/barebones/default/app.conf
splunk/share/splunk/migration/
splunk/share/splunk/migration/app_contents_unix.tar.gz
splunk/share/splunk/migration/app_contents_SplunkDeploymentMonitor.tar.gz
splunk/share/splunk/migration/app_contents_windows.tar.gz
splunk/share/splunk/pdf/
splunk/share/splunk/pdf/node_mapping.js
splunk/share/splunk/pdf/i18n.js
splunk/share/splunk/pdf/gensinglevalue.js
splunk/share/splunk/pdf/genmappng.js
splunk/share/splunk/pdf/node_charting.js
splunk/share/splunk/pdf/node_singlevalue.js
splunk/share/splunk/pdf/highcharts-jsdom.js
splunk/share/splunk/pdf/gensvg.js
splunk/openssl/
splunk/openssl/openssl.cnf
splunk/openssl/misc/
splunk/openssl/misc/tsget
splunk/openssl/misc/c_hash
splunk/openssl/misc/c_issuer
splunk/openssl/misc/c_name
splunk/openssl/misc/c_info
splunk/openssl/misc/CA.pl
splunk/openssl/misc/CA.sh
splunk/openssl/copyright.txt
[root@ip-172-31-30-91 opt]# ls
aws  rh  splunk  splunk-8.2.3-cd0848707637-Linux-x86_64.tgz
[root@ip-172-31-30-91 opt]# rm -rv splunk-8.2.3-cd0848707637-Linux-x86_64.tgz
```

#ls ---->unzip file show(splunk)

rm -rv splunk-8.2.3-cd0848707637-Linux-x86_64.tgz --->remove zip file



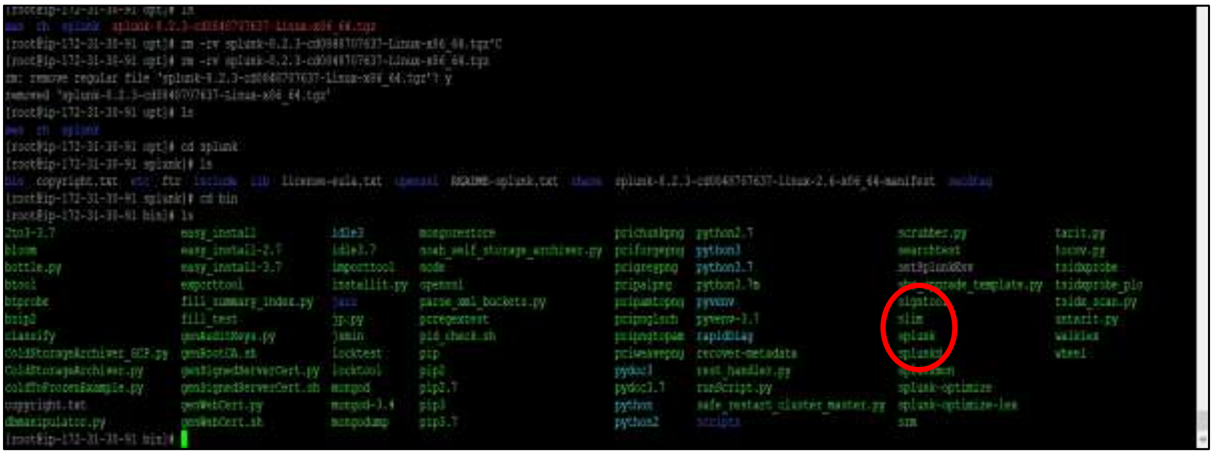
```
splunk/share/splunk/pdf/node_charting.js
splunk/share/splunk/pdf/node_singlevalue.js
splunk/share/splunk/pdf/highcharts-jsdom.js
splunk/share/splunk/pdf/gensvg.js
splunk/openssl/
splunk/openssl/openssl.cnf
splunk/openssl/misc/
splunk/openssl/misc/tsget
splunk/openssl/misc/c_hash
splunk/openssl/misc/c_issuer
splunk/openssl/misc/c_name
splunk/openssl/misc/c_info
splunk/openssl/misc/CA.pl
splunk/openssl/misc/CA.sh
splunk/openssl/copyright.txt
[root@ip-172-31-30-91 opt]# ls
aws  rh  splunk  splunk-8.2.3-cd0848707637-Linux-x86_64.tgz
[root@ip-172-31-30-91 opt]# rm -rv splunk-8.2.3-cd0848707637-Linux-x86_64.tgz^C
[root@ip-172-31-30-91 opt]# rm -rv splunk-8.2.3-cd0848707637-Linux-x86_64.tgz
rm: remove regular file ‘splunk-8.2.3-cd0848707637-Linux-x86_64.tgz’? y
removed ‘splunk-8.2.3-cd0848707637-Linux-x86_64.tgz’
[root@ip-172-31-30-91 opt]# ls
aws  rh  splunk
[root@ip-172-31-30-91 opt]#
```

Removed zip file and show unzip file

#cd splunk

#cd bin

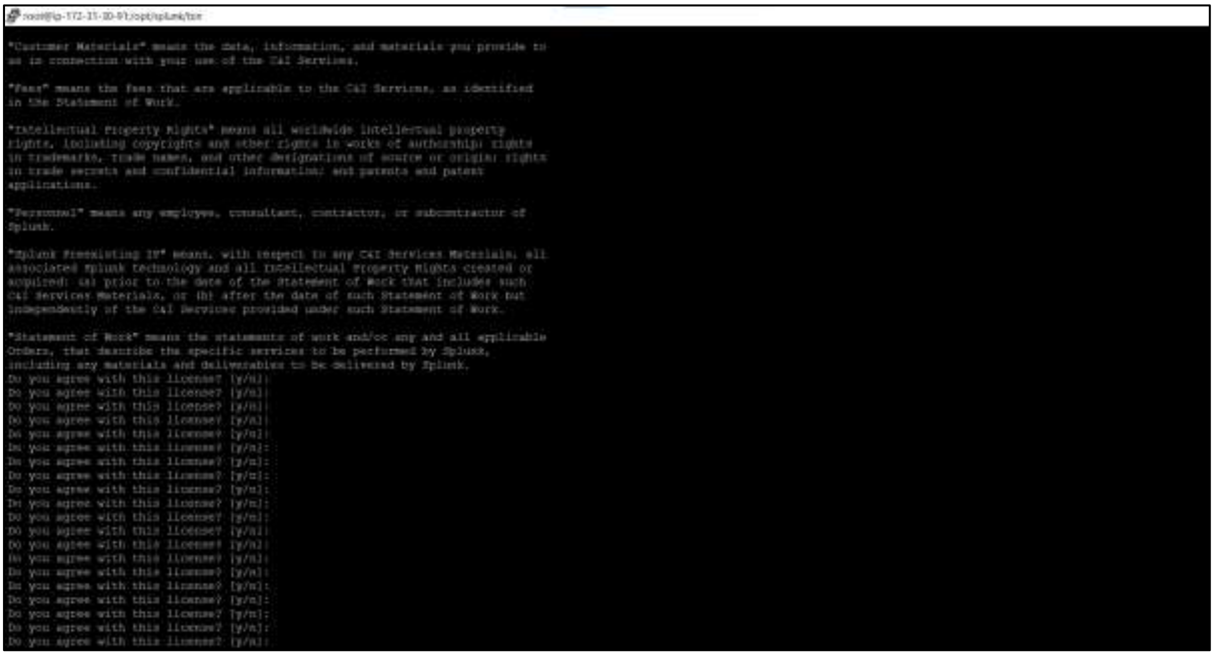
#ls ---->shown splunk



```
[root@ip-172-31-30-91 opt]# ls
aws  ch  splunk  splunk-8.2.3-cd0848707637-Linux-x86_64.tgz
[root@ip-172-31-30-91 opt]# rm -rv splunk-8.2.3-cd0848707637-Linux-x86_64.tgz^C
[root@ip-172-31-30-91 opt]# rm -rv splunk-8.2.3-cd0848707637-Linux-x86_64.tgz
rm: remove regular file 'splunk-8.2.3-cd0848707637-Linux-x86_64.tgz'? y
removed 'splunk-8.2.3-cd0848707637-Linux-x86_64.tgz'
[root@ip-172-31-30-91 opt]# ls
aws  ch  splunk
[root@ip-172-31-30-91 opt]# cd splunk
[root@ip-172-31-30-91 splunk]# ls
bin  copyright.txt  etc  ftr  include  lib  license-eula.txt  openssl  README-splunk.txt  share  splunk-8.2.3-cd0848707637-linux-2.6-x86_64-manifest  swidtag
[root@ip-172-31-30-91 splunk]# cd bin
[root@ip-172-31-30-91 bin]# ls
2to3-3.7                    easy_install              idle3         mongorestore                   prichunkpng  python2.7                       scrubber.py              tarit.py
bloom                       easy_install-2.7          idle3.7       noah_self_storage_archiver.py  priforgepng  python3                         searchtest               tocsv.py
bottle.py                   easy_install-3.7          importtool    node                           prigreypng   python3.7                       setSplunkEnv             tsidxprobe
btool                       exporttool                installit.py  openssl                        pripalpng    python3.7m                      shc_upgrade_template.py  tsidxprobe_plo
btprobe                     fill_summary_index.py     jars          parse_xml_buckets.py           pripamtopng  pyvenv                          signtool                 tsidx_scan.py
bzip2                       fill_test                 jp.py         pcregextest                    pripnglsch   pyvenv-3.7                      slim                     untarit.py
classify                    genAuthKeys.py            jsmin         pid_check.sh                   pripngtopam  rapidDiag                       splunk                   walklex
ColdStorageArchiver_GCP.py  genRootCA.sh              locktest      pip                            priweavepng  recover-metadata                splunkd                  wheel
ColdStorageArchiver.py      genSignedServerCert.py    locktool      pip2                           pydoc3       rest_handler.py                 splunkmon
coldToFrozenExample.py      genSignedServerCert.sh    mongod        pip2.7                         pydoc3.7     runScript.py                    splunk-optimize
copyright.txt               genWebCert.py             mongod-3.4    pip3                           python       safe_restart_cluster_master.py  splunk-optimize-lex
dbmanipulator.py            genWebCert.sh             mongodump     pip3.7                         python2      scripts                         srm
[root@ip-172-31-30-91 bin]# 
```

#./splunk start

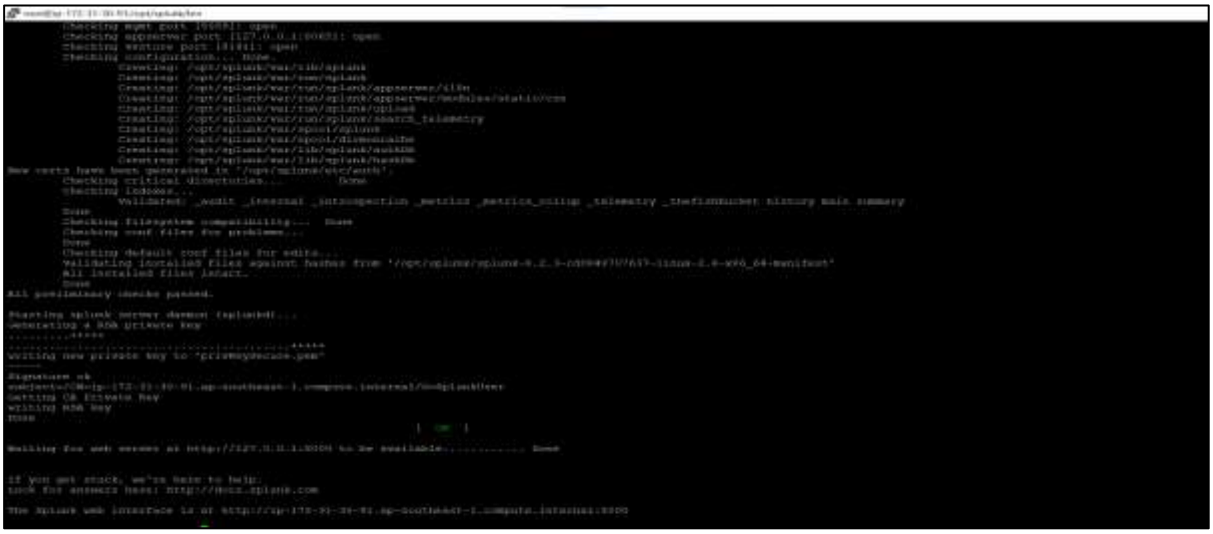
--->y



root@ip-172-31-30-91:/opt/splunk/bin

```
"Customer Materials" means the data, information, and materials you provide to
us in connection with your use of the C&I Services.

"Fees" means the fees that are applicable to the C&I Services, as identified
in the Statement of Work.

"Intellectual Property Rights" means all worldwide intellectual property
rights, including copyrights and other rights in works of authorship; rights
in trademarks, trade names, and other designations of source or origin; rights
in trade secrets and confidential information; and patents and patent
applications.

"Personnel" means any employee, consultant, contractor, or subcontractor of
Splunk.

"Splunk Preexisting IP" means, with respect to any C&I Services Materials, all
associated Splunk technology and all Intellectual Property Rights created or
acquired: (a) prior to the date of the Statement of Work that includes such
C&I Services Materials, or (b) after the date of such Statement of Work but
independently of the C&I Services provided under such Statement of Work.

"Statement of Work" means the statements of work and/or any and all applicable
Orders, that describe the specific services to be performed by Splunk,
including any materials and deliverables to be delivered by Splunk.
Do you agree with this license? [y/n]:
Do you agree with this license? [y/n]:
Do you agree with this license? [y/n]:
Do you agree with this license? [y/n]:
Do you agree with this license? [y/n]:
Do you agree with this license? [y/n]:
Do you agree with this license? [y/n]:
Do you agree with this license? [y/n]:
Do you agree with this license? [y/n]:
Do you agree with this license? [y/n]:
Do you agree with this license? [y/n]:
Do you agree with this license? [y/n]:
Do you agree with this license? [y/n]:
Do you agree with this license? [y/n]:
Do you agree with this license? [y/n]:
Do you agree with this license? [y/n]:
Do you agree with this license? [y/n]:
Do you agree with this license? [y/n]:
Do you agree with this license? [y/n]:
Do you agree with this license? [y/n]:
```

Give username(jayaseelan) and password(jaya1234)

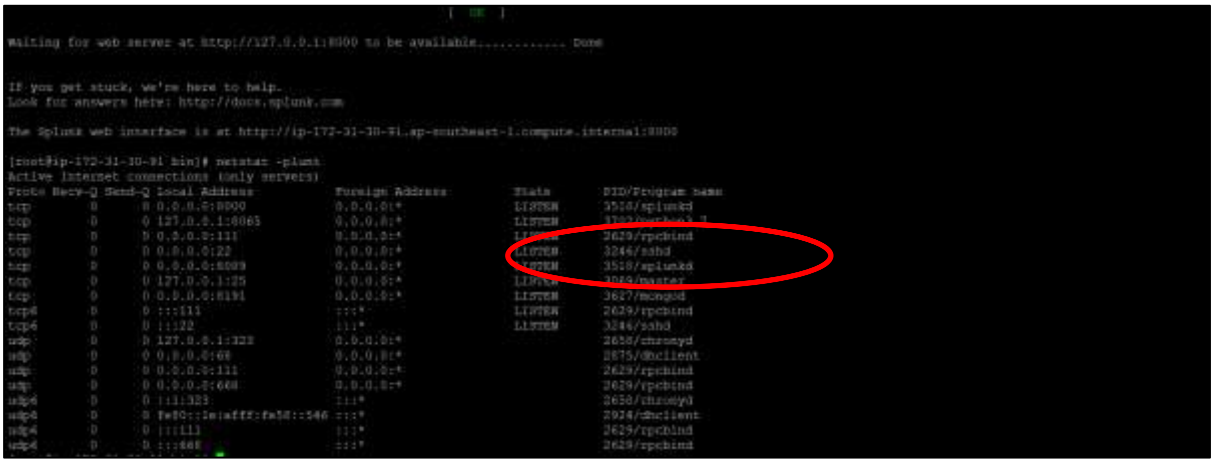


root@ip-172-31-30-91:/opt/splunk/bin

```
        Checking mgmt port [8089]: open
        Checking appserver port [127.0.0.1:8065]: open
        Checking kvstore port [8191]: open
        Checking configuration... Done.
                Creating: /opt/splunk/var/lib/splunk
                Creating: /opt/splunk/var/run/splunk
                Creating: /opt/splunk/var/run/splunk/appserver/i18n
                Creating: /opt/splunk/var/run/splunk/appserver/modules/static/css
                Creating: /opt/splunk/var/run/splunk/upload
                Creating: /opt/splunk/var/run/splunk/search_telemetry
                Creating: /opt/splunk/var/spool/splunk
                Creating: /opt/splunk/var/spool/dirmoncache
                Creating: /opt/splunk/var/lib/splunk/authDb
                Creating: /opt/splunk/var/lib/splunk/hashDb
New certs have been generated in '/opt/splunk/etc/auth'.
        Checking critical directories...        Done
        Checking indexes...
                Validated: _audit _internal _introspection _metrics _metrics_rollup _telemetry _thefishbucket history main summary
        Done
        Checking filesystem compatibility...  Done
        Checking conf files for problems...
        Done
        Checking default conf files for edits...
        Validating installed files against hashes from '/opt/splunk/splunk-8.2.3-cd0848707637-linux-2.6-x86_64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Generating a RSA private key
..........+++++
..............................................+++++
writing new private key to 'privKeySecure.pem'
-----
Signature ok
subject=/CN=ip-172-31-30-91.ap-southeast-1.compute.internal/O=SplunkUser
Getting CA Private Key
writing RSA key
Done
                                                   [  OK  ]

Waiting for web server at http://127.0.0.1:8000 to be available............. Done


If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

The Splunk web interface is at http://ip-172-31-30-91.ap-southeast-1.compute.internal:8000
```

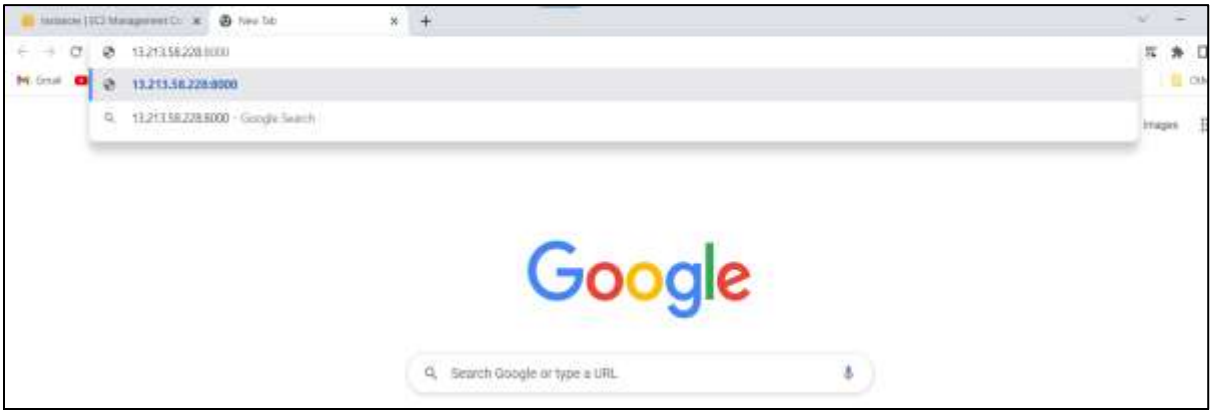
Now check port number

#netstat -plunt



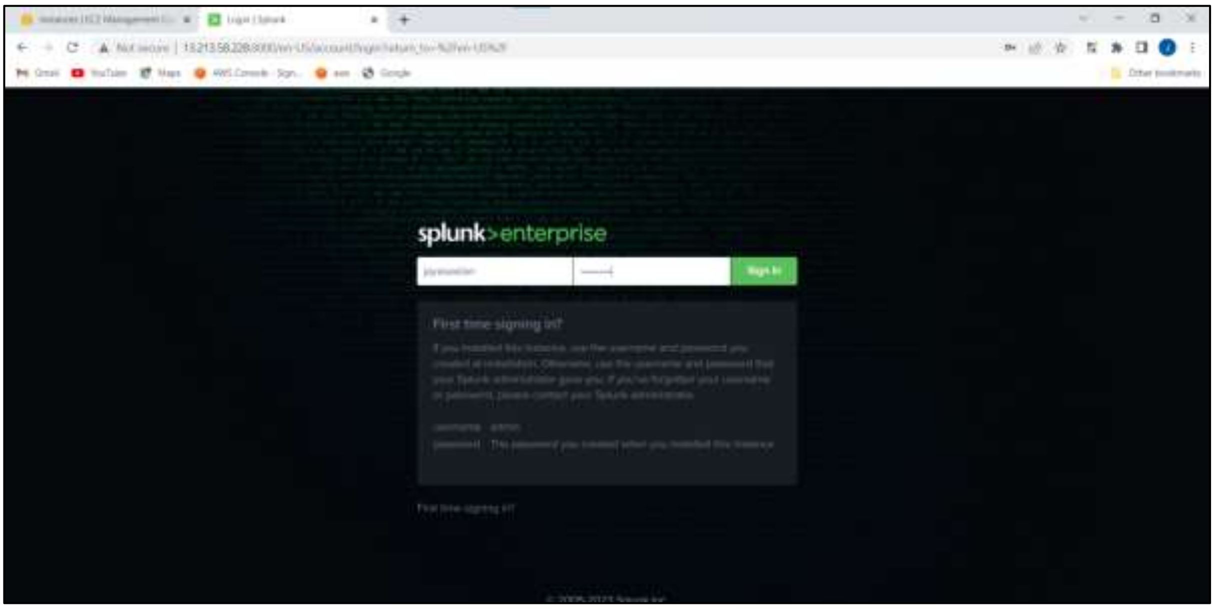
```
                                                                    [  OK  ]

Waiting for web server at http://127.0.0.1:8000 to be available............ Done

If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

The Splunk web interface is at http://ip-172-31-30-91.ap-southeast-1.compute.internal:8000

[root@ip-172-31-30-91 bin]# netstat -plunt
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:8000            0.0.0.0:*               LISTEN      3510/splunkd
tcp        0      0 127.0.0.1:8065          0.0.0.0:*               LISTEN      3702/python3.7
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      2629/rpcbind
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      3246/sshd
tcp        0      0 0.0.0.0:8089            0.0.0.0:*               LISTEN      3510/splunkd
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      3049/master
tcp        0      0 0.0.0.0:8191            0.0.0.0:*               LISTEN      3627/mongod
tcp6       0      0 :::111                  :::*                    LISTEN      2629/rpcbind
tcp6       0      0 :::22                   :::*                    LISTEN      3246/sshd
udp        0      0 127.0.0.1:323           0.0.0.0:*                           2658/chronyd
udp        0      0 0.0.0.0:68              0.0.0.0:*                           2875/dhclient
udp        0      0 0.0.0.0:111             0.0.0.0:*                           2629/rpcbind
udp        0      0 0.0.0.0:668             0.0.0.0:*                           2629/rpcbind
udp6       0      0 ::1:323                 :::*                                2658/chronyd
udp6       0      0 fe80::1e:afff:fe58::546 :::*                                2924/dhclient
udp6       0      0 :::111                  :::*                                2629/rpcbind
udp6       0      0 :::668                  :::*                                2629/rpcbind
```

Step3:master server public ip put chrome(13.213.58.228:8000)



Instances | EC2 Management Co
New Tab
13.213.58.228:8000
13.213.58.228:8000
13.213.58.228:8000 - Google Search
Gmail
Images
Google
Search Google or type a URL

Splunk home page open and put username and password



Instances | EC2 Management Co
Login | Splunk
Not secure | 13.213.58.228:8000/en-US/account/login?return_to=%2Fen-US%2F
Gmail
YouTube
Maps
AWS Console - Sign...
Google
Other bookmarks
splunk>enterprise
Sign In

First time signing in?

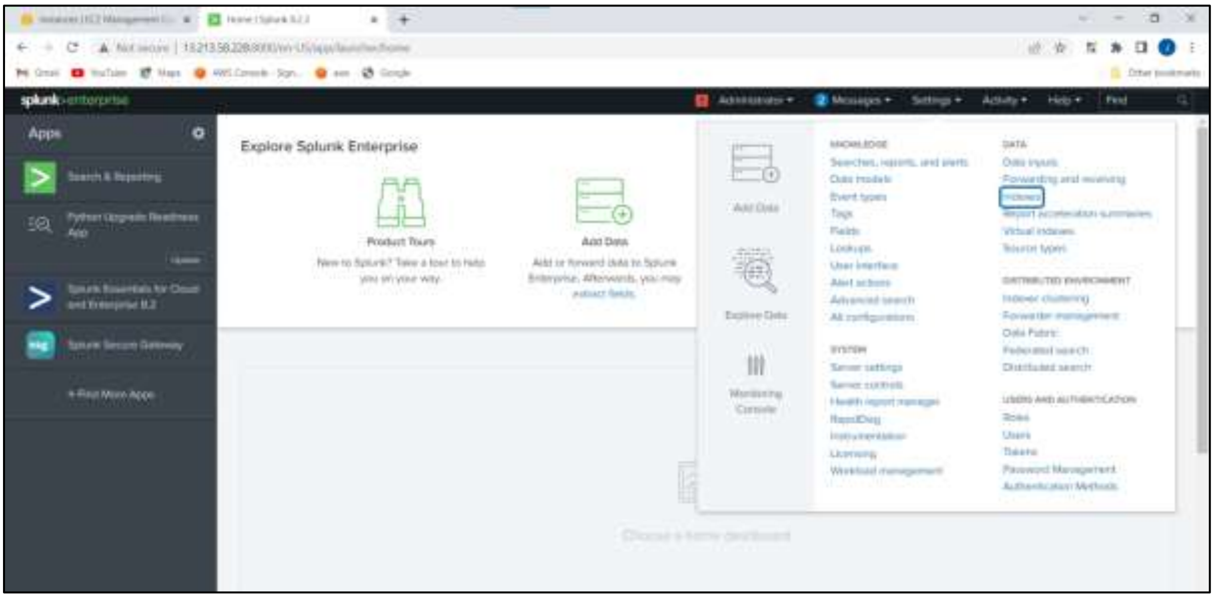
If you installed this instance, use the username and password you created at installation. Otherwise, use the username and password that your Splunk administrator gave you. If you've forgotten your username or password, please contact your Splunk administrator.

username admin

password This password you created when you installed this instance

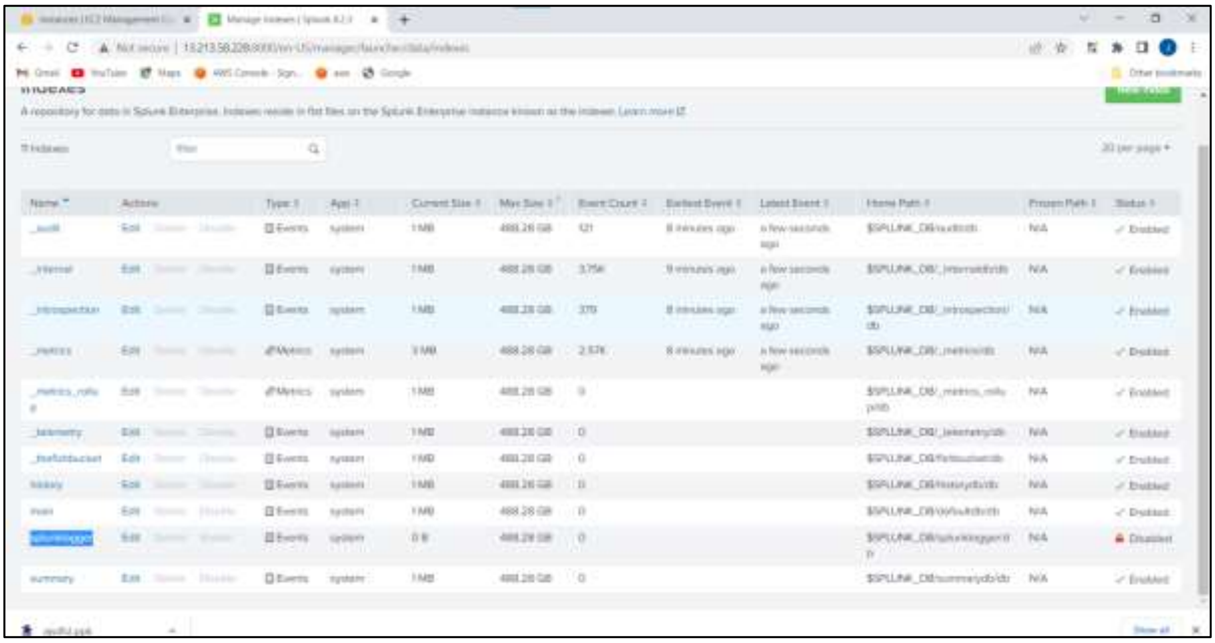
First time signing in?

Setting--->indexes--->



New to Splunk? Take a tour to help you on your way.

Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.



Indexes

A repository for data in Splunk Enterprise. Indexes reside in flat files on the Splunk Enterprise instance known as the indexer. Learn more

11 Indexes

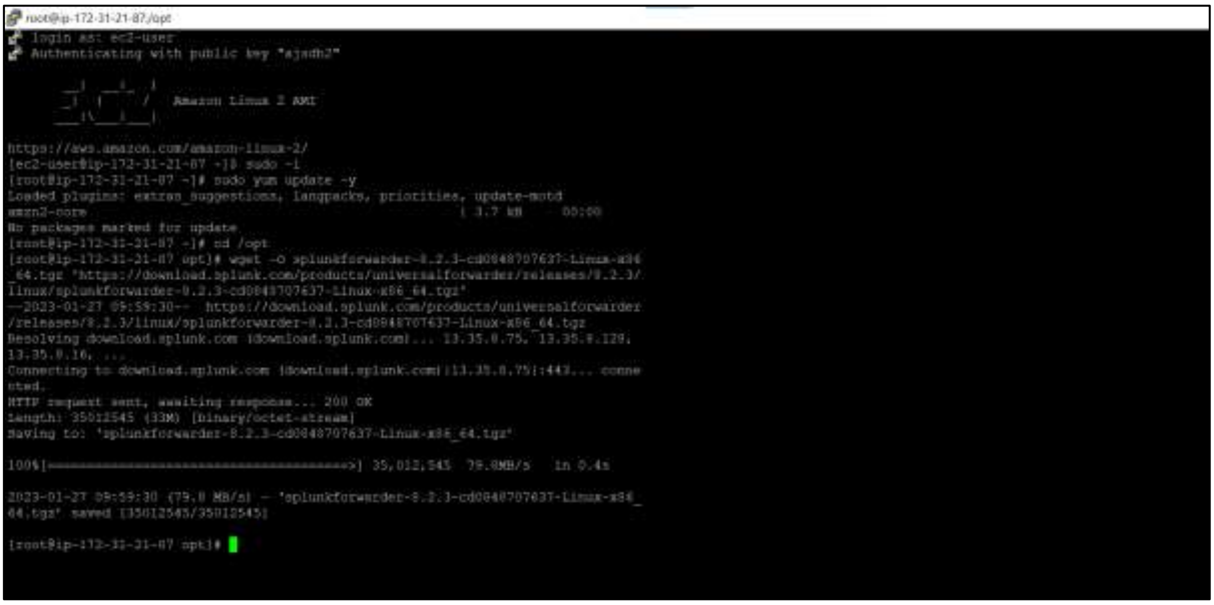
20 per page

Name	Actions	Type	App	Current Size	Max Size	Event Count	Earliest Event	Latest Event	Home Path	Frozen Path	Status
_audit	Edit Delete Disable	Events	system	1 MB	488.28 GB	121	8 minutes ago	a few seconds ago	$SPLUNK_DB/audit/db	N/A	✓ Enabled
_internal	Edit Delete Disable	Events	system	1 MB	488.28 GB	3.75K	9 minutes ago	a few seconds ago	$SPLUNK_DB/_internaldb/db	N/A	✓ Enabled
_introspection	Edit Delete Disable	Events	system	1 MB	488.28 GB	370	8 minutes ago	a few seconds ago	$SPLUNK_DB/_introspection/db	N/A	✓ Enabled
_metrics	Edit Delete Disable	Metrics	system	3 MB	488.28 GB	2.57K	8 minutes ago	a few seconds ago	$SPLUNK_DB/_metrics/db	N/A	✓ Enabled
_metrics_rollup	Edit Delete Disable	Metrics	system	1 MB	488.28 GB	0			$SPLUNK_DB/_metrics_rollup/db	N/A	✓ Enabled
_telemetry	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			$SPLUNK_DB/_telemetry/db	N/A	✓ Enabled
_thefishbucket	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			$SPLUNK_DB/fishbucket/db	N/A	✓ Enabled
history	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			$SPLUNK_DB/historydb/db	N/A	✓ Enabled
main	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			$SPLUNK_DB/defaultdb/db	N/A	✓ Enabled
splunklogger	Edit Delete Enable	Events	system	0 B	488.28 GB	0			$SPLUNK_DB/splunklogger/db	N/A	🔒 Disabled
summary	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			$SPLUNK_DB/summarydb/db	N/A	✓ Enabled

Step4:login slave server(**forwarder Server**)--->sudo –i

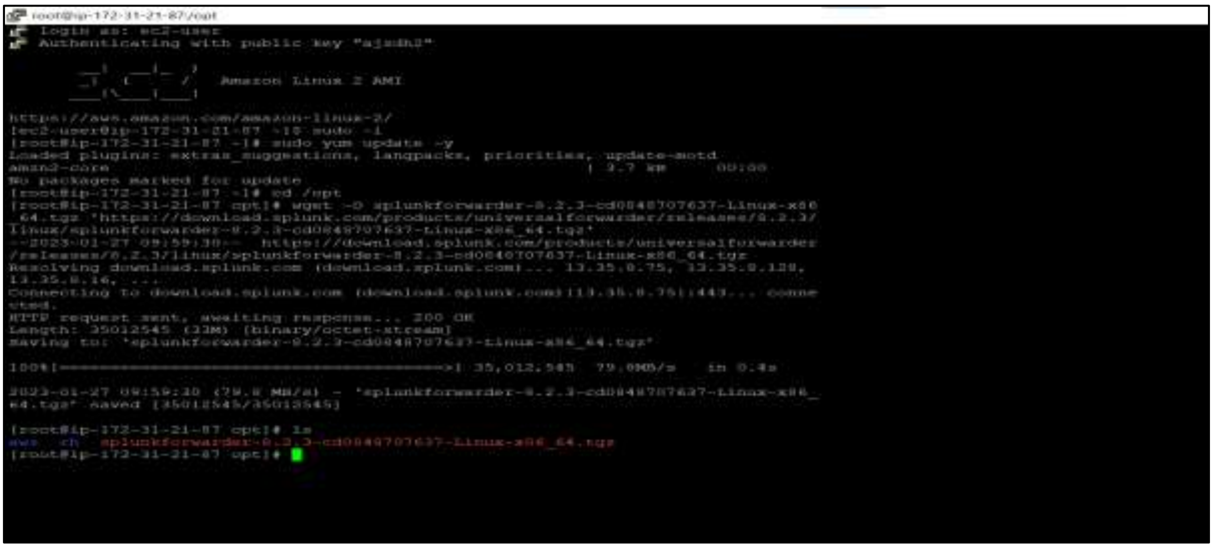
#sudo yum update –y (or) #cd /opt

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' ------>(splunk forwarder download)



```
root@ip-172-31-21-87:/opt
login as: ec2-user
Authenticating with public key "ajadh2"

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-21-87 ~]$ sudo -i
[root@ip-172-31-21-87 ~]# sudo yum update -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core                                               | 3.7 kB     00:00
No packages marked for update
[root@ip-172-31-21-87 ~]# cd /opt
[root@ip-172-31-21-87 opt]# 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'
--2023-01-27 09:59:30--  https://download.splunk.com/products/universalforwarder
/releases/8.2.3/linux/splunkforwarder-8.2.3-cd0848707637-Linux-x86_64.tgz
Resolving download.splunk.com (download.splunk.com)... 13.35.8.75, 13.35.8.128,
13.35.8.16, ...
Connecting to download.splunk.com (download.splunk.com)|13.35.8.75|:443... conne
cted.
HTTP request sent, awaiting response... 200 OK
Length: 35012545 (33M) [binary/octet-stream]
Saving to: 'splunkforwarder-8.2.3-cd0848707637-Linux-x86_64.tgz'

100%[======================================>] 35,012,545  79.8MB/s   in 0.4s

2023-01-27 09:59:30 (79.8 MB/s) - 'splunkforwarder-8.2.3-cd0848707637-Linux-x86_
64.tgz' saved [35012545/35012545]

[root@ip-172-31-21-87 opt]#
```

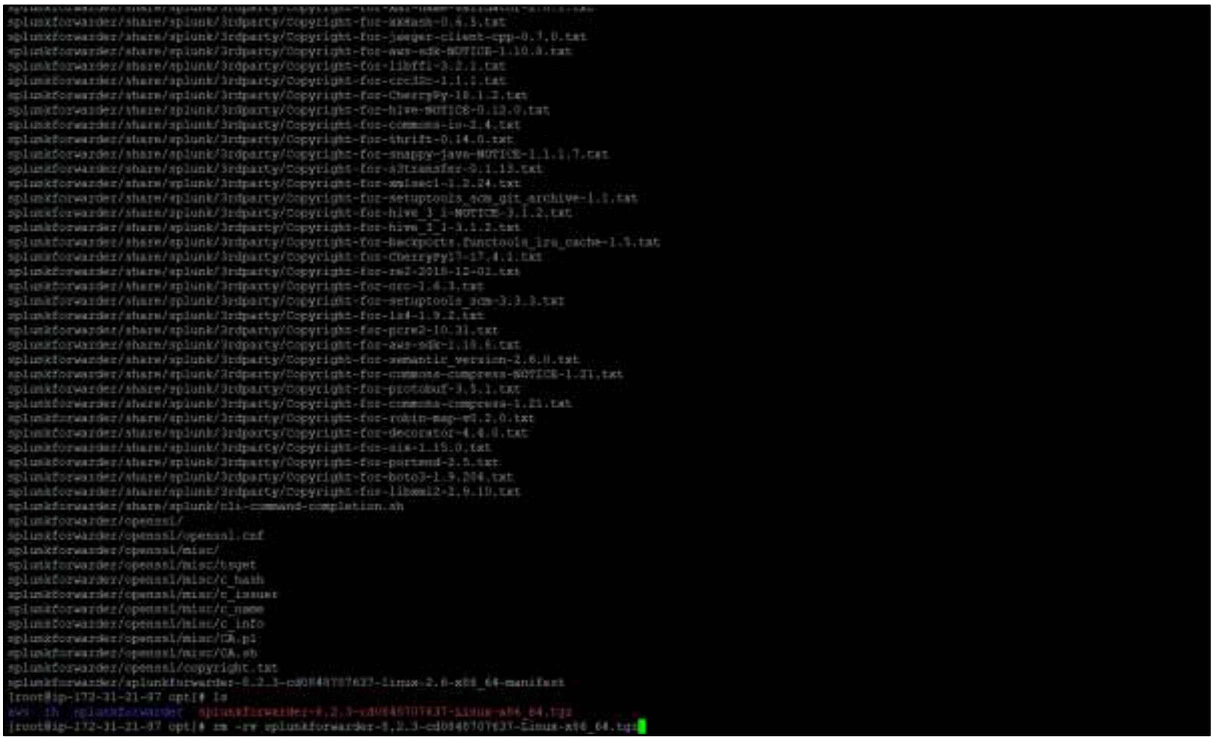
#ls ------>shown splunk file



```
root@ip-172-31-21-87:/opt
login as: ec2-user
Authenticating with public key "ajadh2"

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-21-87 ~]$ sudo -i
[root@ip-172-31-21-87 ~]# sudo yum update -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core                                               | 3.7 kB     00:00
No packages marked for update
[root@ip-172-31-21-87 ~]# cd /opt
[root@ip-172-31-21-87 opt]# 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'
--2023-01-27 09:59:30--  https://download.splunk.com/products/universalforwarder
/releases/8.2.3/linux/splunkforwarder-8.2.3-cd0848707637-Linux-x86_64.tgz
Resolving download.splunk.com (download.splunk.com)... 13.35.8.75, 13.35.8.128,
13.35.8.16, ...
Connecting to download.splunk.com (download.splunk.com)|13.35.8.75|:443... conne
cted.
HTTP request sent, awaiting response... 200 OK
Length: 35012545 (33M) [binary/octet-stream]
Saving to: 'splunkforwarder-8.2.3-cd0848707637-Linux-x86_64.tgz'

100%[======================================>] 35,012,545  79.8MB/s   in 0.4s

2023-01-27 09:59:30 (79.8 MB/s) - 'splunkforwarder-8.2.3-cd0848707637-Linux-x86_
64.tgz' saved [35012545/35012545]

[root@ip-172-31-21-87 opt]# ls
aws  ch  splunkforwarder-8.2.3-cd0848707637-Linux-x86_64.tgz
[root@ip-172-31-21-87 opt]#
```

#tar –xvzf splunkforwarder-8.2.3-cd0848707637-Linux-x86_64.tgz--->unzip

#rm –rv splunkforwarder-8.2.3-cd0848707637-Linux-x86_64.tgz



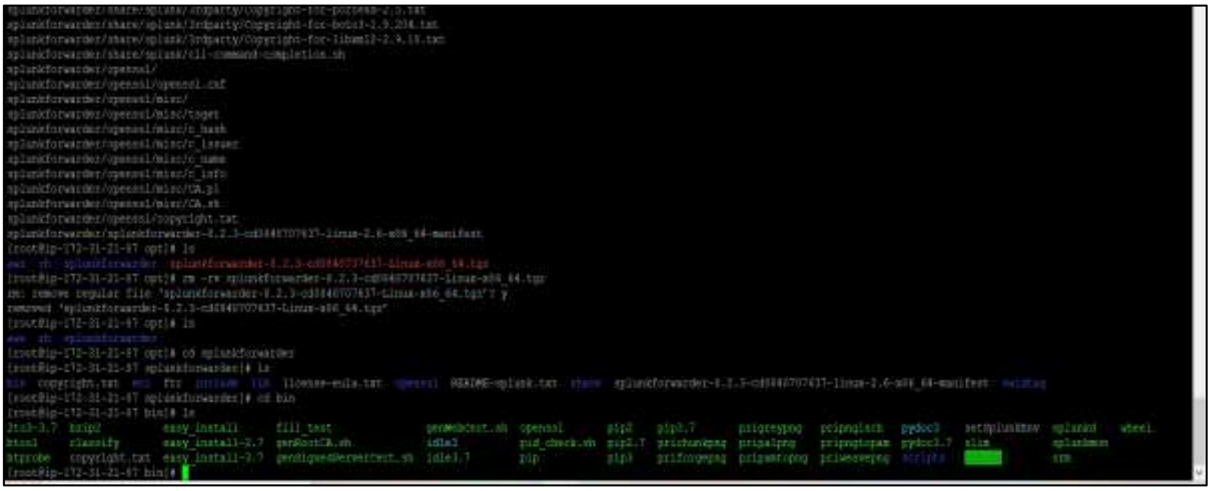
```
splunkforwarder/share/splunk/3rdparty/Copyright-for-[illegible]
splunkforwarder/share/splunk/3rdparty/Copyright-for-xxhash-0.4.5.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-jaeger-client-cpp-0.7.0.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-aws-sdk-NOTICE-1.10.6.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-libffi-3.2.1.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-crc32c-1.1.1.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-CherryPy-18.1.2.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-hive-NOTICE-0.12.0.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-commons-io-2.4.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-thrift-0.14.0.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-snappy-java-NOTICE-1.1.1.7.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-s3transfer-0.1.13.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-xmlsec1-1.2.24.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-setuptools_scm_git_archive-1.1.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-hive_1_1-NOTICE-3.1.2.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-hive_1_1-3.1.2.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-backports.functools_lru_cache-1.5.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-CherryPy17-17.4.1.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-re2-2018-12-01.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-orc-1.6.3.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-setuptools_scm-3.3.3.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-lz4-1.9.2.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-pcre2-10.31.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-aws-sdk-1.10.6.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-semantic_version-2.6.0.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-commons-compress-NOTICE-1.21.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-protobuf-3.5.1.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-commons-compress-1.21.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-robin-map-v0.2.0.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-decorator-4.4.0.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-six-1.15.0.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-portend-2.5.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-boto3-1.9.204.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-libxml2-2.9.10.txt
splunkforwarder/share/splunk/cli-command-completion.sh
splunkforwarder/openssl/
splunkforwarder/openssl/openssl.cnf
splunkforwarder/openssl/misc/
splunkforwarder/openssl/misc/tsget
splunkforwarder/openssl/misc/c_hash
splunkforwarder/openssl/misc/c_issuer
splunkforwarder/openssl/misc/c_name
splunkforwarder/openssl/misc/c_info
splunkforwarder/openssl/misc/CA.pl
splunkforwarder/openssl/misc/CA.sh
splunkforwarder/openssl/copyright.txt
splunkforwarder/splunkforwarder-8.2.3-cd0848707637-linux-2.6-x86_64-manifest
[root@ip-172-31-21-87 opt]# ls
aws  rh  splunkforwarder  splunkforwarder-8.2.3-cd0848707637-Linux-x86_64.tgz
[root@ip-172-31-21-87 opt]# rm -rv splunkforwarder-8.2.3-cd0848707637-Linux-x86_64.tgz
```

Removed zip file and show unzip file

#cd splunk

#cd bin

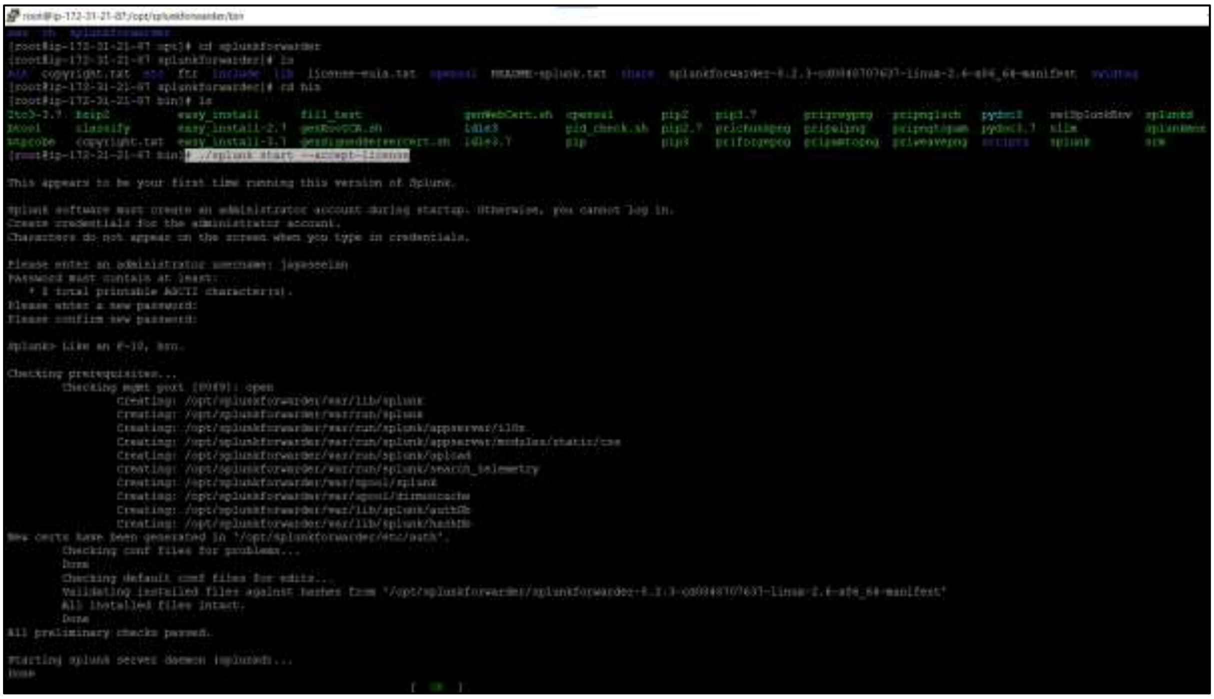
#ls ---->shown splunk



```
splunkforwarder/share/splunk/3rdparty/Copyright-for-portend-2.5.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-boto3-1.9.204.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-libxml2-2.9.10.txt
splunkforwarder/share/splunk/cli-command-completion.sh
splunkforwarder/openssl/
splunkforwarder/openssl/openssl.cnf
splunkforwarder/openssl/misc/
splunkforwarder/openssl/misc/tsget
splunkforwarder/openssl/misc/c_hash
splunkforwarder/openssl/misc/c_issuer
splunkforwarder/openssl/misc/c_name
splunkforwarder/openssl/misc/c_info
splunkforwarder/openssl/misc/CA.pl
splunkforwarder/openssl/misc/CA.sh
splunkforwarder/openssl/copyright.txt
splunkforwarder/splunkforwarder-8.2.3-cd0848707637-linux-2.6-x86_64-manifest
[root@ip-172-31-21-87 opt]# ls
aws  rh  splunkforwarder  splunkforwarder-8.2.3-cd0848707637-Linux-x86_64.tgz
[root@ip-172-31-21-87 opt]# rm -rv splunkforwarder-8.2.3-cd0848707637-Linux-x86_64.tgz
rm: remove regular file 'splunkforwarder-8.2.3-cd0848707637-Linux-x86_64.tgz'? y
removed 'splunkforwarder-8.2.3-cd0848707637-Linux-x86_64.tgz'
[root@ip-172-31-21-87 opt]# ls
aws  rh  splunkforwarder
[root@ip-172-31-21-87 opt]# cd splunkforwarder
[root@ip-172-31-21-87 splunkforwarder]# ls
bin  copyright.txt  etc  ftr  include  lib  license-eula.txt  openssl  README-splunk.txt  share  splunkforwarder-8.2.3-cd0848707637-linux-2.6-x86_64-manifest  swidtag
[root@ip-172-31-21-87 splunkforwarder]# cd bin
[root@ip-172-31-21-87 bin]# ls
2to3-3.7  bzip2          easy_install      fill_test               genWebCert.sh  openssl       pip2    pip3.7       prigreypng   pripnglsch   pydoc3    setSplunkEnv  splunkd    wheel
btool     classify       easy_install-2.7  genRootCA.sh            idle2          pid_check.sh  pip2.7  prichunkpng  pripalpng    pripngtopam  pydoc3.7  slim          splunkmon
btprobe   copyright.txt  easy_install-3.7  genSignedServerCert.sh  idle3.7        pip           pip3    priforgepng  pripamtopng  priweavepng  scripts   splunk        srm
[root@ip-172-31-21-87 bin]#
```

./splunk start --accept-license   ---->(splunk start)

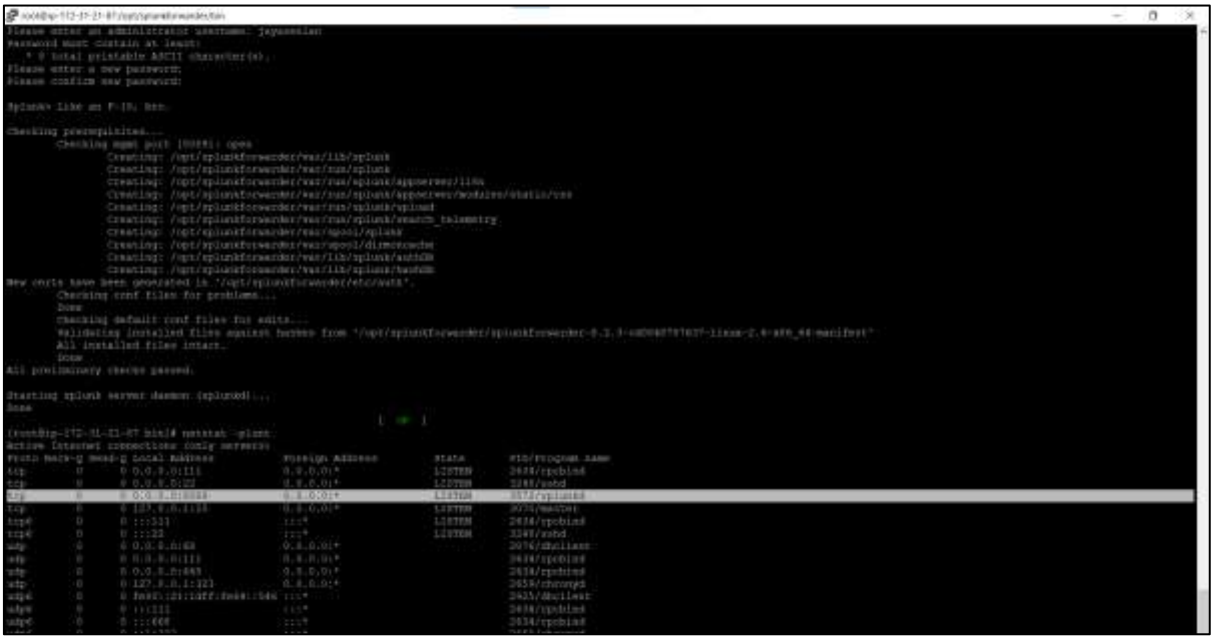
Username(jayaseelan)& password(jaya1234)



```
root@ip-172-31-21-87:/opt/splunkforwarder/bin
aws  rh  splunkforwarder
[root@ip-172-31-21-87 opt]# cd splunkforwarder
[root@ip-172-31-21-87 splunkforwarder]# ls
bin  copyright.txt  etc  ftr  include  lib  license-eula.txt  openssl  README-splunk.txt  share  splunkforwarder-8.2.3-cd0848707637-linux-2.6-x86_64-manifest  swidtag
[root@ip-172-31-21-87 splunkforwarder]# cd bin
[root@ip-172-31-21-87 bin]# ls
2to3-2.7  bzip2      easy_install      fill_test                genWebCert.sh  openssl       pip2    pip3.7      prigreypng   pripnglsch   pydoc3    setSplunkEnv  splunkd
btool     classify   easy_install-2.7  genRootCA.sh             idle3          pid_check.sh  pip2.7  prichunkpng prigalpng    pripngtopam  pydoc3.7  slim          splunkmon
bspcode   copyright.txt  easy_install-3.7  genSignedServerCert.sh  idle3.7      pip           pip3    priforgepng pripamtopng  priweavepng  scripts   splunk        srm
[root@ip-172-31-21-87 bin]# ./splunk start --accept-license

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

Splunk software must create an administrator account during startup. Otherwise, you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.

Please enter an administrator username: jayaseelan
Password must contain at least:
   * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:

Splunk> Like an F-18, bro.

Checking prerequisites...
        Checking mgmt port [8089]: open
                Creating: /opt/splunkforwarder/var/lib/splunk
                Creating: /opt/splunkforwarder/var/run/splunk
                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/run/splunk/search_telemetry
                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/splunkforwarder-8.2.3-cd0848707637-linux-2.6-x86_64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done
                                                           [  OK  ]
```

Now check port number

#netstat -plunt



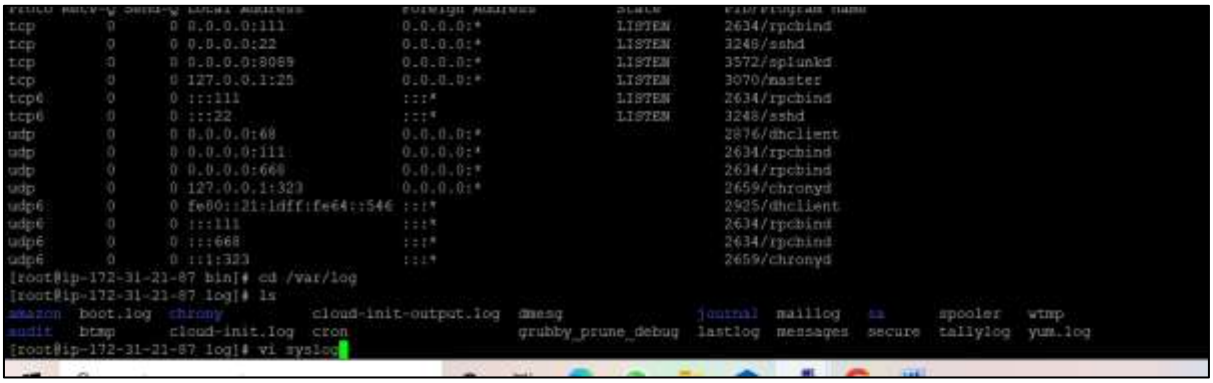
```
root@ip-172-31-21-87:/opt/splunkforwarder/bin
Please enter an administrator username: jayaseelan
Password must contain at least:
   * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:

Splunk> Like an F-18, bro.

Checking prerequisites...
        Checking mgmt port [8089]: open
                Creating: /opt/splunkforwarder/var/lib/splunk
                Creating: /opt/splunkforwarder/var/run/splunk
                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/run/splunk/search_telemetry
                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/splunkforwarder-8.2.3-cd0848707637-linux-2.6-x86_64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done
                                                           [  OK  ]

[root@ip-172-31-21-87 bin]# netstat -plunt
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      2634/rpcbind
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      3248/sshd
tcp        0      0 0.0.0.0:8089            0.0.0.0:*               LISTEN      3572/splunkd
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      3076/master
tcp6       0      0 :::111                  :::*                    LISTEN      2634/rpcbind
tcp6       0      0 :::22                   :::*                    LISTEN      3248/sshd
udp        0      0 0.0.0.0:68              0.0.0.0:*                           2976/dhclient
udp        0      0 0.0.0.0:111             0.0.0.0:*                           2634/rpcbind
udp        0      0 0.0.0.0:665             0.0.0.0:*                           2634/rpcbind
udp        0      0 127.0.0.1:323           0.0.0.0:*                           2659/chronyd
udp6       0      0 fe80::21:1dff:fe44::546 :::*                                3035/dhclient
udp6       0      0 :::111                  :::*                                2634/rpcbind
udp6       0      0 :::666                  :::*                                2634/rpcbind
```

It shownd splunk port number

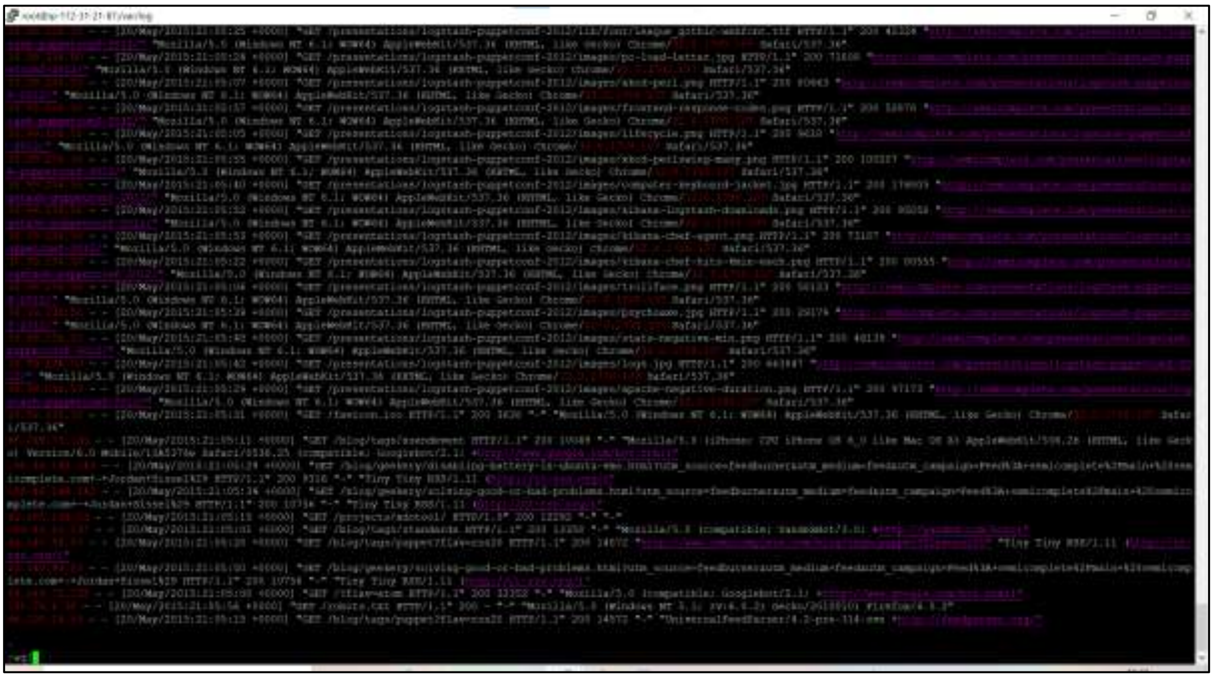
Step5:any content copy slave server

#cd /var/log

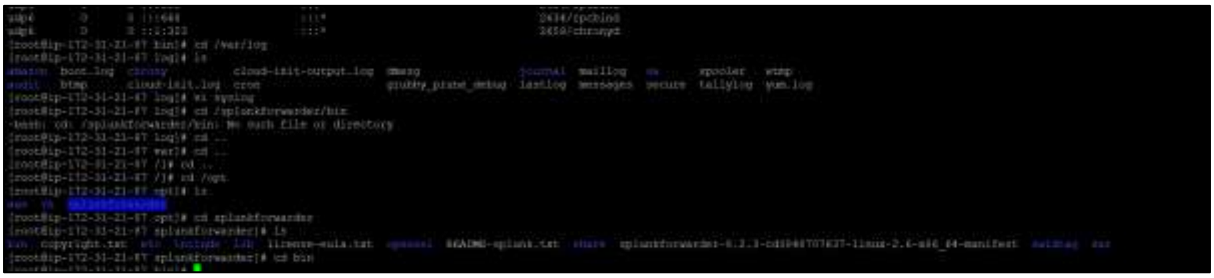
#vi syslog ---->copy content and paste and save(:wq!)



```
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      2634/rpcbind
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      3248/sshd
tcp        0      0 0.0.0.0:8089            0.0.0.0:*               LISTEN      3572/splunkd
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      3070/master
tcp6       0      0 :::111                  :::*                    LISTEN      2634/rpcbind
tcp6       0      0 :::22                   :::*                    LISTEN      3248/sshd
udp        0      0 0.0.0.0:68              0.0.0.0:*                           2876/dhclient
udp        0      0 0.0.0.0:111             0.0.0.0:*                           2634/rpcbind
udp        0      0 0.0.0.0:668             0.0.0.0:*                           2634/rpcbind
udp        0      0 127.0.0.1:323           0.0.0.0:*                           2659/chronyd
udp6       0      0 fe80::21:1dff:fe64::546 :::*                                2925/dhclient
udp6       0      0 :::111                  :::*                                2634/rpcbind
udp6       0      0 :::668                  :::*                                2634/rpcbind
udp6       0      0 ::1:323                 :::*                                2659/chronyd
[root@ip-172-31-21-87 bin]# cd /var/log
[root@ip-172-31-21-87 log]# ls
amazon  boot.log  chrony          cloud-init-output.log  dmesg               journal  maillog   rs      spooler   wtmp
audit   btmp      cloud-init.log  cron                   grubby_prune_debug  lastlog  messages  secure  tallylog  yum.log
[root@ip-172-31-21-87 log]# vi syslog
```



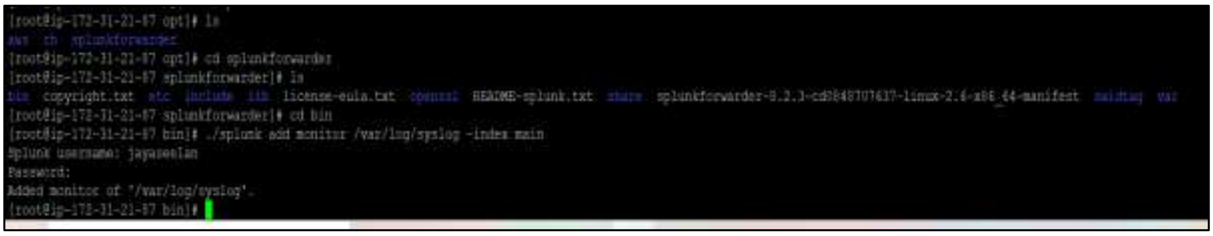
#cd /splunkforwarder/bin



```
udp6       0      0 :::668                  :::*                                2634/rpcbind
udp6       0      0 ::1:323                 :::*                                2659/chronyd
[root@ip-172-31-21-87 bin]# cd /var/log
[root@ip-172-31-21-87 log]# ls
amazon  boot.log  chrony          cloud-init-output.log  dmesg               journal  maillog   rs      spooler   wtmp
audit   btmp      cloud-init.log  cron                   grubby_prune_debug  lastlog  messages  secure  tallylog  yum.log
[root@ip-172-31-21-87 log]# vi syslog
[root@ip-172-31-21-87 log]# cd /splunkforwarder/bin
-bash: cd: /splunkforwarder/bin: No such file or directory
[root@ip-172-31-21-87 log]# cd ..
[root@ip-172-31-21-87 var]# cd ..
[root@ip-172-31-21-87 /]# cd ..
[root@ip-172-31-21-87 /]# cd /opt
[root@ip-172-31-21-87 opt]# ls
aws  rh  splunkforwarder
[root@ip-172-31-21-87 opt]# cd splunkforwarder
[root@ip-172-31-21-87 splunkforwarder]# ls
bin  copyright.txt  etc  include  lib  license-eula.txt  openssl  README-splunk.txt  share  splunkforwarder-6.2.3-[illegible]-linux-2.6-x86_64-manifest  swidtag  var
[root@ip-172-31-21-87 splunkforwarder]# cd bin
[root@ip-172-31-21-87 bin]#
```

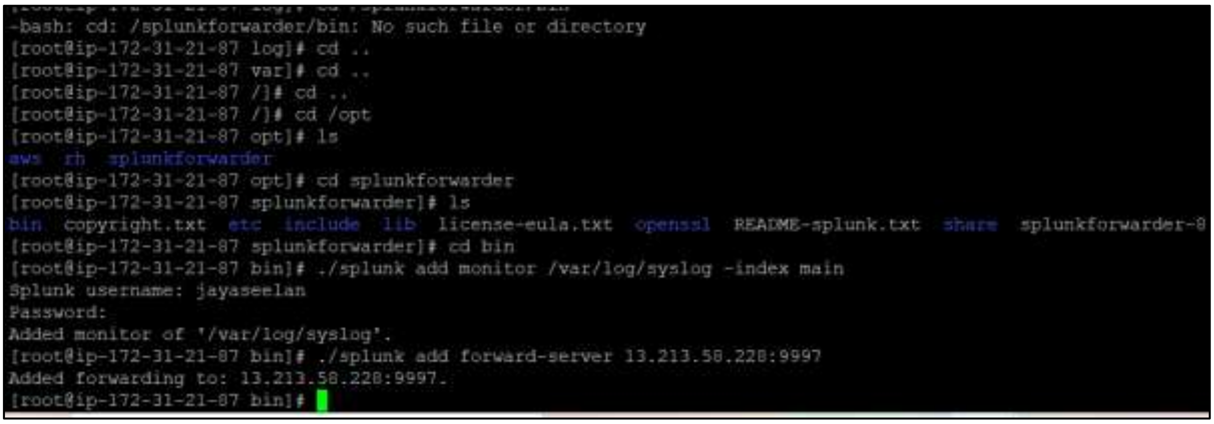
#./splunk add monitor /var/log/syslog -index main

Ask username and password give correctly



```
[root@ip-172-31-21-87 opt]# ls
aws  rh  splunkforwarder
[root@ip-172-31-21-87 opt]# cd splunkforwarder
[root@ip-172-31-21-87 splunkforwarder]# ls
bin  copyright.txt  etc  include  lib  license-eula.txt  openssl  README-splunk.txt  share  splunkforwarder-9.2.3-cd0848707637-linux-2.6-x86_64-manifest  swidtag  var
[root@ip-172-31-21-87 splunkforwarder]# cd bin
[root@ip-172-31-21-87 bin]# ./splunk add monitor /var/log/syslog -index main
Splunk username: jayaseelan
Password:
Added monitor of '/var/log/syslog'.
[root@ip-172-31-21-87 bin]#
```

#./splunk add forward-server Master's Public IP:9997
# ./splunk add forward-server 13.213.58.228:9997

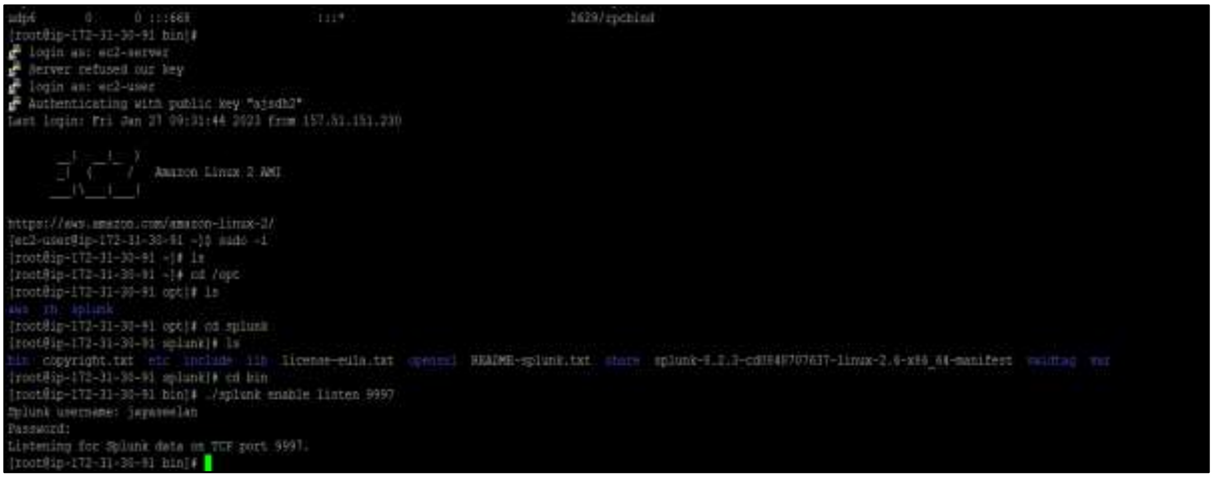


```
-bash: cd: /splunkforwarder/bin: No such file or directory
[root@ip-172-31-21-87 log]# cd ..
[root@ip-172-31-21-87 var]# cd ..
[root@ip-172-31-21-87 /]# cd ..
[root@ip-172-31-21-87 /]# cd /opt
[root@ip-172-31-21-87 opt]# ls
aws  rh  splunkforwarder
[root@ip-172-31-21-87 opt]# cd splunkforwarder
[root@ip-172-31-21-87 splunkforwarder]# ls
bin  copyright.txt  etc  include  lib  license-eula.txt  openssl  README-splunk.txt  share  splunkforwarder-8
[root@ip-172-31-21-87 splunkforwarder]# cd bin
[root@ip-172-31-21-87 bin]# ./splunk add monitor /var/log/syslog -index main
Splunk username: jayaseelan
Password:
Added monitor of '/var/log/syslog'.
[root@ip-172-31-21-87 bin]# ./splunk add forward-server 13.213.58.228:9997
Added forwarding to: 13.213.58.228:9997.
[root@ip-172-31-21-87 bin]#
```

Added forwarding to master server

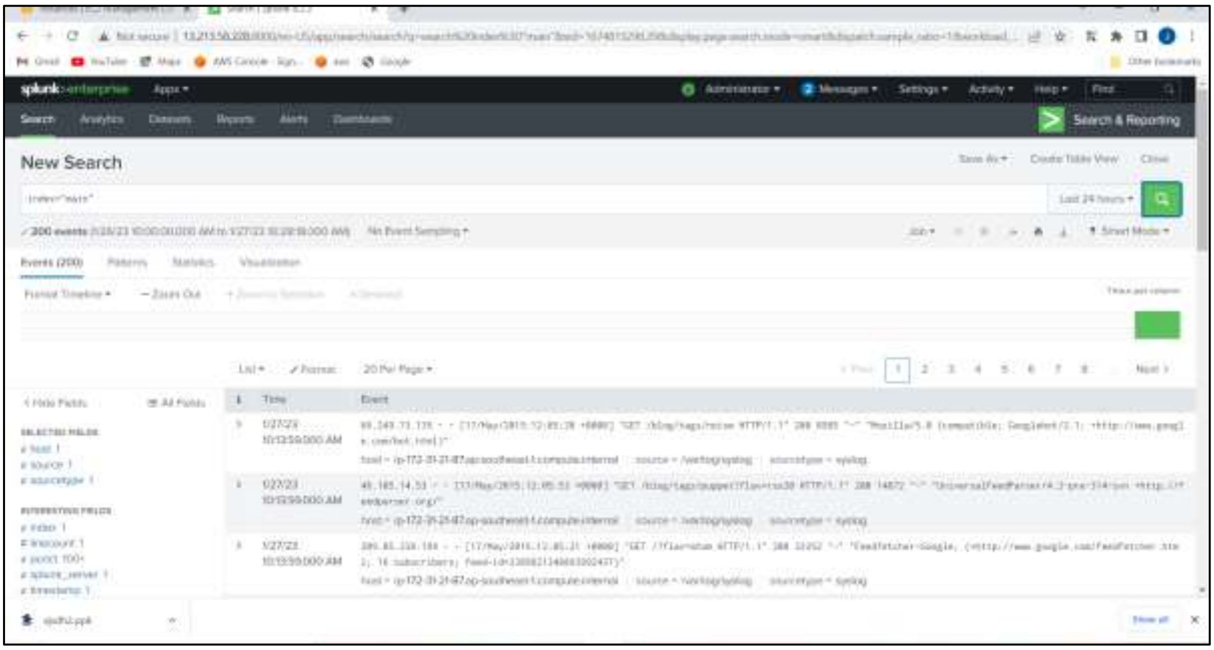
Step6:Master server --->#./splunk enable listen 9997

Username and password ask and give correctly



```
udp6       0      0 :::668                  :::*                                2629/rpcbind
[root@ip-172-31-30-91 bin]#
login as: ec2-server
Server refused our key
login as: ec2-user
Authenticating with public key "ajsdh2"
Last login: Fri Jan 27 09:31:44 2023 from 157.51.151.230

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-30-91 ~]$ sudo -i
[root@ip-172-31-30-91 ~]# ls
[root@ip-172-31-30-91 ~]# cd /opt
[root@ip-172-31-30-91 opt]# ls
aws  rh  splunk
[root@ip-172-31-30-91 opt]# cd splunk
[root@ip-172-31-30-91 splunk]# ls
bin  copyright.txt  etc  include  lib  license-eula.txt  openssl  README-splunk.txt  share  splunk-9.2.3-cd0848707637-linux-2.6-x86_64-manifest  swidtag  var
[root@ip-172-31-30-91 splunk]# cd bin
[root@ip-172-31-30-91 bin]# ./splunk enable listen 9997
Splunk username: jayaseelan
Password:
Listening for Splunk data on TCP port 9997.
[root@ip-172-31-30-91 bin]#
```

Step7:splunk home page---->search(index=”main”)



index="main"

✓ 200 events (1/26/23 10:00:00.000 AM to 1/27/23 10:29:18.000 AM)

i	Time	Event
>	1/27/23 10:13:59.000 AM	66.249.73.135 - - [17/May/2015:12:05:28 +0000] "GET /blog/tags/noise HTTP/1.1" 200 8085 "-" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)" host = ip-172-31-21-87.ap-southeast-1.compute.internal | source = /var/log/syslog | sourcetype = syslog
>	1/27/23 10:13:59.000 AM	46.105.14.53 - - [17/May/2015:12:05:53 +0000] "GET /blog/tags/puppet?flav=rss20 HTTP/1.1" 200 14872 "-" "UniversalFeedParser/4.2-pre-314-svn +http://feedparser.org/" host = ip-172-31-21-87.ap-southeast-1.compute.internal | source = /var/log/syslog | sourcetype = syslog
>	1/27/23 10:13:59.000 AM	209.85.238.199 - - [17/May/2015:12:05:21 +0000] "GET /?flav=atom HTTP/1.1" 200 32352 "-" "FeedFetcher-Google; (+http://www.google.com/feedfetcher.html; 16 subscribers; feed-id=3389821348893992437)" host = ip-172-31-21-87.ap-southeast-1.compute.internal | source = /var/log/syslog | sourcetype = syslog

It will shown all log deatails..