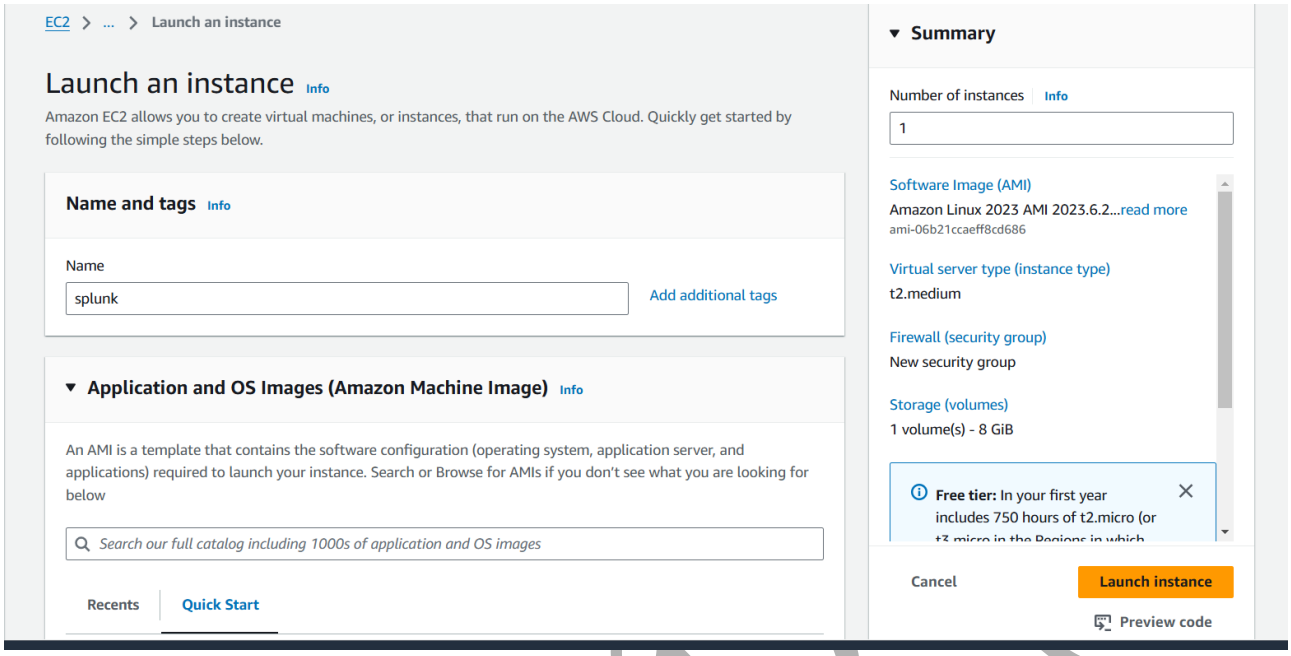
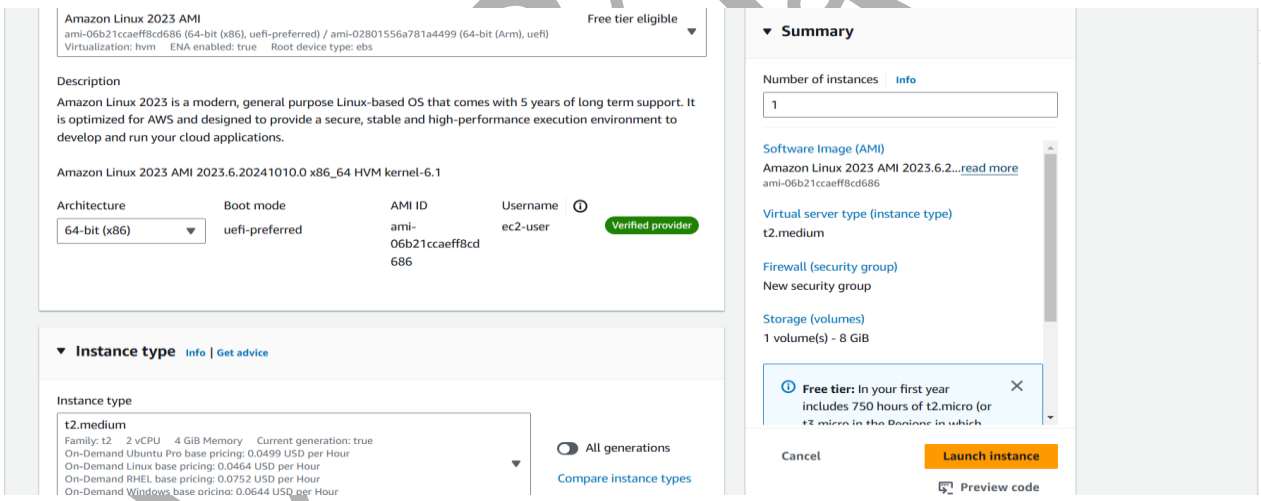
SPLUNK LOGS

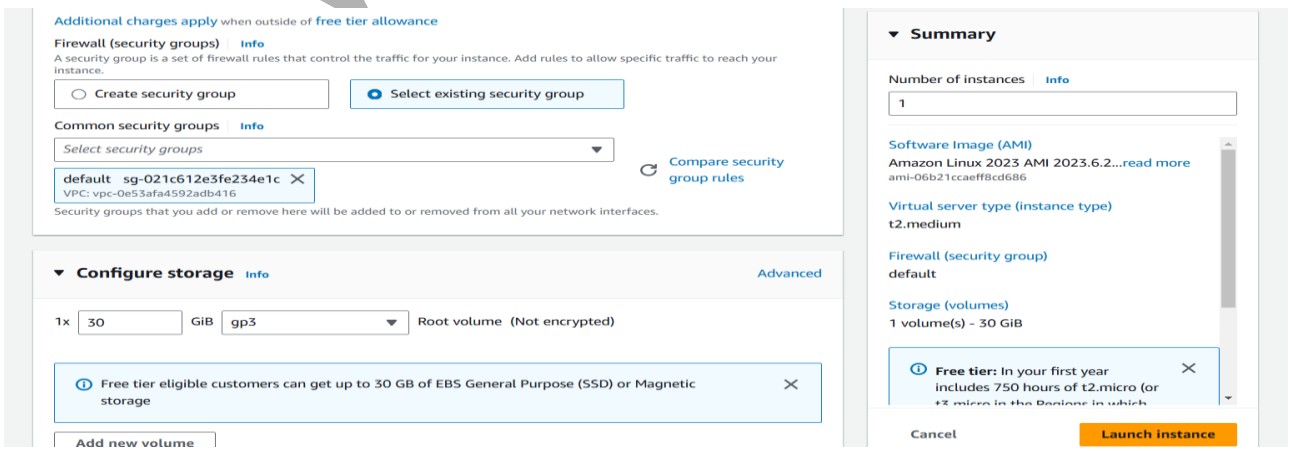
Create ec2 with below specifications



- Instance type is t2.medium



- Select sg and allow all traffic
- Take ebs volume 30gb



- Connect to instance install splunk

wget -O splunk-9.3.1-0b8d769cb912.x86_64.rpm "https://download.splunk.com/products/splunk/releases/9.3.1/linux/splunk-9.3.1-0b8d769cb912.x86_64.rpm"

```
[ec2-user@ip-172-31-91-152 ~]$ wget -O splunk-9.3.1-0b8d769cb912.x86_64.rpm "https://download.splunk.com/products/splunk/releases/9.3.1/linux/splunk-9.3.1-0b8d769
cb912.x86_64.rpm"

--2024-11-06 08:20:52--  https://download.splunk.com/products/splunk/releases/9.3.1/linux/splunk-9.3.1-0b8d769cb912.x86_64.rpm
Resolving download.splunk.com (download.splunk.com)... 3.167.37.33, 3.167.37.110, 3.167.37.9, ...
Connecting to download.splunk.com (download.splunk.com)|3.167.37.33|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 990009597 (944M) [binary/octet-stream]
Saving to: 'splunk-9.3.1-0b8d769cb912.x86_64.rpm'

splunk-9.3.1-0b8d769cb912.x86_64.rpm     100%[=============================================================================>] 944.15M  77.4MB/s    in 12s

2024-11-06 08:21:04 (76.0 MB/s) - 'splunk-9.3.1-0b8d769cb912.x86_64.rpm' saved [990009597/990009597]

[ec2-user@ip-172-31-91-152 ~]$
```

- Install downloaded rpm package

sudo yum install splunk-9.3.1-0b8d769cb912.x86_64.rpm -y

```
[ec2-user@ip-172-31-91-152 ~]$ ls
splunk-9.3.1-0b8d769cb912.x86_64.rpm
[ec2-user@ip-172-31-91-152 ~]$ sudo yum install splunk-9.3.1-0b8d769cb912.x86_64.rpm -y
Last metadata expiration check: 0:01:49 ago on Wed Nov  6 08:20:09 2024.
Dependencies resolved.
================================================================================
 Package                 Architecture            Version                 Repository                  Size
================================================================================
Installing:
 splunk                  x86_64                  9.3.1-0b8d769cb912      @commandline                944 M

Transaction Summary
================================================================================
Install  1 Package

Total size: 944 M
Installed size: 2.5 G
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :                                                        1/1
```

- Switch to root user then go to splunk bin directory

cd /opt/splunk/bin/

```
[ec2-user@ip-172-31-91-152 ~]$ sudo su -
[root@ip-172-31-91-152 ~]# cd /opt/splunk/bin/
[root@ip-172-31-91-152 bin]#
```

- Strat the splunk

sudo ./splunk start --accept-license --answer-yes

- It will ask usename password

Username :admin

Password : admin1234 [give your custom password]

```
[root@ip-172-31-91-152 bin]# sudo ./splunk start --accept-license --answer-yes

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: admin
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
.....................................................................................................................
.....................................................+++++
e is 65537 (0x10001)
writing RSA key

Generating RSA private key, 2048 bit long modulus
.+++++
.....................................................................................+++++
e is 65537 (0x10001)
writing RSA key

Moving '/opt/splunk/share/splunk/search_mrsparkle/modules.new' to '/opt/splunk/share/splunk/search_mrsparkle/modules'.
```

- Successfully started the splunk

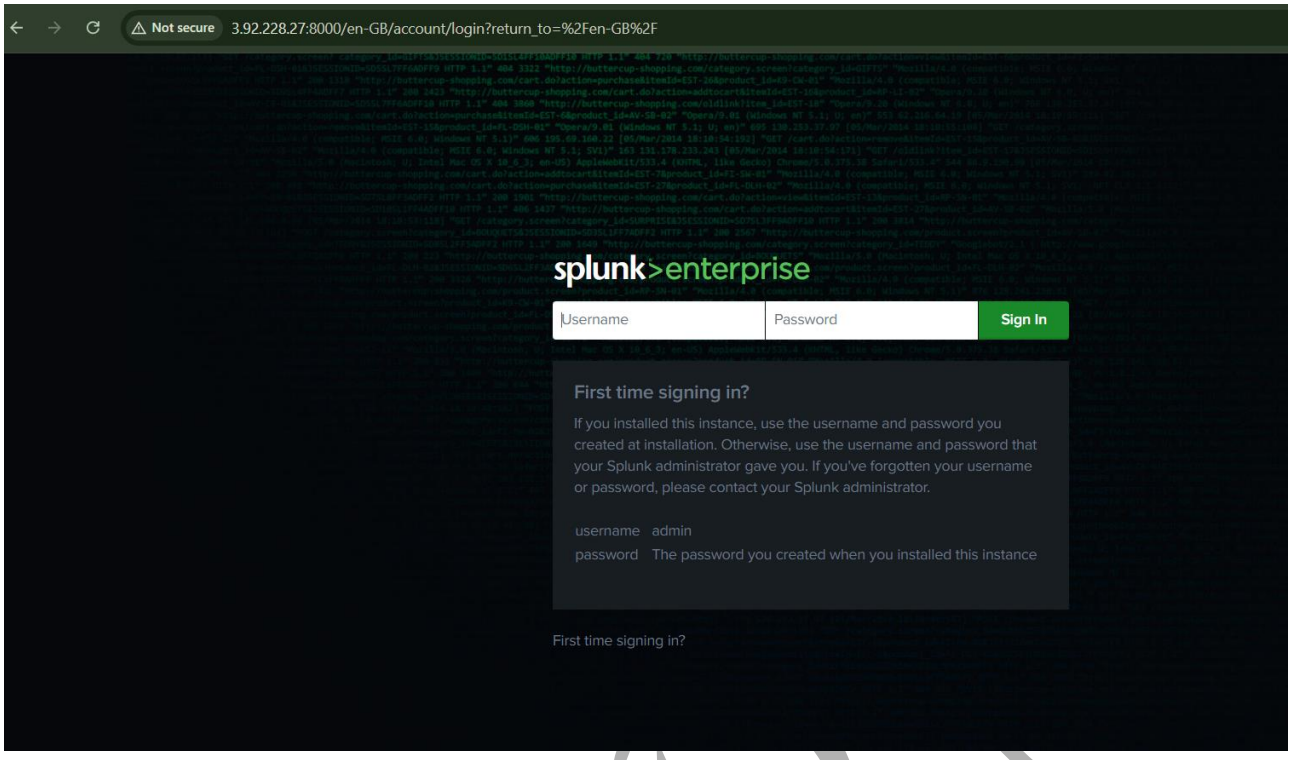
```
Signature ok
subject=/CN=ip-172-31-91-152.ec2.internal/O=SplunkUser
Getting CA Private Key
writing RSA key
PYTHONHTTPSVERIFY is set to 0 in splunk-launch.conf disabling certificate validation for the httplib
eter; must be set to "1" for increased security
Done
                                                           [  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-172-31-91-152.ec2.internal:8000

[root@ip-172-31-91-152 bin]#
```

- Enable the splunk

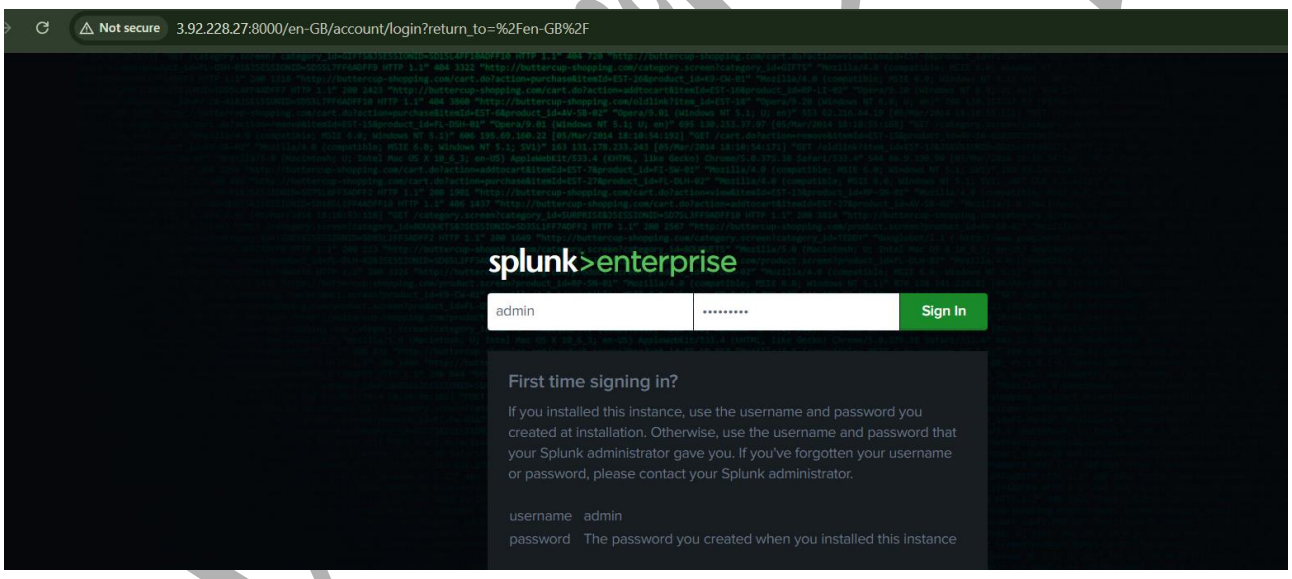
./splunk enable boot-start

```
[root@ip-172-31-86-68 bin]# ./splunk enable boot-start
Init script installed at /etc/init.d/splunk.
Init script is configured to run at boot.
[root@ip-172-31-86-68 bin]#
```

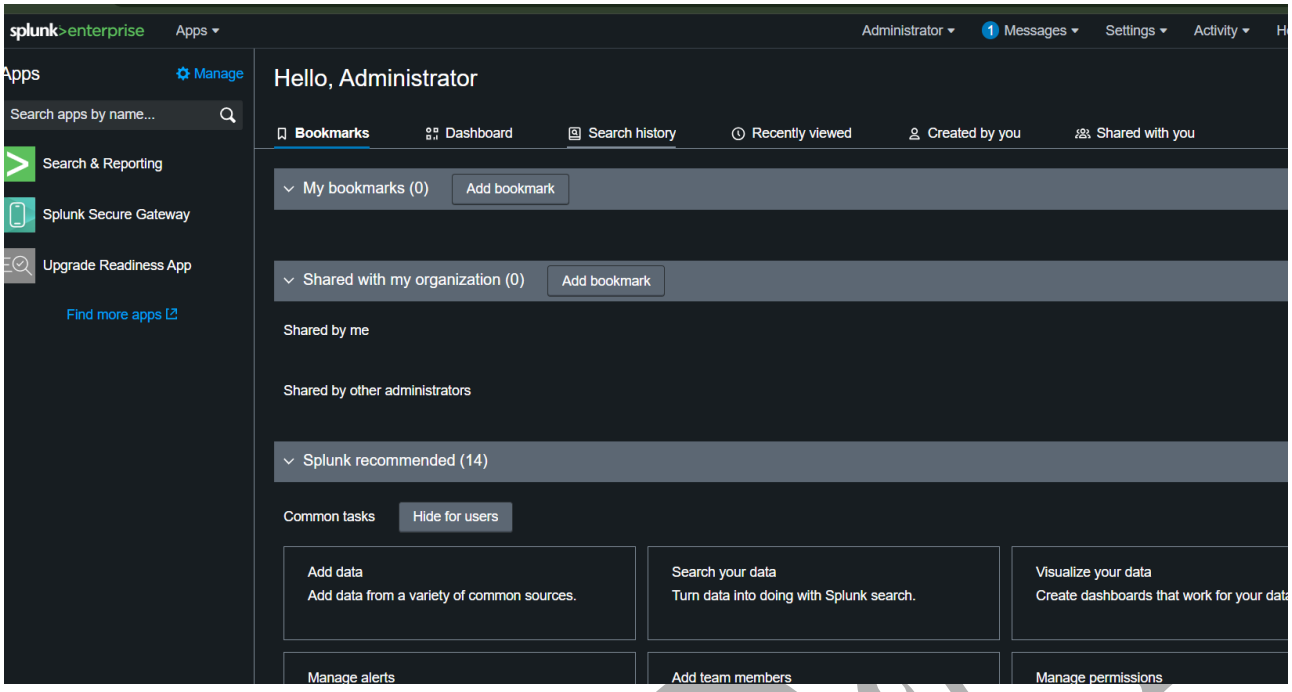
- the public ip and enter port
- http://3.92.228.27:8000



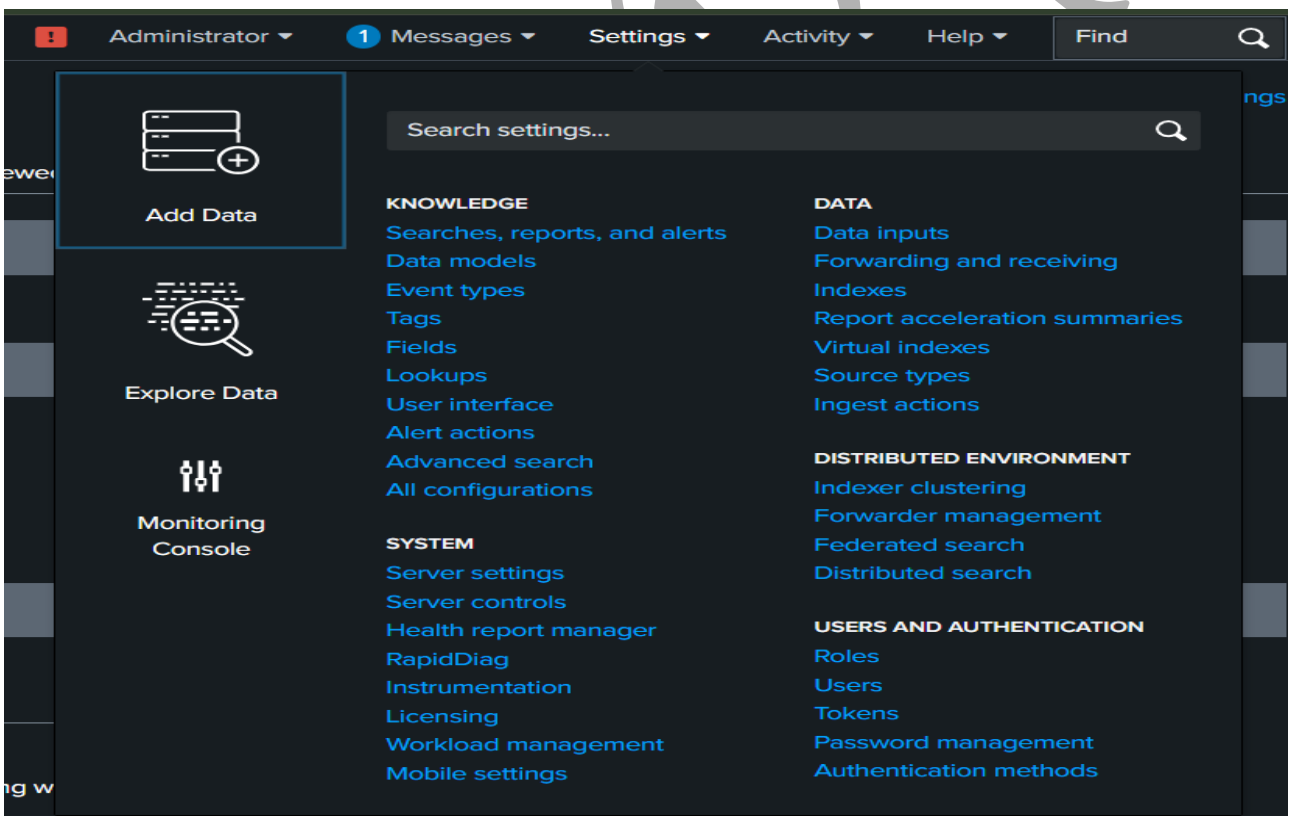
- enter the user name and password



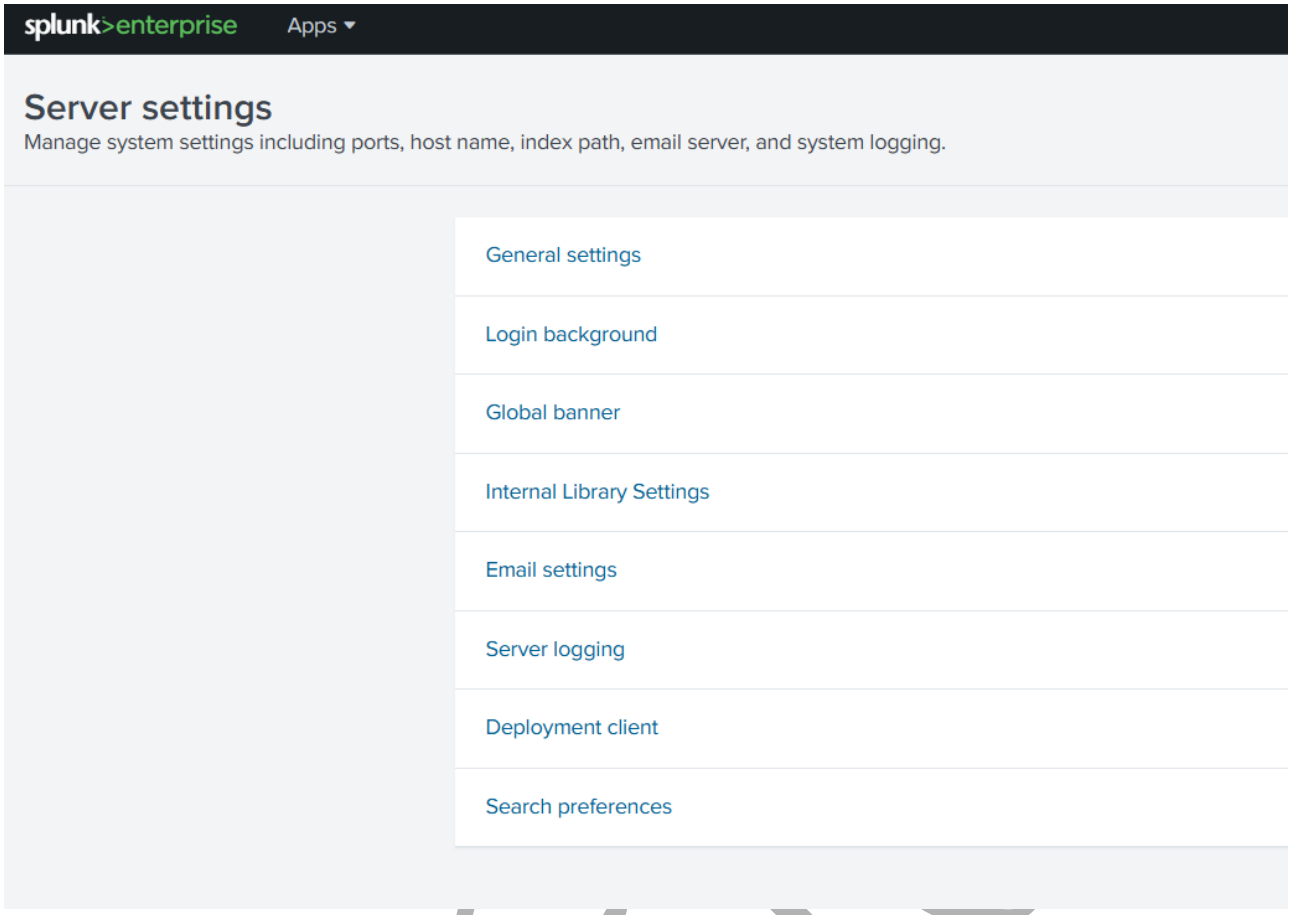
- this is the dashboard of splunk



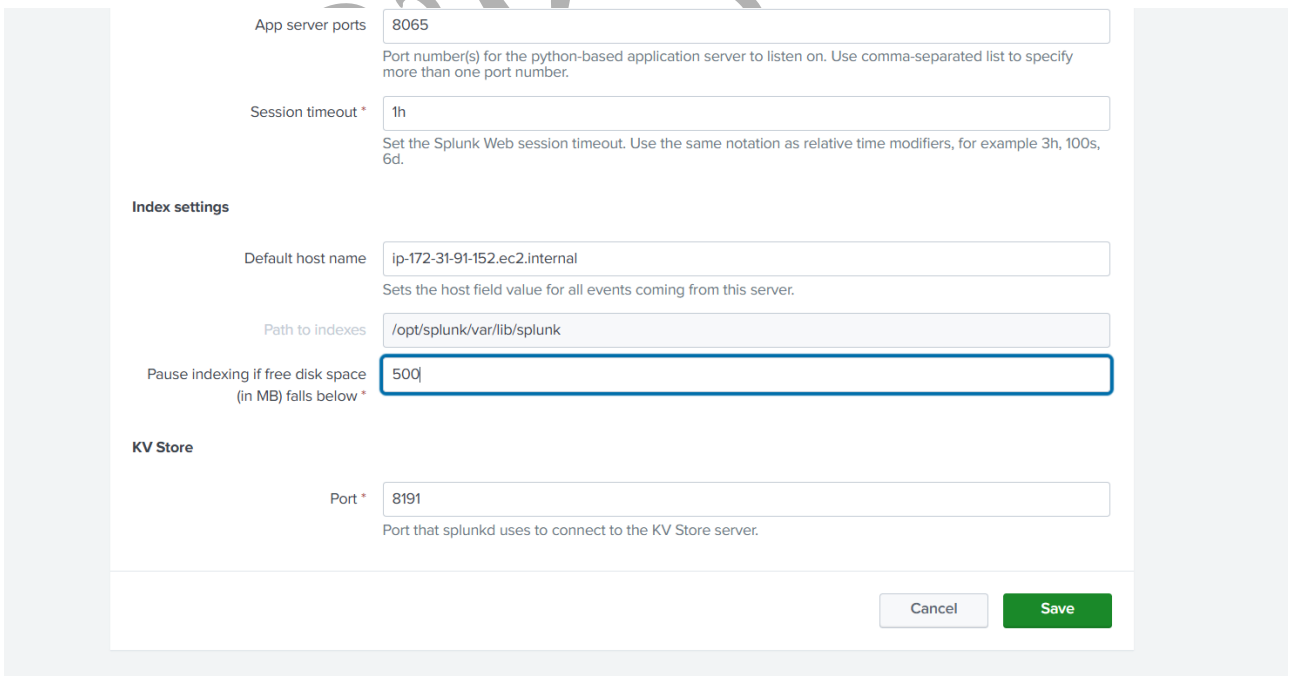
- click on settings
- select server settings



- after selecting server settings
- click on general settings



- change free disk space 5000 to 500
- than save it



- Now its time to install splunk forwader

wget -O splunkforwarder-9.3.1-0b8d769cb912.x86_64.rpm "https://download.splunk.com/products/universalforwarder/releases/9.3.1/linux/splunkforwarder-9.3.1-0b8d769cb912.x86_64.rpm"

```
[root@ip-172-31-91-152 ~]# wget -O splunkforwarder-9.3.1-0b8d769cb912.x86_64.rpm "https://download.splunk.com/products/universalforwarder/releases/9.3.1/linu
unkforwarder-9.3.1-0b8d769cb912.x86_64.rpm"
--2024-11-06 08:31:35--  https://download.splunk.com/products/universalforwarder/releases/9.3.1/linux/splunkforwarder-9.3.1-0b8d769cb912.x86_64.rpm
Resolving download.splunk.com (download.splunk.com)... 3.167.37.124, 3.167.37.110, 3.167.37.33, ...
Connecting to download.splunk.com (download.splunk.com)|3.167.37.124|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 49250063 (47M) [binary/octet-stream]
Saving to: 'splunkforwarder-9.3.1-0b8d769cb912.x86_64.rpm'

splunkforwarder-9.3.1-0b8d769cb912.x86_6 100%[=====================================================================================>]  46.97M  88.2MB/s    in 0.5s

2024-11-06 08:31:35 (88.2 MB/s) - 'splunkforwarder-9.3.1-0b8d769cb912.x86_64.rpm' saved [49250063/49250063]

[root@ip-172-31-91-152 ~]#
```

- Install downloaded rpm package

sudo yum install splunkforwarder-9.3.1-0b8d769cb912.x86_64.rpm -y

```
[root@ip-172-31-91-152 ~]# sudo yum install splunkforwarder-9.3.1-0b8d769cb912.x86_64.rpm -y
Last metadata expiration check: 0:11:55 ago on Wed Nov  6 08:20:09 2024.
Dependencies resolved.
================================================================================================================================================
 Package                          Architecture                 Version                                  Repository
================================================================================================================================================
Installing:
 splunkforwarder                  x86_64                       9.3.1-0b8d769cb912                       @commandline

Transaction Summary
================================================================================================================================================
Install  1 Package

Total size: 47 M
Installed size: 132 M
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :
  Running scriptlet: splunkforwarder-9.3.1-0b8d769cb912.x86_64
  Installing       : splunkforwarder-9.3.1-0b8d769cb912.x86_64
  Running scriptlet: splunkforwarder-9.3.1-0b8d769cb912.x86_64
find: '/opt/splunkforwarder/lib/python3.7/site-packages': No such file or directory
find: '/opt/splunkforwarder/lib/python3.9/site-packages': No such file or directory
```

- Switch to splunkforwarder bin directory

cd /opt/splunkforwarder/bin/

```
[root@ip-172-31-91-152 ~]# cd /opt/splunkforwarder/bin/
[root@ip-172-31-91-152 bin]#
```

- Strat the splunk

sudo ./splunk start --accept-license --answer-yes

- It will ask usename password
- Better to give splunk credentials

Username :admin

Password : admin1234 [give your custom password]

```
[root@ip-172-31-91-152 bin]# sudo ./splunk start --accept-license --answer-yes
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"

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: admin
Password must contain at least:
   * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
Creating unit file...
Important: splunk will start under systemd as user: splunkfwd
The unit file has been created.
```

- It will ask mgmt port change just give yes
- Then enter port number 8091

```
        Checking mgmt port [8089]: not available
ERROR: mgmt port [8089] - port is already bound.  Splunk needs to use this port.
Would you like to change ports? [y/n]: y
Enter a new mgmt port: 8091
Setting mgmt to port: 8091
The server's splunkd port has been changed.
8       Checking mgmt port [8091]: open
```

- Splunk forwarder is successfully started

```
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/splunkforwarc
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done
                                                           [  OK  ]
[root@ip-172-31-91-152 bin]#
```

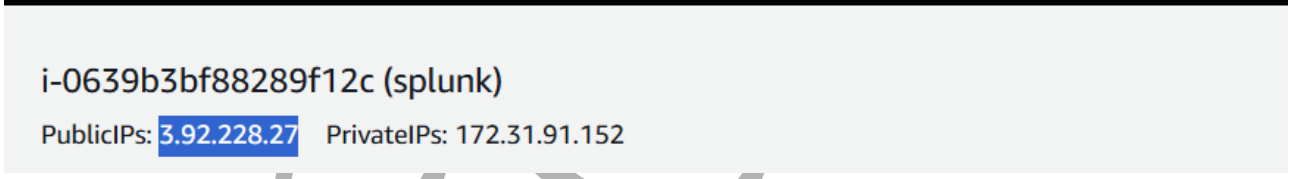
- We need to add forward server
- This splunk forwarder forwared the logs to splunk

./splunk add forward-server <your splunk public-ip>:9997

Ex: ./splunk add forward-server 8.253.63.35:9997

- It will ask your splunk user name and password

```
[root@ip-172-31-91-152 bin]# ./splunk add forward-server 3.92.228.27:9997
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Splunk username: admin
Password:
Added forwarding to: 3.92.228.27:9997.
[root@ip-172-31-91-152 bin]#
```



- After that restart the splunk forwarder

./splunk restart

```
[root@ip-172-31-91-152 bin]# ./splunk restart
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Stopping splunkd...
Shutting down.  Please wait, as this may take a few minutes.
                                                           [  OK  ]
Stopping splunk helpers...
                                                           [  OK  ]
Done.
splunkd.pid doesn't exist...

Splunk> Finding your faults, just like mom.

Checking prerequisites...
        Checking mgmt port [8091]: open
        Checking conf files for problems...
        Done
        Checking default conf files for edits...
        Validating installed files against hashes from '/opt/splunkforwarder/splunkforwa
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done
                                                           [  OK  ]
[root@ip-172-31-91-152 bin]#
```

- Now add the log path to splunk forwarder

./splunk add monitor /var/log

- Enter the splunk user name and password

```
[root@ip-172-31-86-68 bin]# ./splunk add monitor /var/log
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Your session is invalid.  Please login.
Splunk username: admin
Password:
Added monitor of '/var/log'.
[root@ip-172-31-86-68 bin]#
```

- Now again restart the splunk forwarder
- Restart is mandatory after doing any changes

```
[root@ip-172-31-91-152 bin]# ./splunk restart
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Stopping splunkd...
Shutting down.  Please wait, as this may take a few minutes.
                                                           [  OK  ]
Stopping splunk helpers...
                                                           [  OK  ]
Done.
splunkd.pid doesn't exist...

Splunk> Finding your faults, just like mom.

Checking prerequisites...
        Checking mgmt port [8091]: open
        Checking conf files for problems...
        Done
        Checking default conf files for edits...
        Validating installed files against hashes from '/opt/splunkforwarder/splunkforwa
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done
                                                           [  OK  ]
[root@ip-172-31-91-152 bin]#
```

- Now switch to splunk bin folder

cd /opt/splunk/bin

```
[root@ip-172-31-91-152 bin]# cd /opt/splunk/bin
[root@ip-172-31-91-152 bin]#
```

- Enable the 9997 port requests

./splunk enable listen 9997

- It will ask the username and password just enter and continue

```
[root@ip-172-31-91-152 bin]# ./splunk enable listen 9997
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.
Splunk username: admin
Password:
Listening for Splunk data on TCP port 9997.
[root@ip-172-31-91-152 bin]#
```

- Restart the splunk

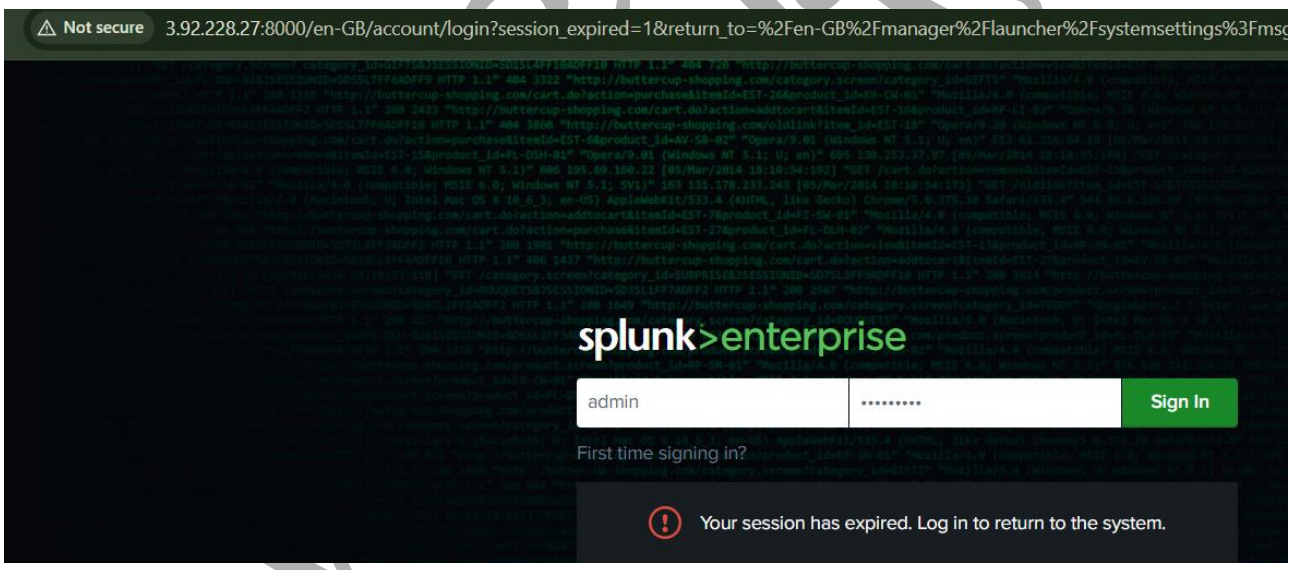
./splunk restart

```
[root@ip-172-31-91-152 bin]# ./splunk restart
Stopping splunkd...
Shutting down.  Please wait, as this may take a few minutes.
..                                                         [  OK  ]
Stopping splunk helpers...
                                                           [  OK  ]
Done.

Splunk> Finding your faults, just like mom.

Checking prerequisites...
        Checking http port [8000]: open
        Checking mgmt port [8089]: open
        Checking appserver port [127.0.0.1:8065]: open
        Checking kvstore port [8191]: open
        Checking configuration... Done.
        Checking critical directories...        Done
        Checking indexes...
                Validated: _audit _configtracker _dsappevent _dsclient _dsphonehome _internal _introspect
story 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-9.3.1-0b8d769cb912-linux-2.6-x
        All installed files intact.
        Done
```

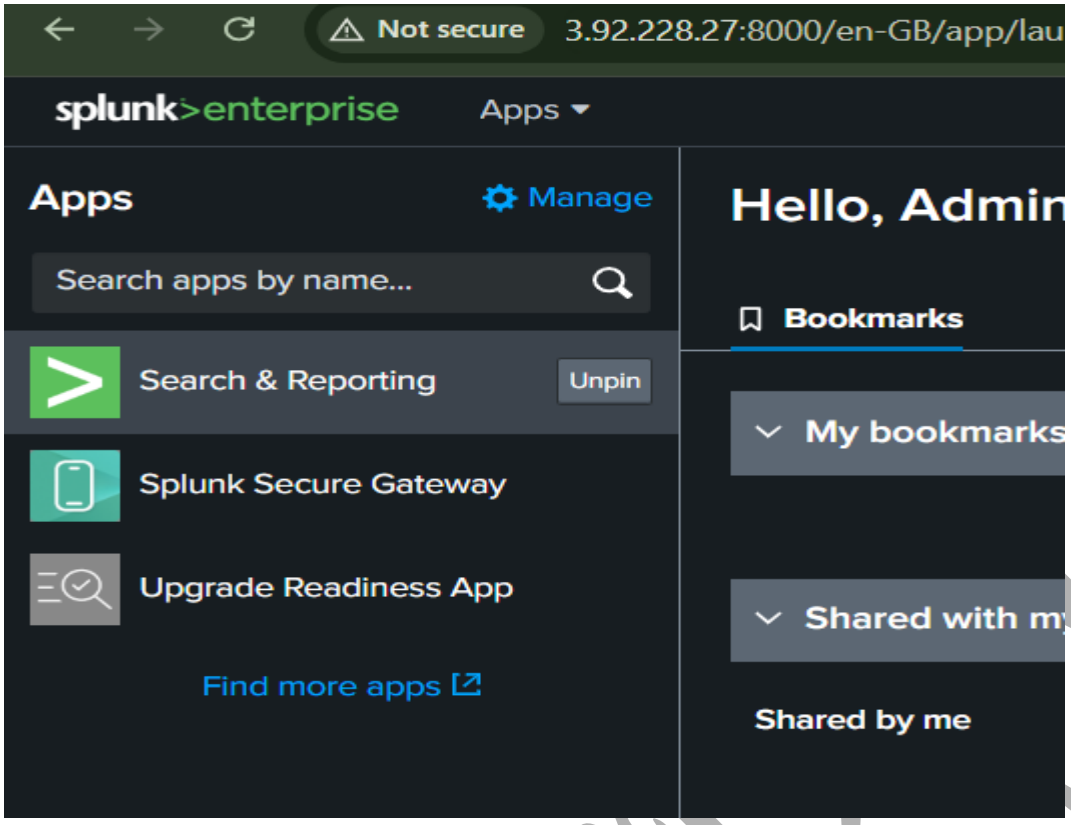
i-0639b3bf88289f12c (splunk)

PublicIPs: 3.92.228.27 PrivateIPs: 172.31.91.152

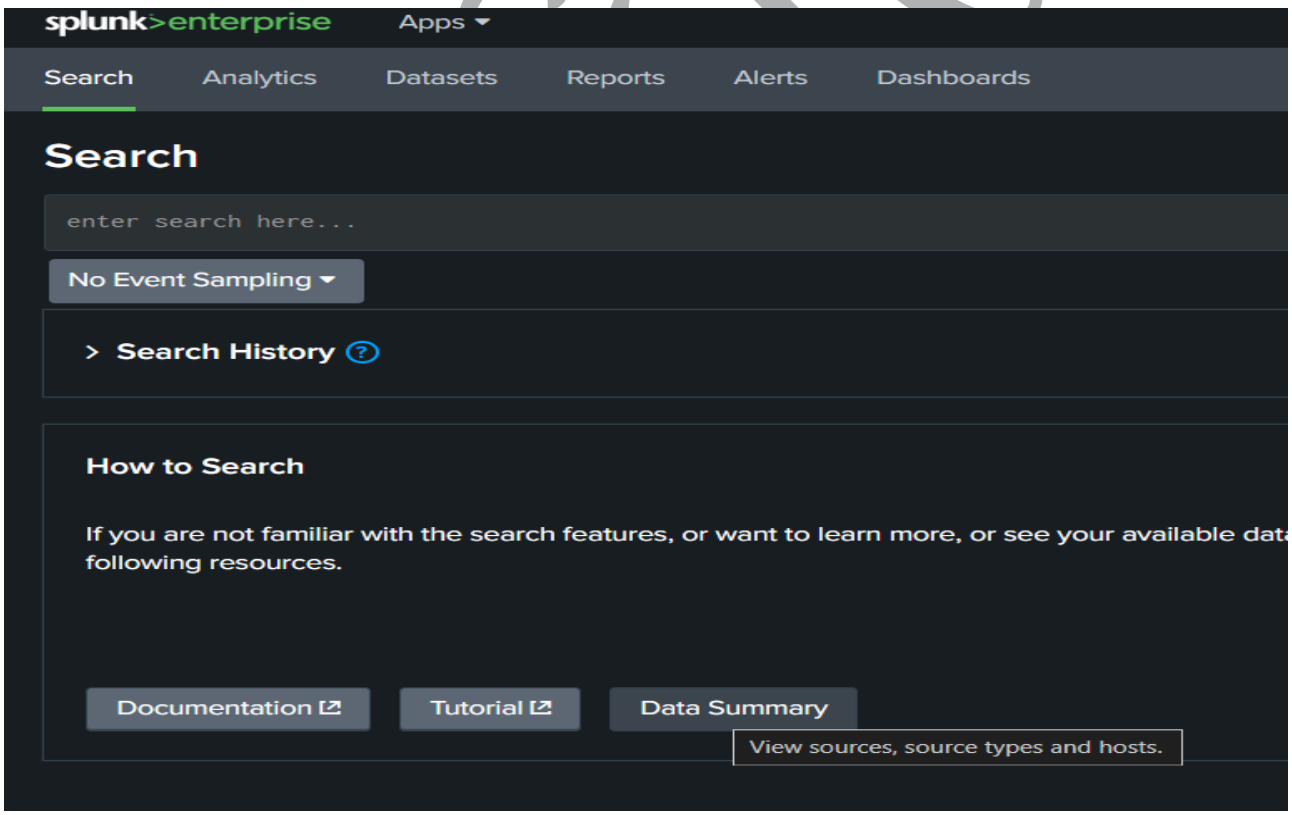
- Again to the login to the splunk



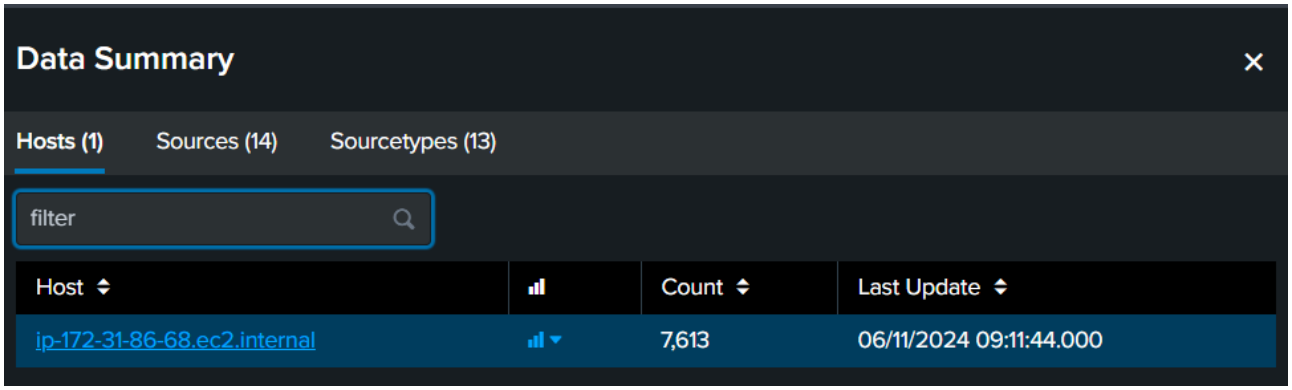
- Click in search and reporting
- If you not find serch and reporting just click on splunk>enterprise



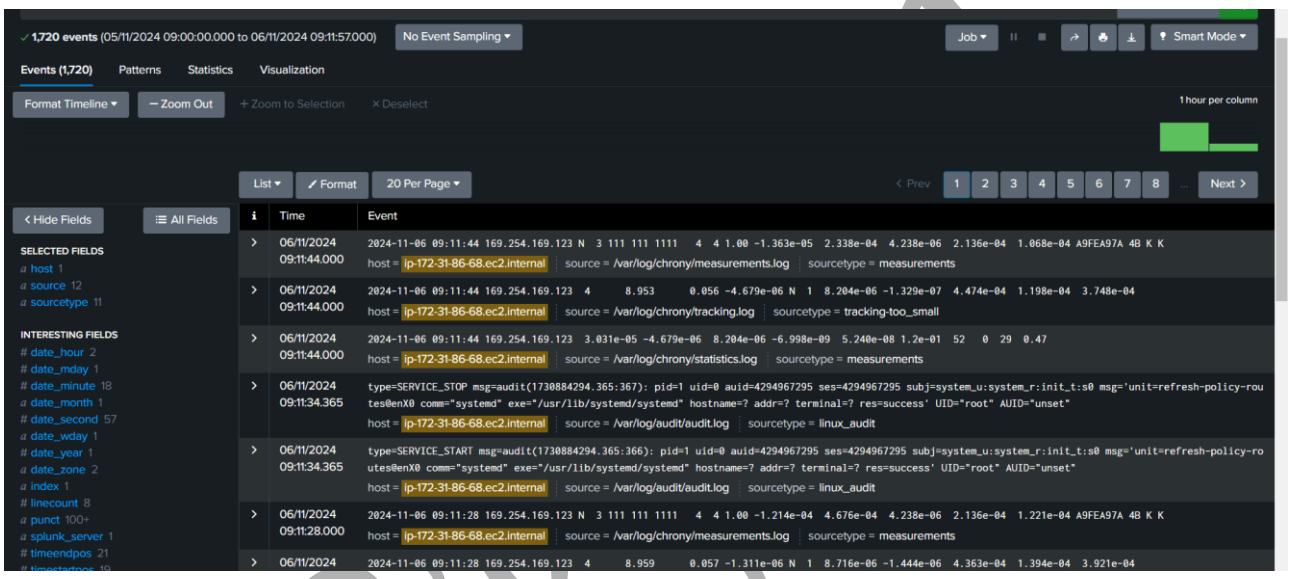
- Click on data summary



- Click on your ip address



- These are your splunk logs



Testing the splunk

Install httpd in splunk server

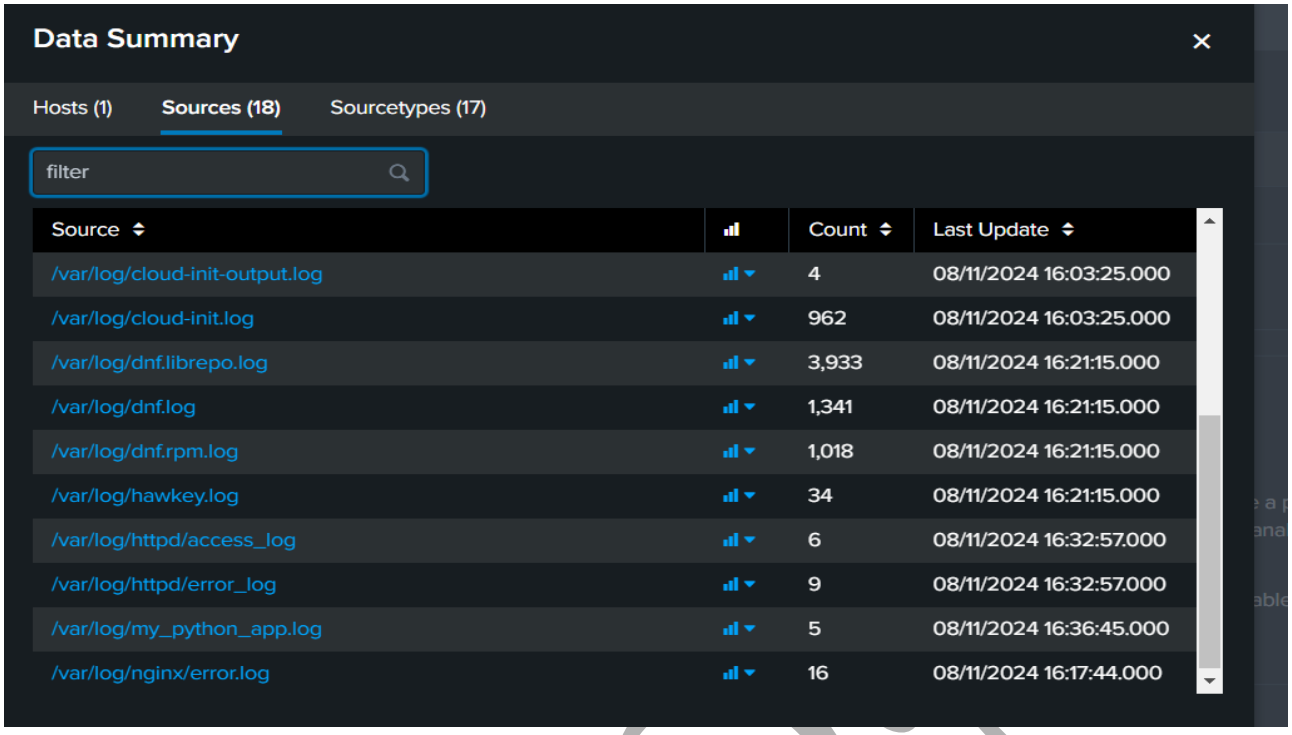
yum install httpd -y

systemctl strat httpd

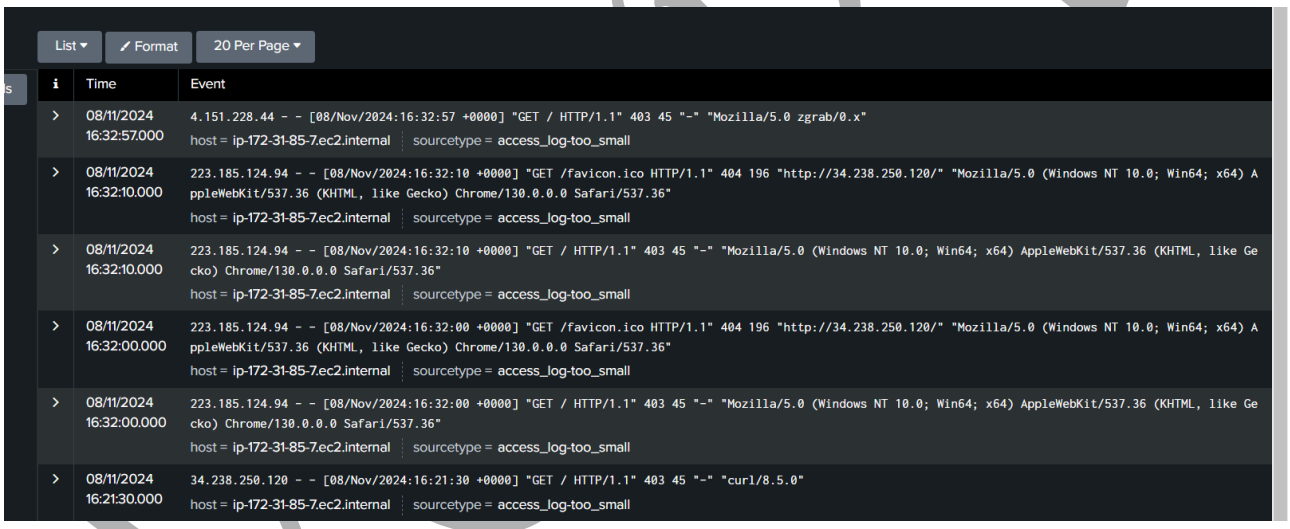
- Then search your public ip in browser

Next go to splunk click on data summery select sources

- Click on httpd/accesslog



- Click on httpd/accesslog ### these are the httpd application access logs



Testing method 2

- Create a test.py file add the bellow script

```
import logging

# Configure logging settings
logging.basicConfig(
    level=logging.INFO,
    format='%(asctime)s - %(levelname)s - %(message)s',
    handlers=[
```

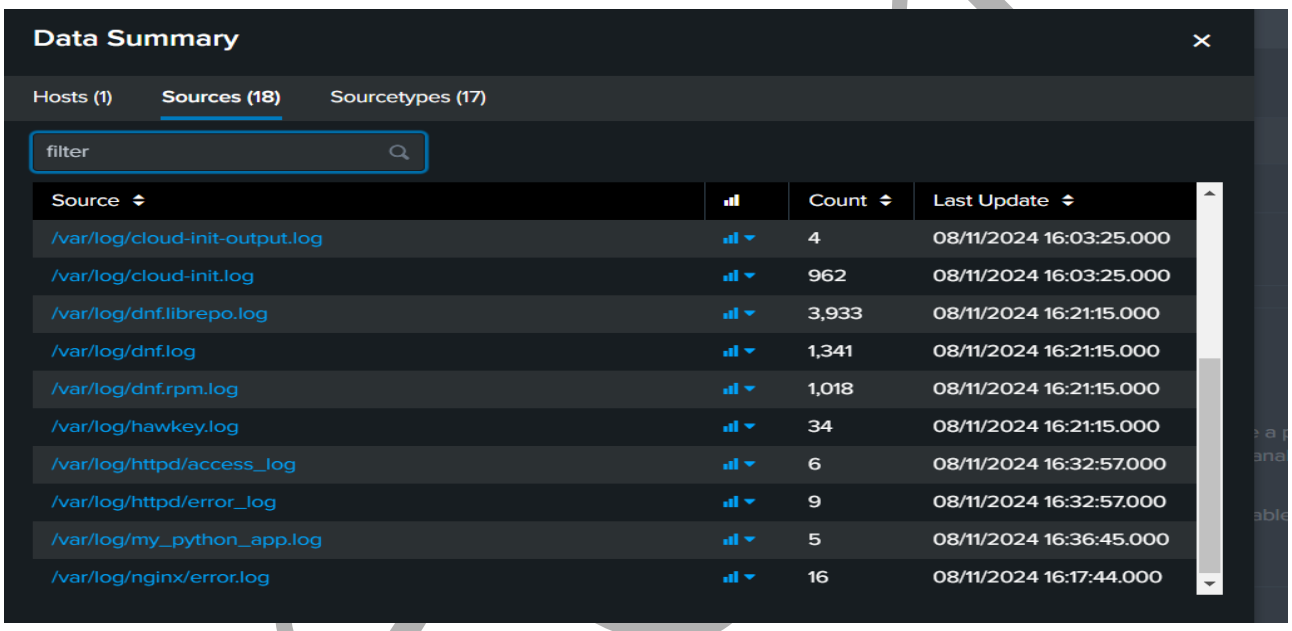
```
        logging.FileHandler("/var/log/my_python_app.log"),  # Change path if needed
        logging.StreamHandler()
    ]
)

# Example usage
logging.info("This is a success log message.")
logging.error("This is an error log message.")
```

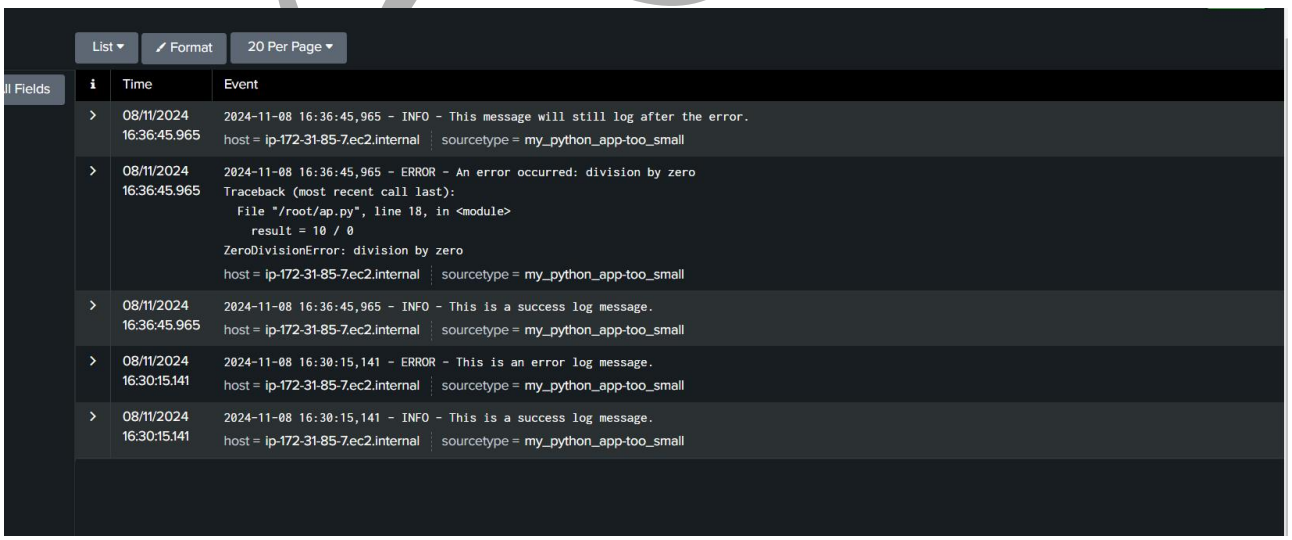
- Create another file app.py enter the below script

```
import logging

# Configure logging settings
logging.basicConfig(
    level=logging.INFO,
    format='%(asctime)s - %(levelname)s - %(message)s',
    handlers=[
        logging.FileHandler("/var/log/my_python_app.log"),  # Ensure path is writable
        logging.StreamHandler()
    ]
)

# Success log
logging.info("This is a success log message.")

try:
    # Intentional error: Divide by zero
    result = 10 / 0
except ZeroDivisionError as e:
```

```
# Log the error with stack trace
logging.error("An error occurred: %s", e, exc_info=True)

# Additional success log
logging.info("This message will still log after the error.")
```

- Then open splunk data summary select sources
- Click on python_app.log





These are the python application logs