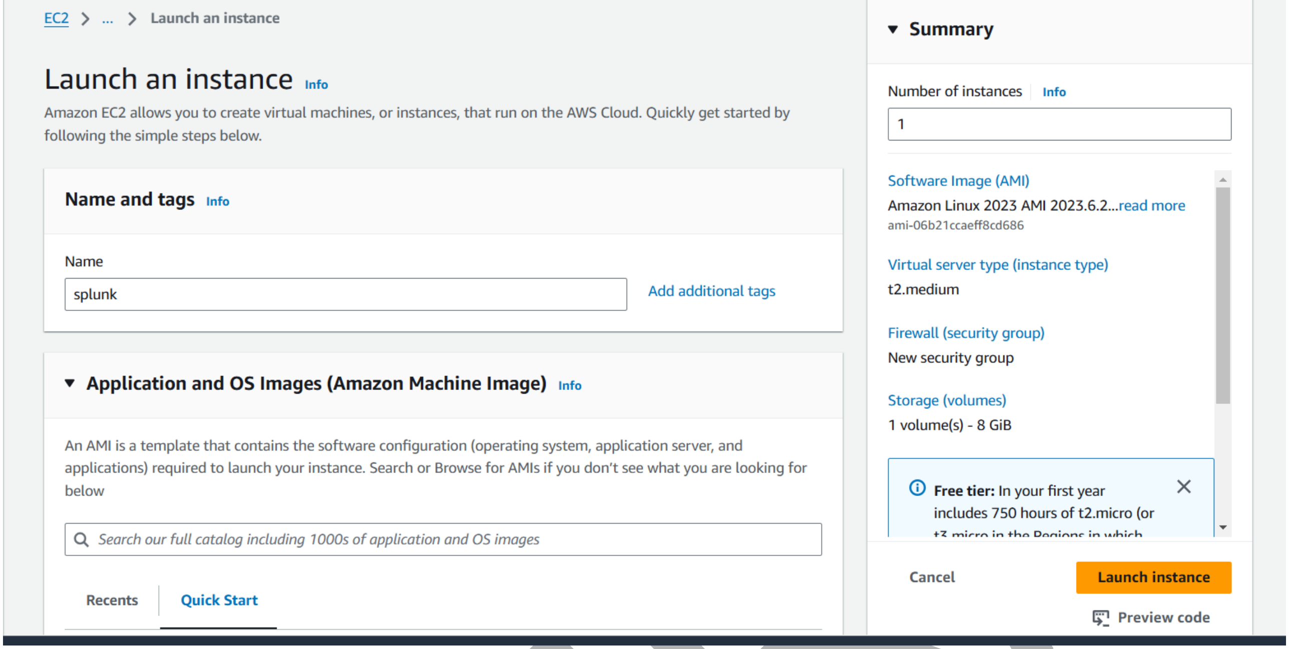
SPLUNK LOGS

Create ec2 with below specifications



EC2 > ... > Launch an instance

Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name: splunk

Add additional tags

Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Recents | Quick Start

Summary

Number of instances: 1

Software Image (AMI): Amazon Linux 2023 AMI 2023.6.2...read more
ami-06b21ccaeff8cd686

Virtual server type (instance type): t2.medium

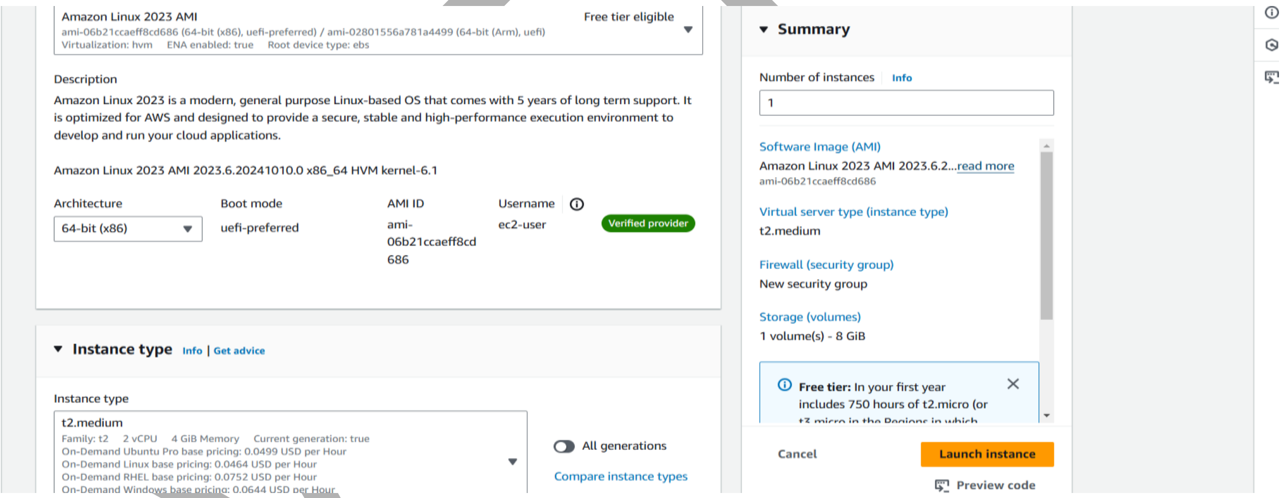
Firewall (security group): New security group

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

Cancel | Launch instance | Preview code

- Instance type is t2.medium



Amazon Linux 2023 AMI — Free tier eligible
ami-06b21ccaeff8cd686 (64-bit (x86), uefi-preferred) / ami-02801556a781a4499 (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs

Description
Amazon Linux 2023 is a modern, general purpose Linux-based OS that comes with 5 years of long term support. It is optimized for AWS and designed to provide a secure, stable and high-performance execution environment to develop and run your cloud applications.

Amazon Linux 2023 AMI 2023.6.20241010.0 x86_64 HVM kernel-6.1

Architecture	Boot mode	AMI ID	Username
64-bit (x86)	uefi-preferred	ami-06b21ccaeff8cd686	ec2-user

Verified provider

Instance type Info | Get advice

Instance type: t2.medium
Family: t2 2 vCPU 4 GiB Memory Current generation: true
On-Demand Ubuntu Pro base pricing: 0.0499 USD per Hour
On-Demand Linux base pricing: 0.0464 USD per Hour
On-Demand RHEL base pricing: 0.0752 USD per Hour
On-Demand Windows base pricing: 0.0644 USD per Hour

All generations | Compare instance types

Summary

Number of instances: 1

Software Image (AMI): Amazon Linux 2023 AMI 2023.6.2...read more
ami-06b21ccaeff8cd686

Virtual server type (instance type): t2.medium

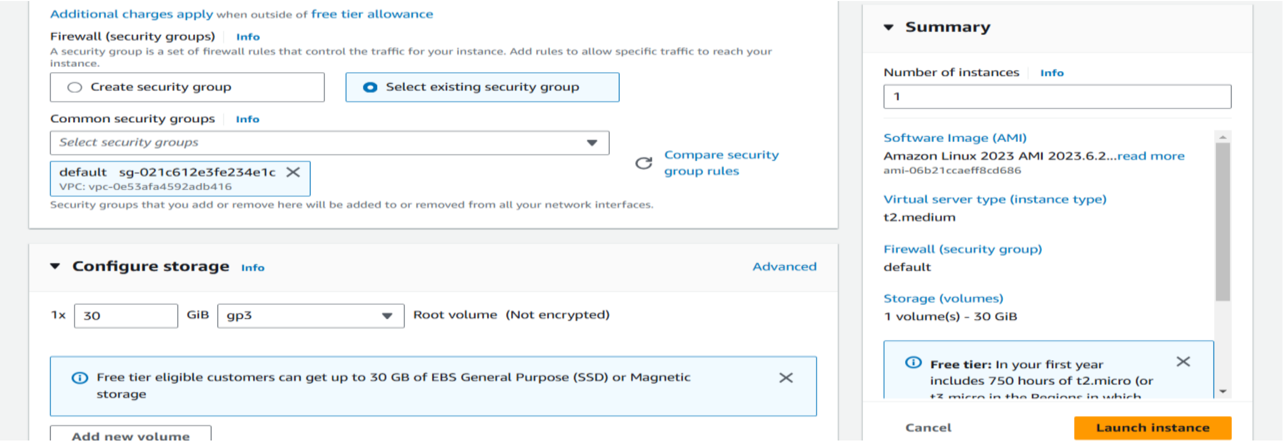
Firewall (security group): New security group

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

Cancel | Launch instance | Preview code

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



Additional charges apply when outside of free tier allowance

Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

○ Create security group ● Select existing security group

Common security groups Info
Select security groups
default sg-021c612e3fe234e1c
VPC: vpc-0e53afa4592adb416
Compare security group rules
Security groups that you add or remove here will be added to or removed from all your network interfaces.

Configure storage Info — Advanced

1x 30 GiB gp3 Root volume (Not encrypted)

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

Add new volume

Summary

Number of instances: 1

Software Image (AMI): Amazon Linux 2023 AMI 2023.6.2...read more
ami-06b21ccaeff8cd686

Virtual server type (instance type): t2.medium

Firewall (security group): default

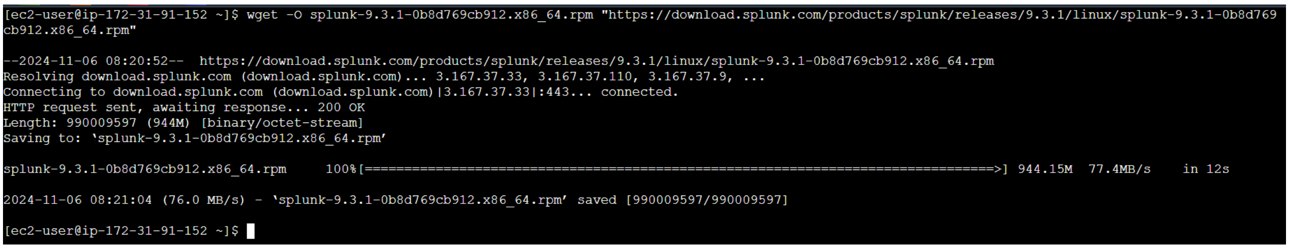
Storage (volumes): 1 volume(s) - 30 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which

Cancel | Launch instance

- Connect to instance install splunk

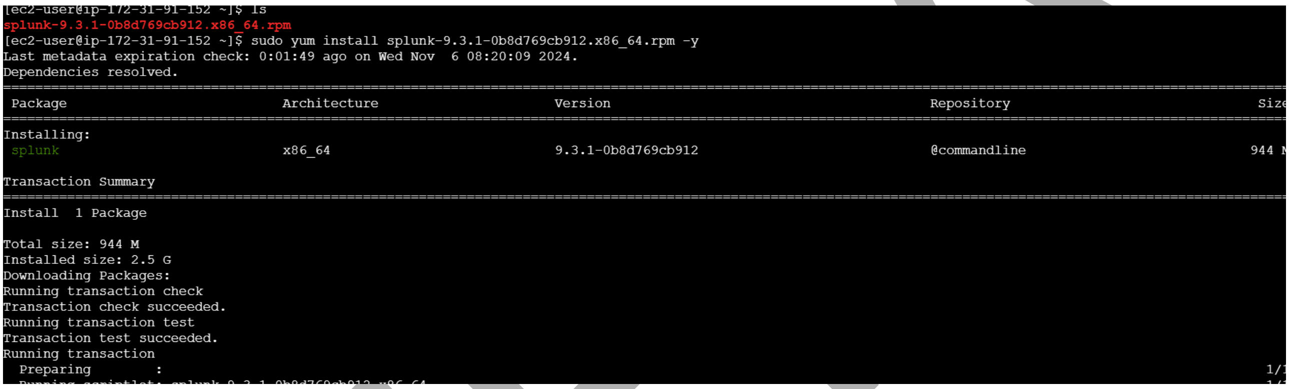
wget -O splunk-9.3.1-0b8d769cb912.x86_64.rpm "https://download.splunk.com/products/splunk/releases/9.3.1/linux/splunk-9.3.1-0b8d769cb912.x86_64.rpm"



```
[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

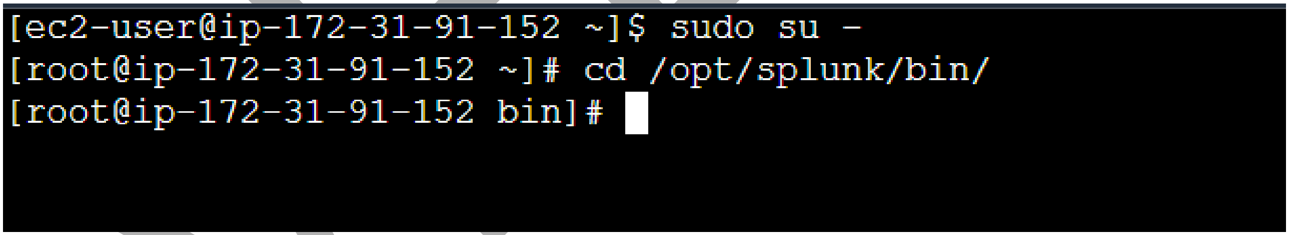
sudo yum install splunk-9.3.1-0b8d769cb912.x86_64.rpm -y



```
[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
  Running scriptlet: splunk-9.3.1-0b8d769cb912.x86_64                                                                                                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]#
```

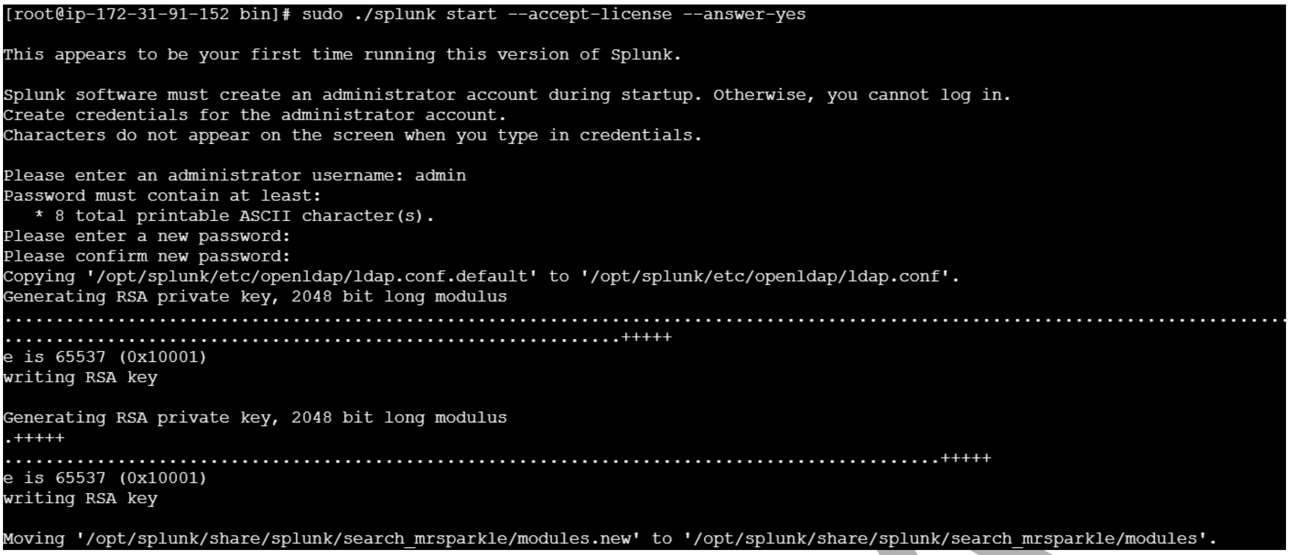
- Strat the splunk

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

- It will ask usename password

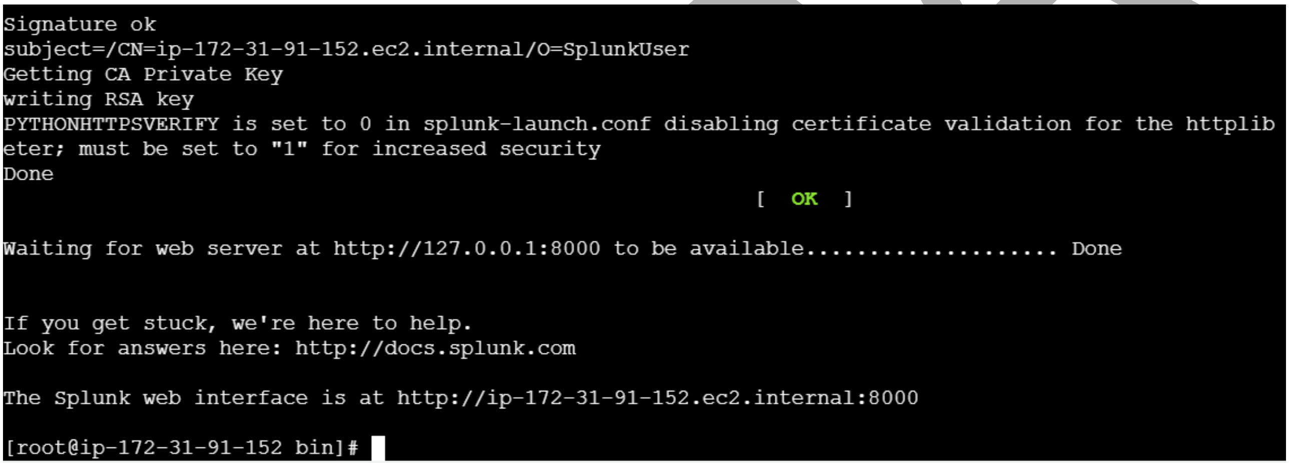
Username :admin

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'.
```

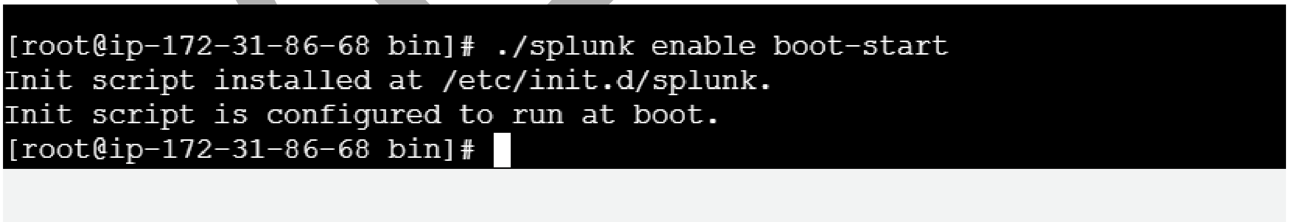
- Successfully started the splunk



```
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]#
```

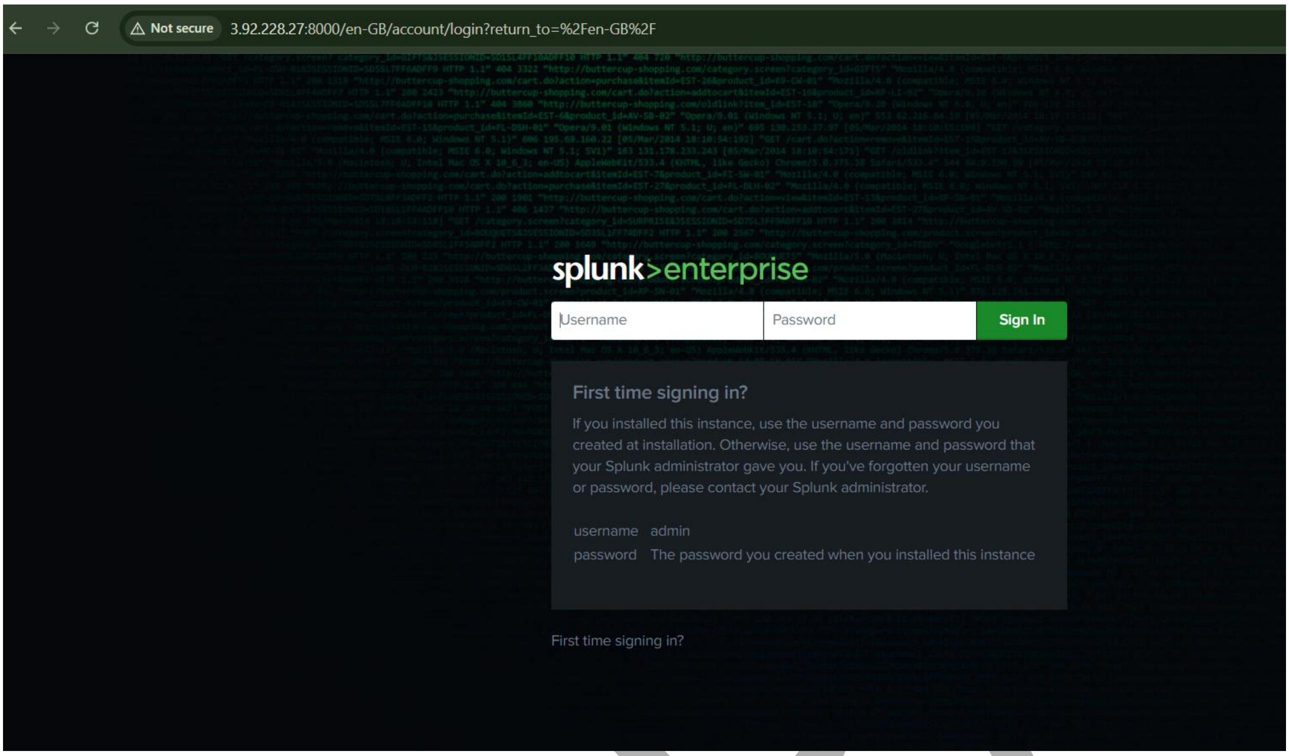
- Enable the splunk

./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



Not secure 3.92.228.27:8000/en-GB/account/login?return_to=%2Fen-GB%2F

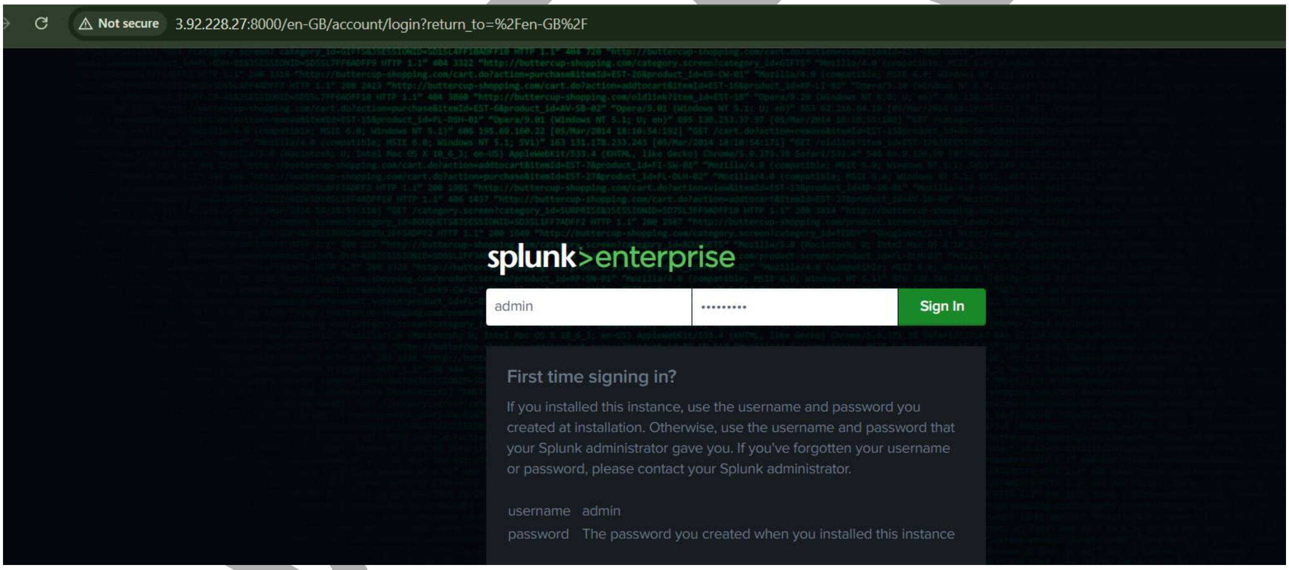
First time signing in?

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 The password you created when you installed this instance

First time signing in?

- enter the user name and password



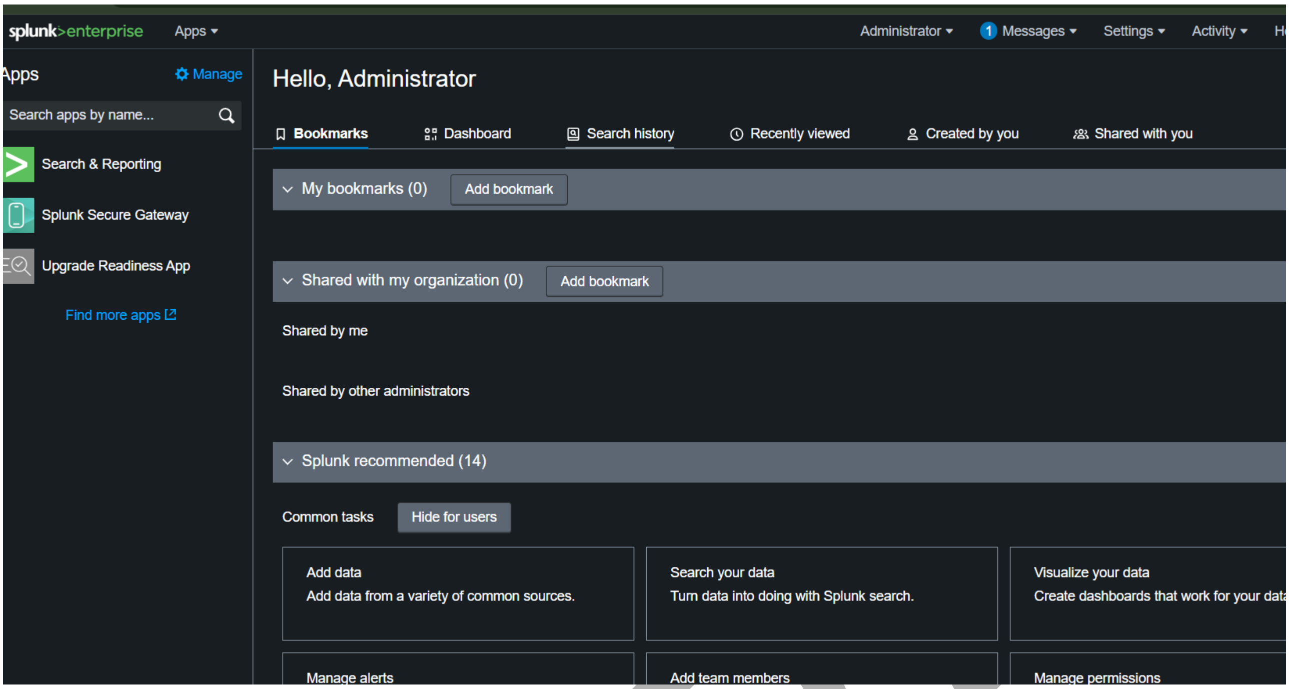
Not secure 3.92.228.27:8000/en-GB/account/login?return_to=%2Fen-GB%2F

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 The password you created when you installed this instance

- this is the dashboard of splunk

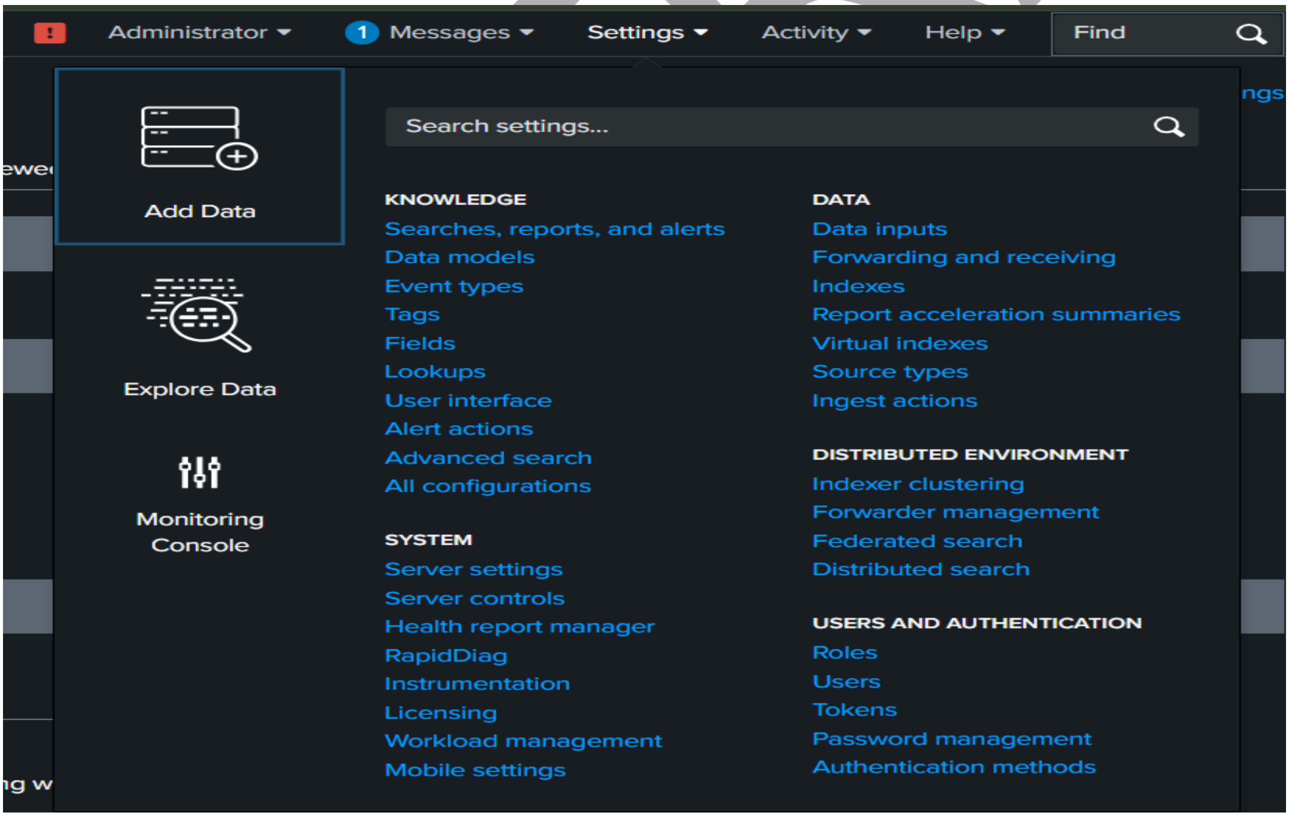


Add data
Add data from a variety of common sources.

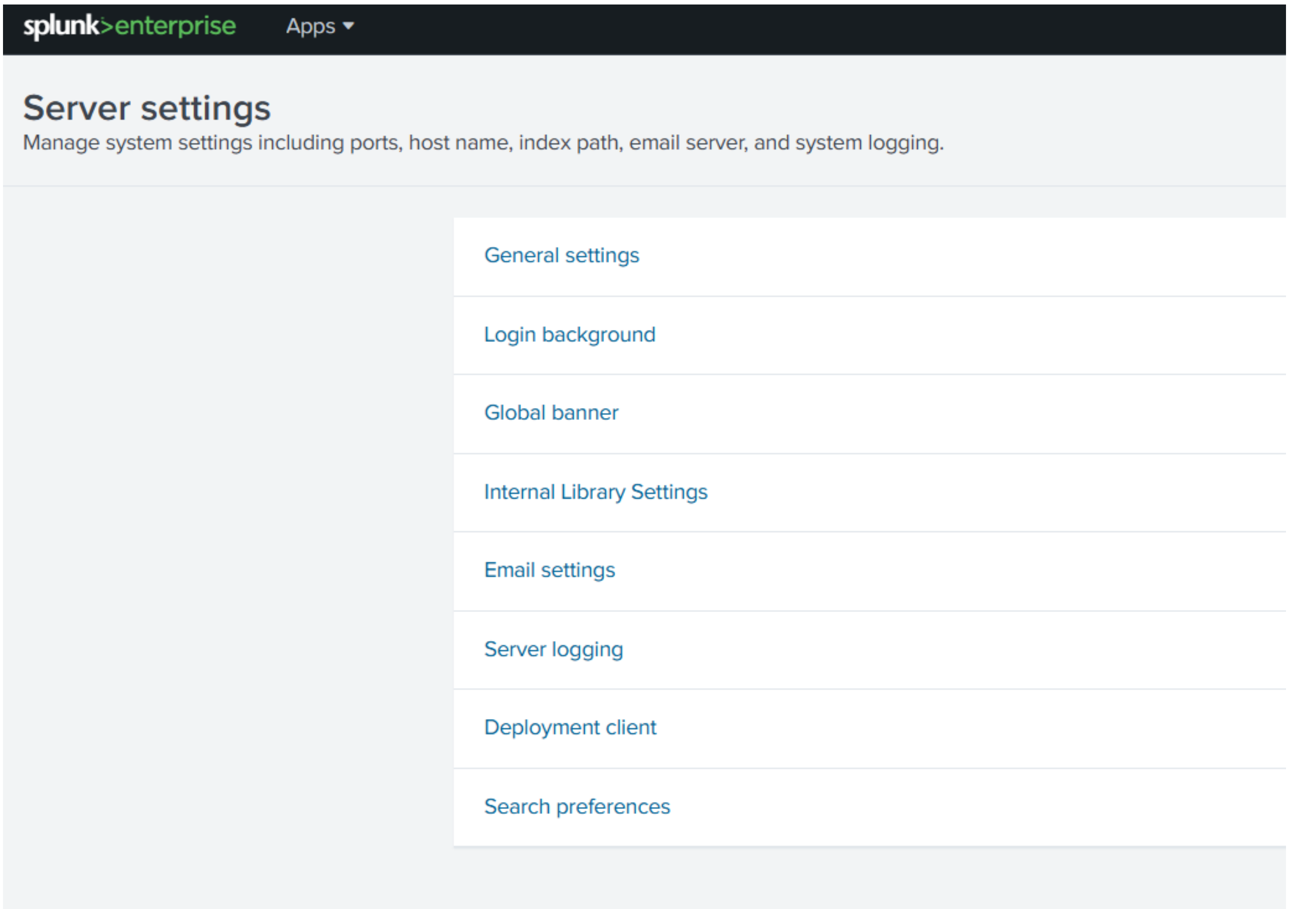
Search your data
Turn data into doing with Splunk search.

Visualize your data
Create dashboards that work for your dat

- click on settings
- select server settings



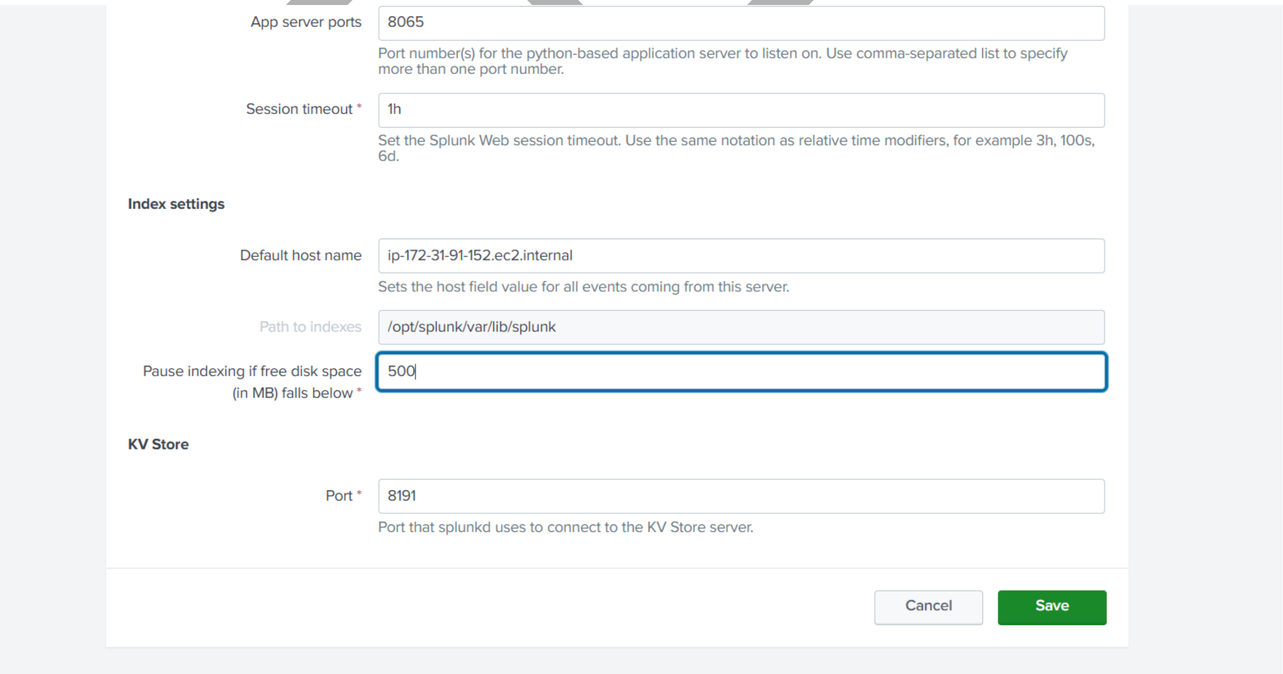
- after selecting server settings
- click on general settings



Server settings

Manage system settings including ports, host name, index path, email server, and system logging.

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



App server ports: 8065

Port number(s) for the python-based application server to listen on. Use comma-separated list to specify more than one port number.

Session timeout *: 1h

Set the Splunk Web session timeout. Use the same notation as relative time modifiers, for example 3h, 100s, 6d.

Index settings

Default host name: ip-172-31-91-152.ec2.internal

Sets the host field value for all events coming from this server.

Path to indexes: /opt/splunk/var/lib/splunk

Pause indexing if free disk space (in MB) falls below *: 500

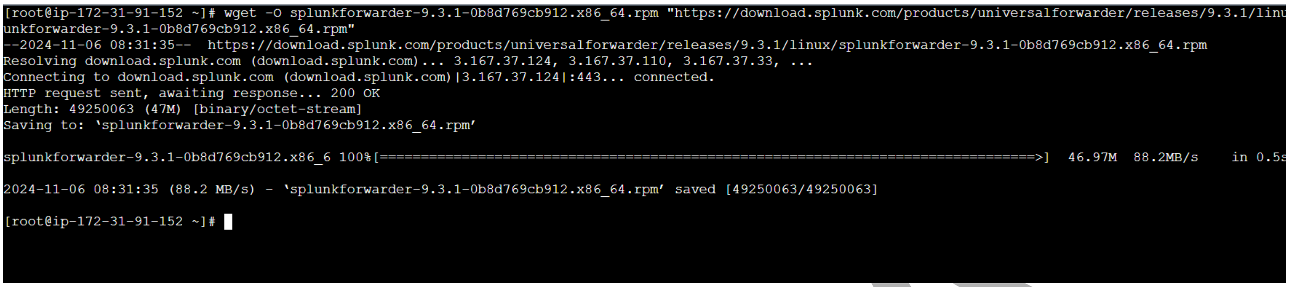
KV Store

Port *: 8191

Port that splunkd uses to connect to the KV Store server.

- Now its time to install splunk forwader

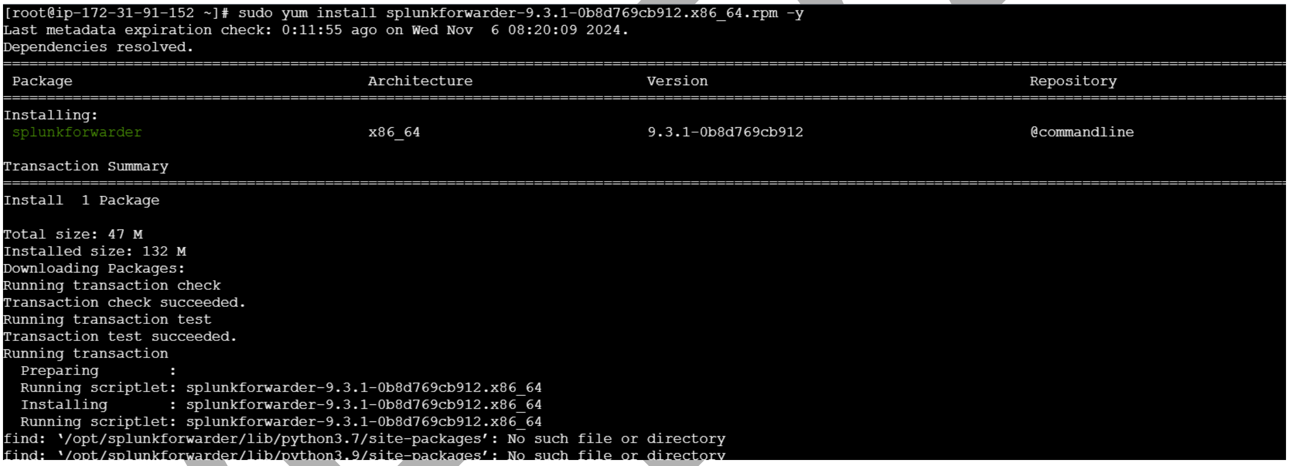
wget -O splunkforwarder-9.3.1-0b8d769cb912.x86_64.rpm "https://download.splunk.com/products/universalforwarder/releases/9.3.1/linux/splunkforwarder-9.3.1-0b8d769cb912.x86_64.rpm"



```
[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

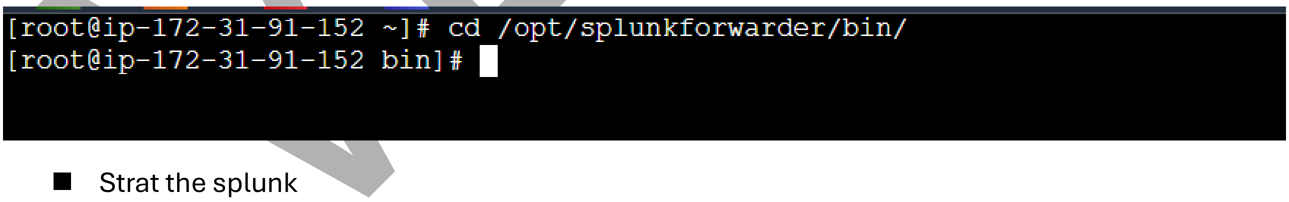
sudo yum install splunkforwarder-9.3.1-0b8d769cb912.x86_64.rpm -y



```
[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]# 
```

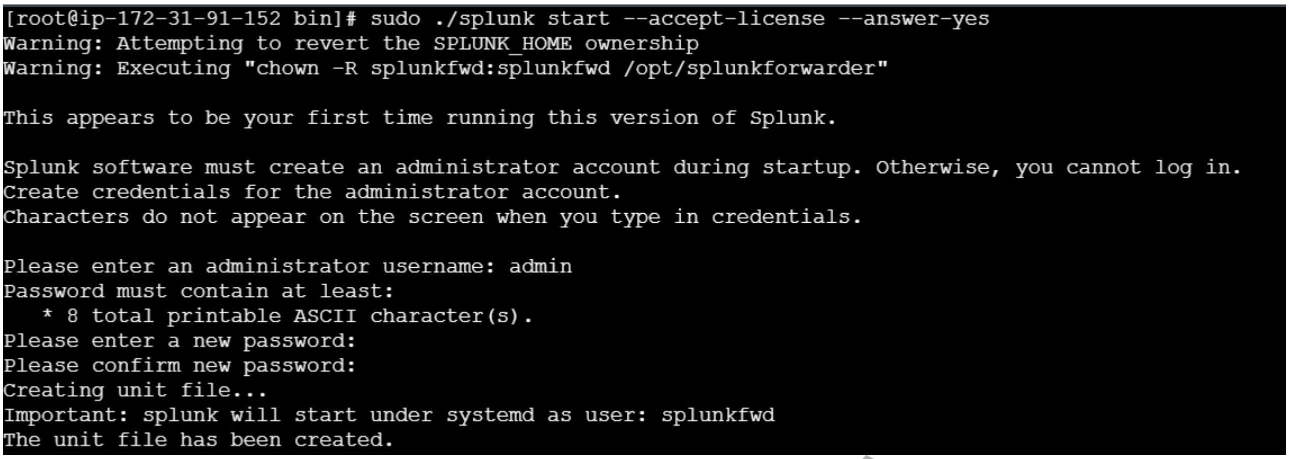
- Strat the splunk

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

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

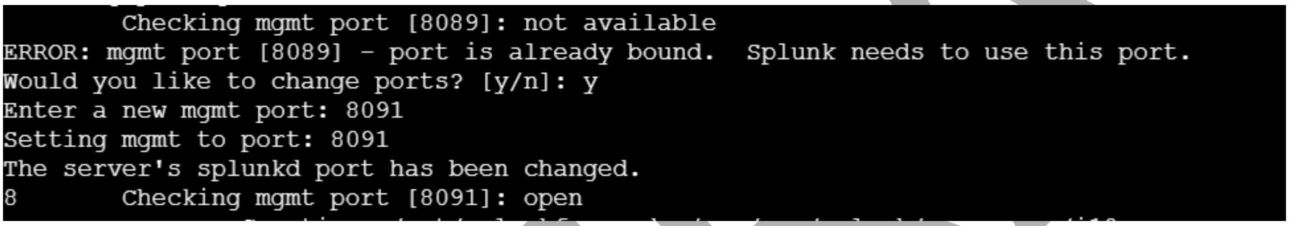
Username :admin

Password : admin1234 [give your custom password]



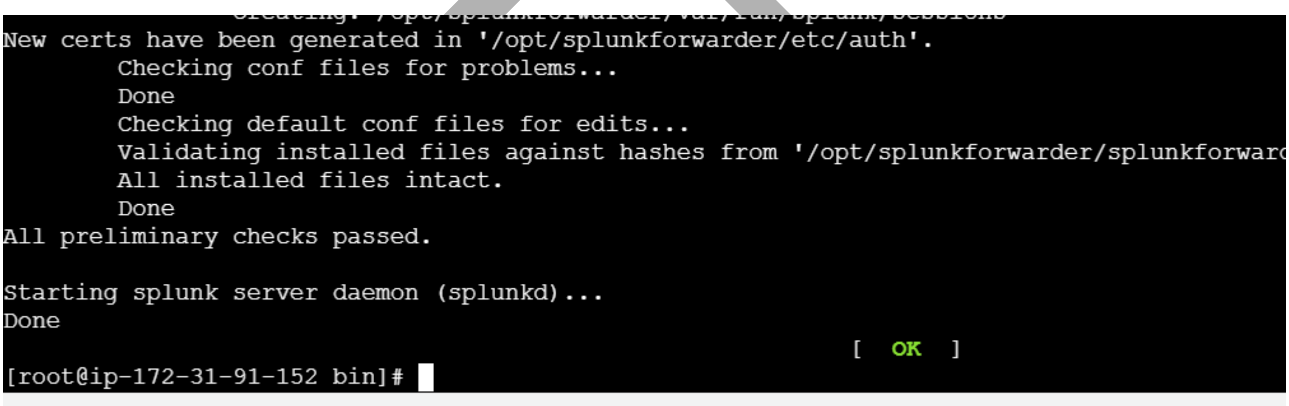
```
[root@ip-172-31-91-152 bin]# sudo ./splunk start --accept-license --answer-yes
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"

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



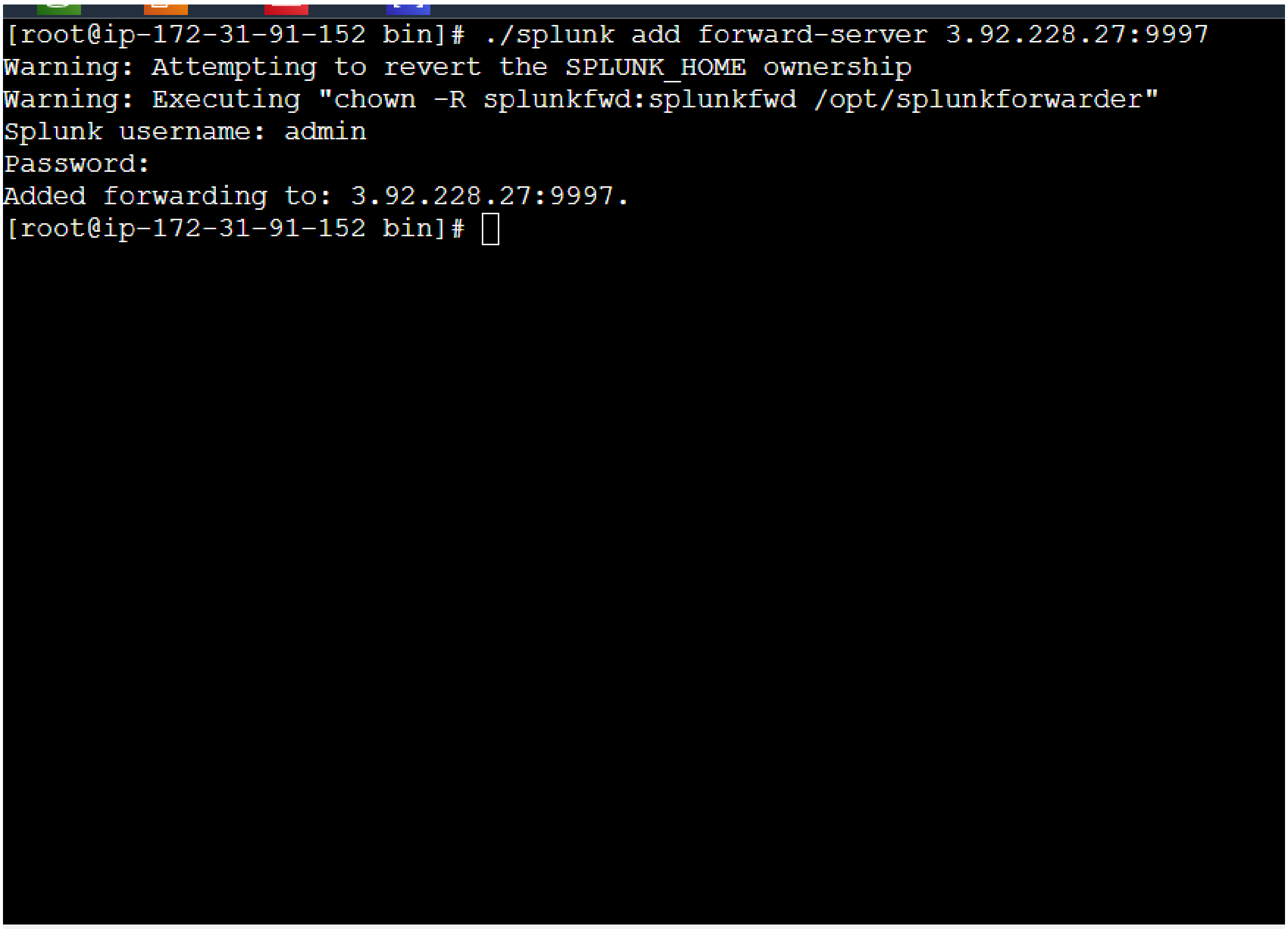
```
                Creating: /opt/splunkforwarder/var/run/splunk/sessions
New certs have been generated in '/opt/splunkforwarder/etc/auth'.
        Checking conf files for problems...
        Done
        Checking default conf files for edits...
        Validating installed files against hashes from '/opt/splunkforwarder/splunkforward
        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

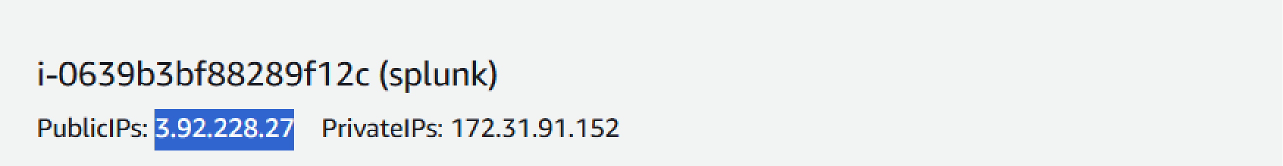
./splunk add forward-server <your splunk public-ip>:9997

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]# 
```

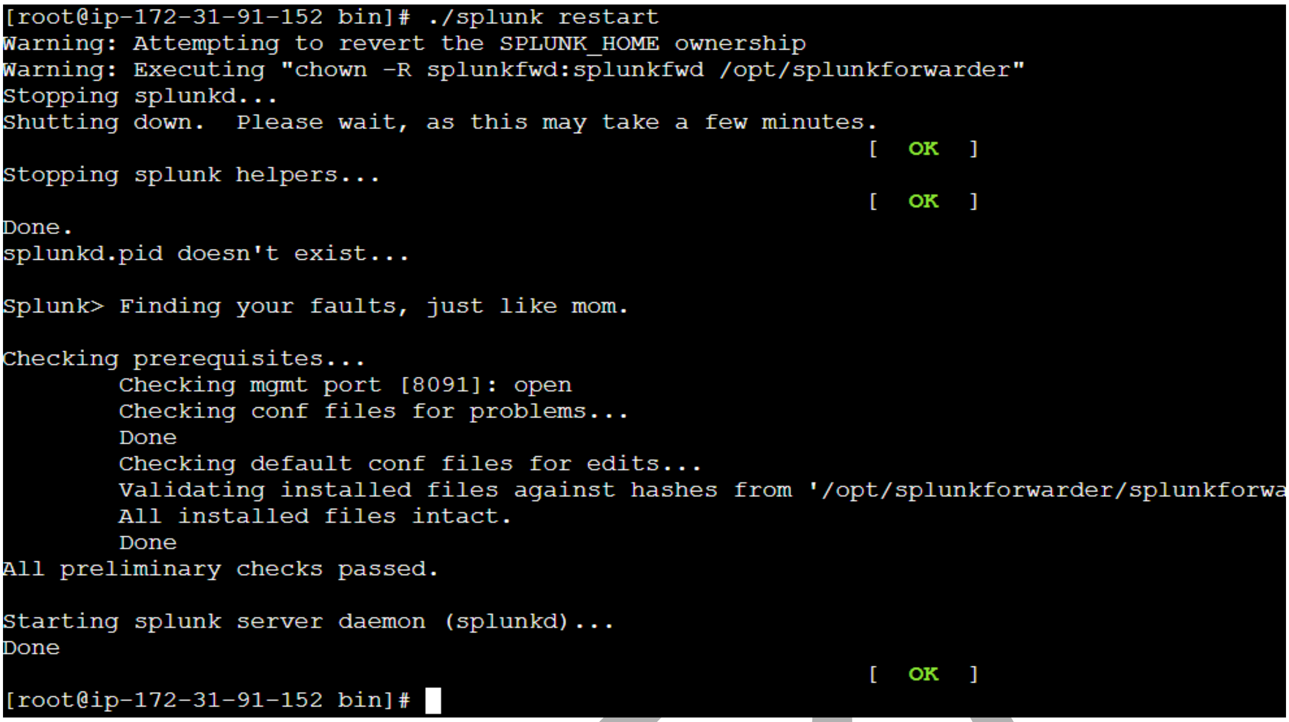


i-0639b3bf88289f12c (splunk)

PublicIPs: 3.92.228.27 PrivateIPs: 172.31.91.152

- After that restart the splunk forwarder

./splunk restart

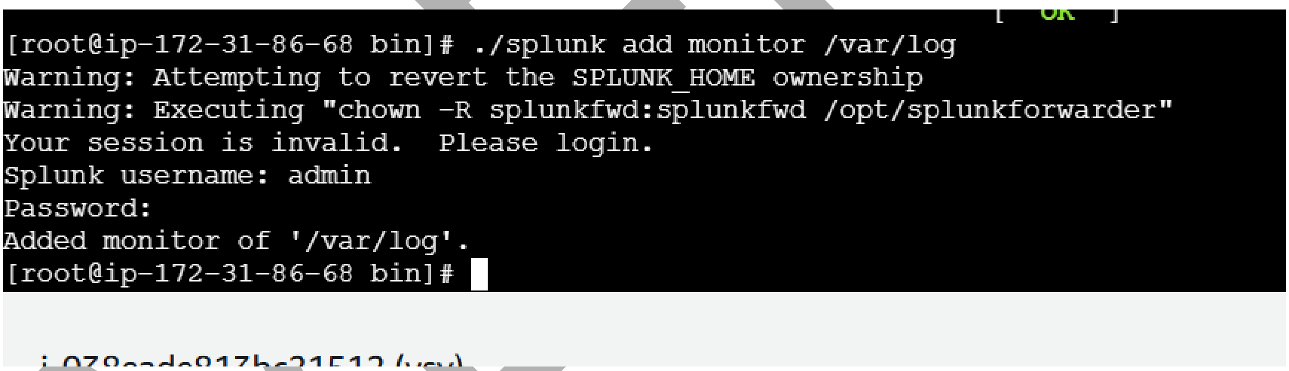


```
[root@ip-172-31-91-152 bin]# ./splunk restart
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Stopping splunkd...
Shutting down.  Please wait, as this may take a few minutes.
                                                           [  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

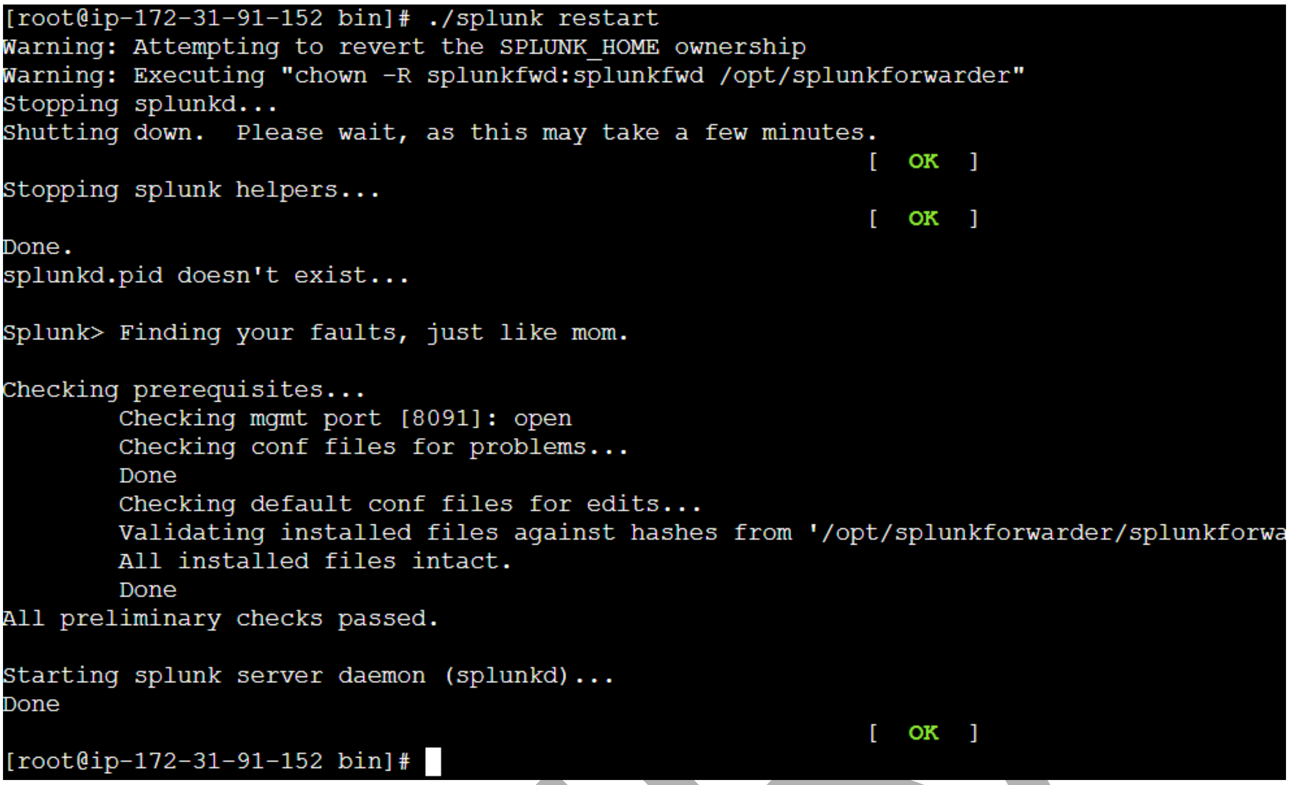


```
                                                           [  OK  ]
[root@ip-172-31-86-68 bin]# ./splunk add monitor /var/log
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Your session is invalid.  Please login.
Splunk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

i-078eade817bc21513 (vsv)

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

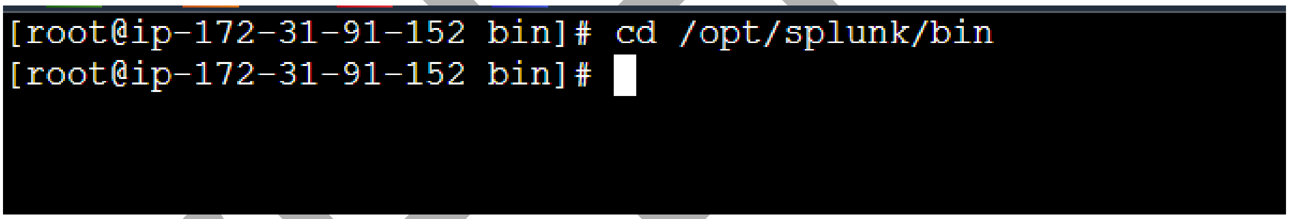
./splunk restart



```
[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 switch to splunk bin folder

cd /opt/splunk/bin

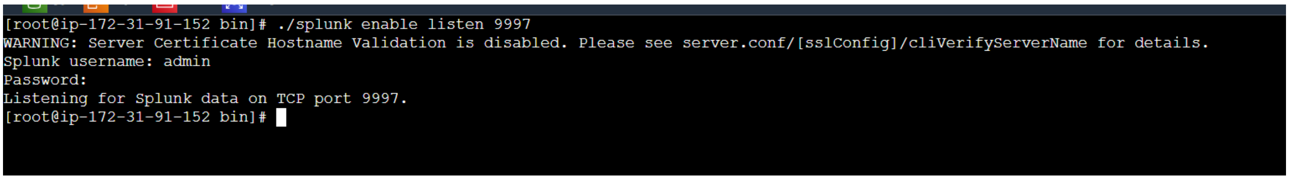


```
[root@ip-172-31-91-152 bin]# cd /opt/splunk/bin
[root@ip-172-31-91-152 bin]#
```

- Enable the 9997 port requests

./splunk enable listen 9997

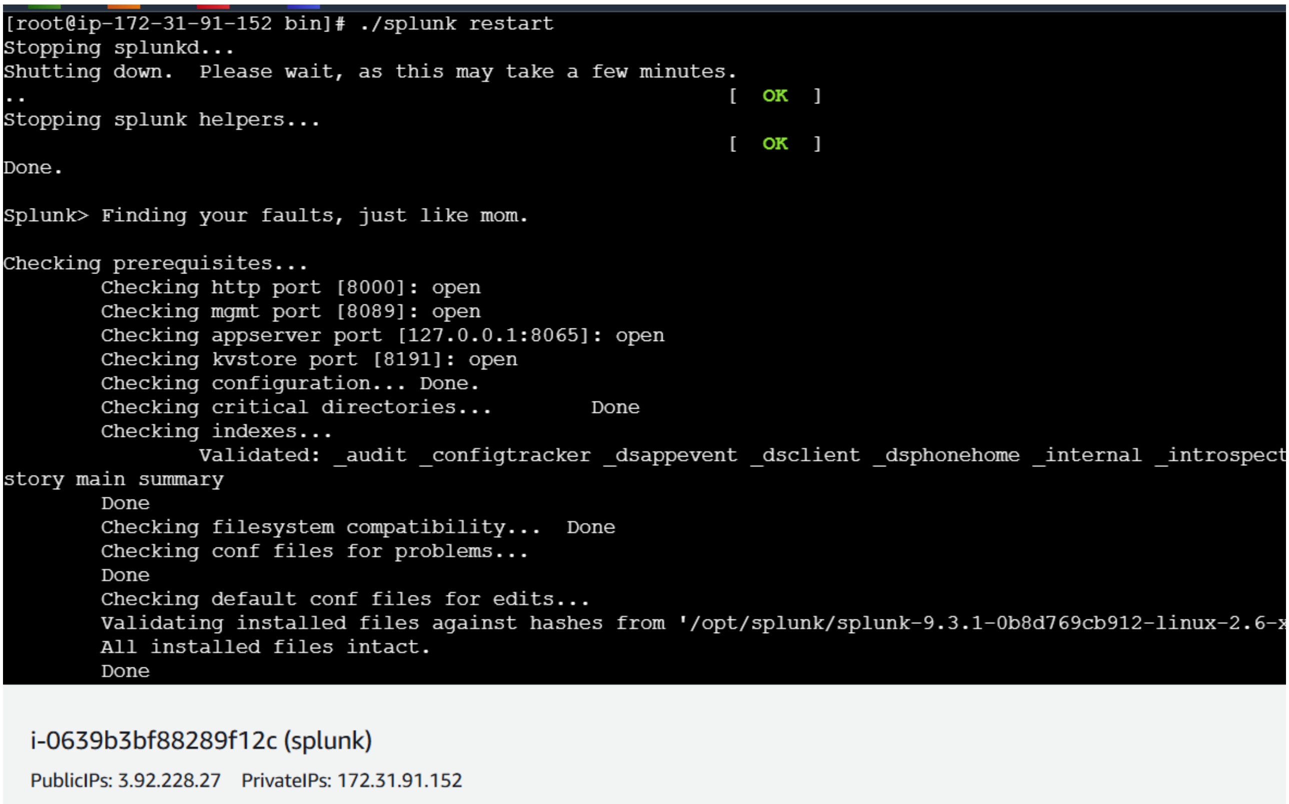
- It will ask the username and password just enter and continue



```
[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

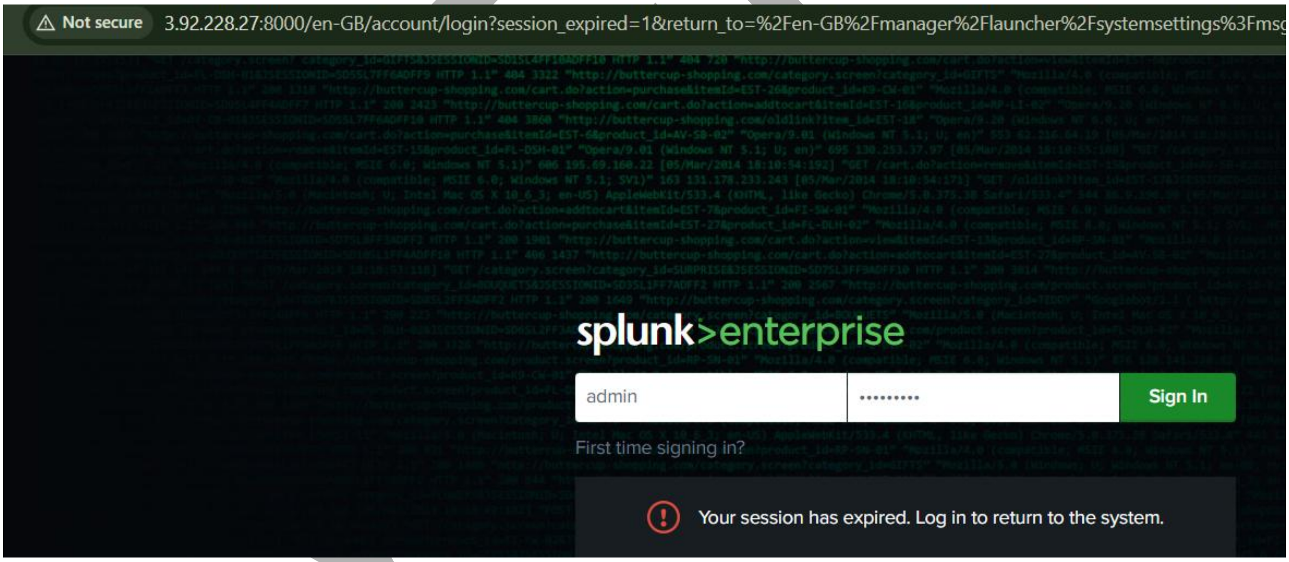


```
[root@ip-172-31-91-152 bin]# ./splunk restart
Stopping splunkd...
Shutting down.  Please wait, as this may take a few minutes.
..                                                          [  OK  ]
Stopping splunk helpers...
                                                            [  OK  ]
Done.

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

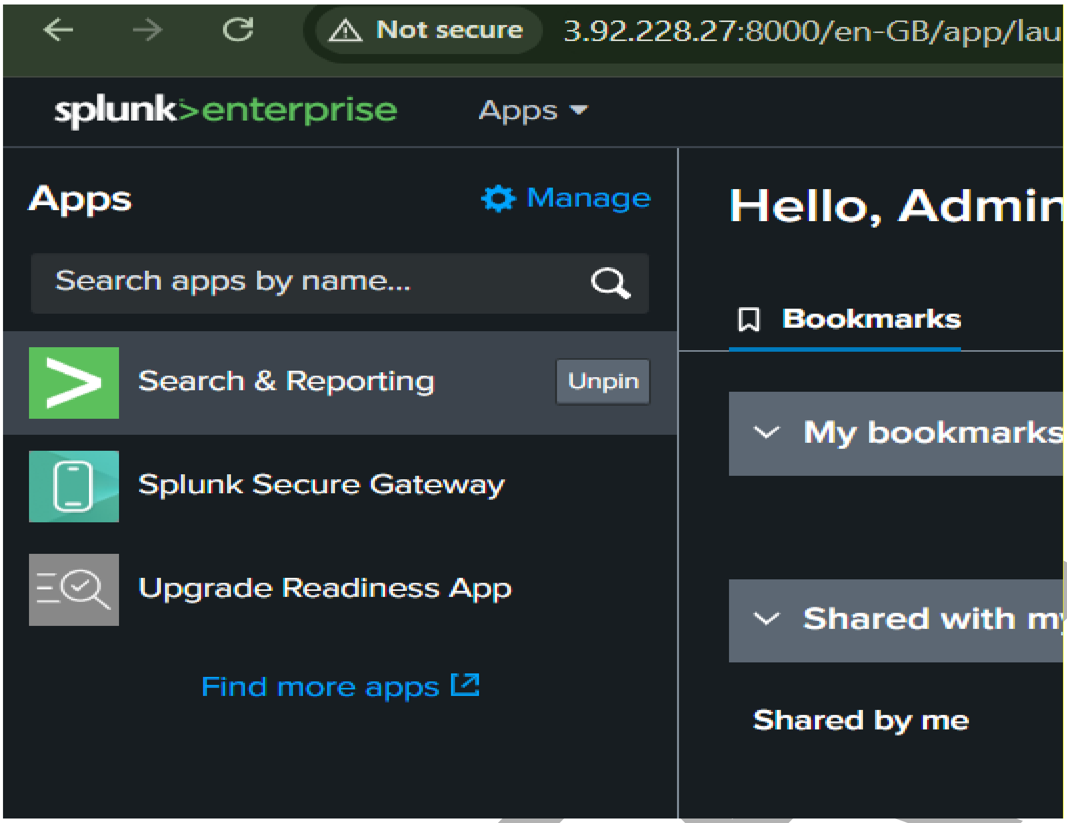


⚠ Not secure   3.92.228.27:8000/en-GB/account/login?session_expired=1&return_to=%2Fen-GB%2Fmanager%2Flauncher%2Fsystemsettings%3Fmsg

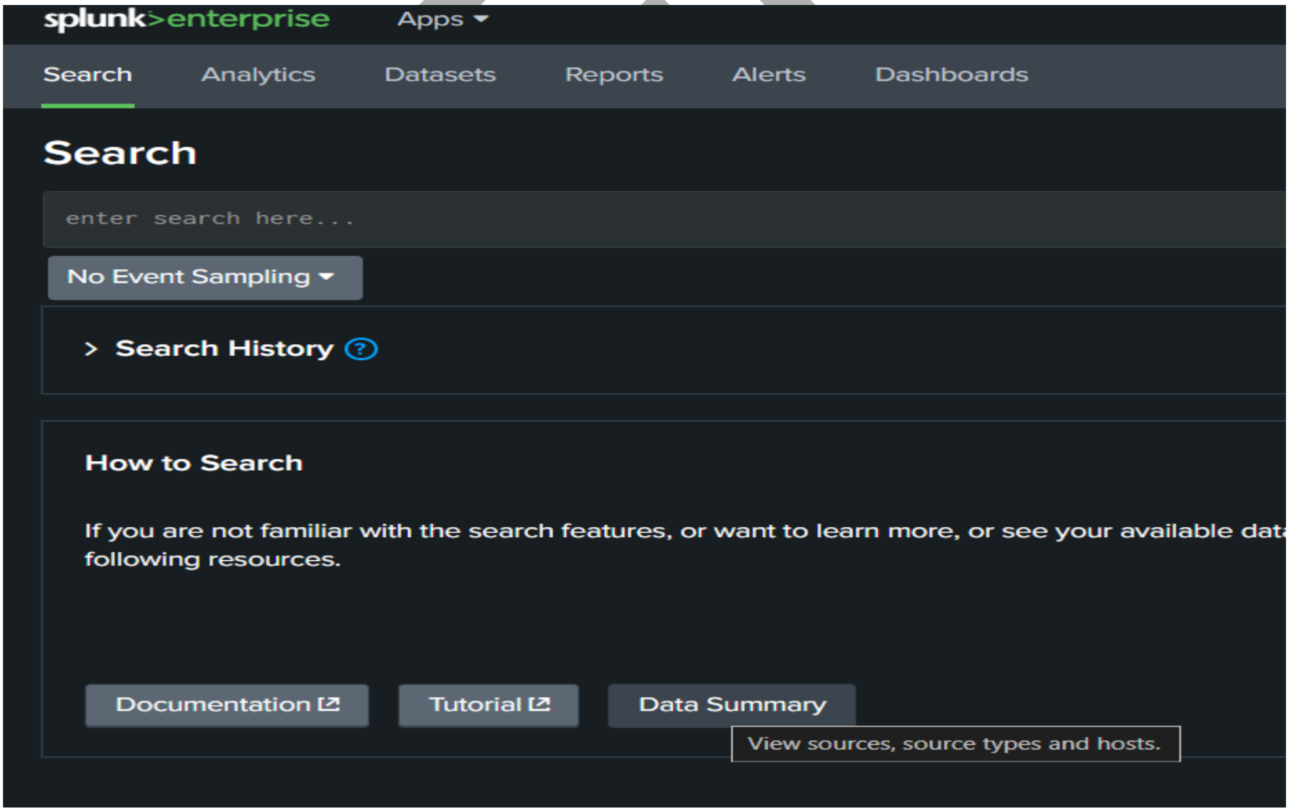
First time signing in?

Your session has expired. Log in to return to the system.

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

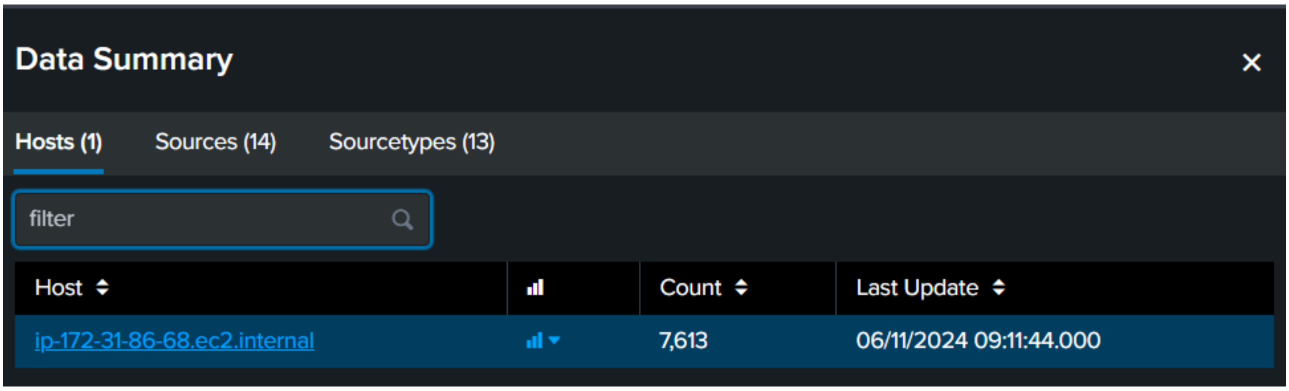


- Click on data summary



If you are not familiar with the search features, or want to learn more, or see your available dat following resources.

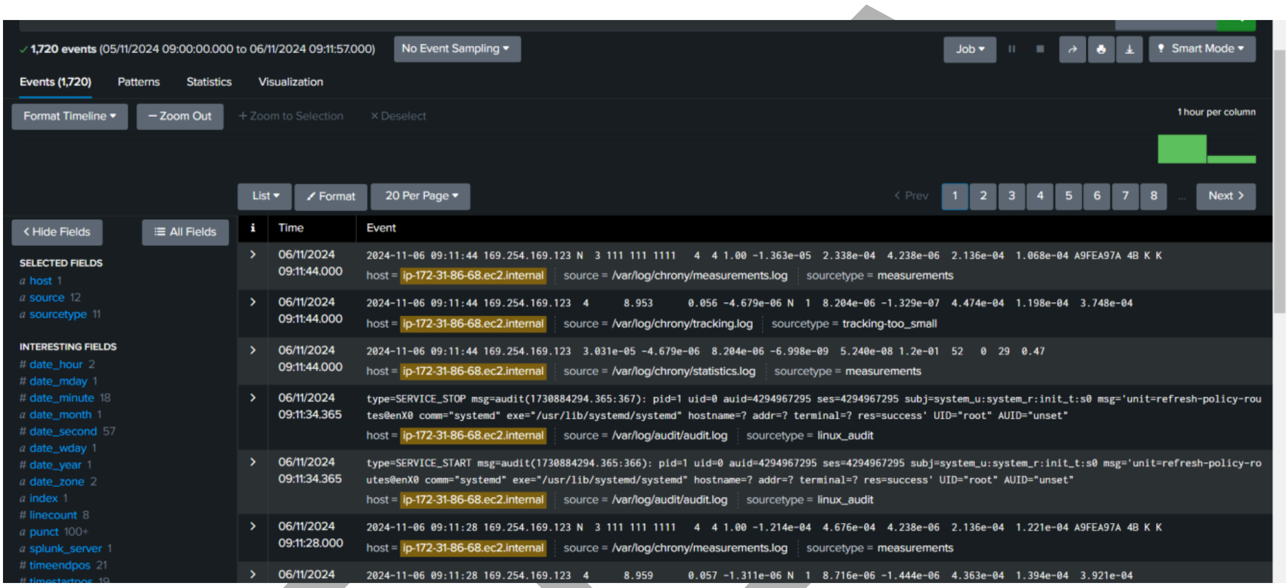
- Click on your ip address



Data Summary

Host		Count	Last Update
ip-172-31-86-68.ec2.internal		7,613	06/11/2024 09:11:44.000

- These are your splunk logs



✓ 1,720 events (05/11/2024 09:00:00.000 to 06/11/2024 09:11:57.000)

```
i  Time                     Event
>  06/11/2024 09:11:44.000  2024-11-06 09:11:44 169.254.169.123 N  3 111 111 1111   4  4 1.00 -1.363e-05  2.338e-04  4.238e-06  2.136e-04  1.068e-04 A9FEA97A 4B K K
                            host = ip-172-31-86-68.ec2.internal  source = /var/log/chrony/measurements.log  sourcetype = measurements
>  06/11/2024 09:11:44.000  2024-11-06 09:11:44 169.254.169.123  4      8.953      0.056 -4.679e-06 N  1  8.204e-06 -1.329e-07  4.474e-04  1.198e-04  3.748e-04
                            host = ip-172-31-86-68.ec2.internal  source = /var/log/chrony/tracking.log  sourcetype = tracking-too_small
>  06/11/2024 09:11:44.000  2024-11-06 09:11:44 169.254.169.123  3.031e-05 -4.679e-06  8.204e-06 -6.998e-09  5.240e-08 1.2e-01  52   0  29  0.47
                            host = ip-172-31-86-68.ec2.internal  source = /var/log/chrony/statistics.log  sourcetype = measurements
>  06/11/2024 09:11:34.365  type=SERVICE_STOP msg=audit(1730884294.365:367): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=refresh-policy-rou
                            tes@enX0 comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success' UID="root" AUID="unset"
                            host = ip-172-31-86-68.ec2.internal  source = /var/log/audit/audit.log  sourcetype = linux_audit
>  06/11/2024 09:11:34.365  type=SERVICE_START msg=audit(1730884294.365:366): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=refresh-policy-ro
                            utes@enX0 comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success' UID="root" AUID="unset"
                            host = ip-172-31-86-68.ec2.internal  source = /var/log/audit/audit.log  sourcetype = linux_audit
>  06/11/2024 09:11:28.000  2024-11-06 09:11:28 169.254.169.123 N  3 111 111 1111   4  4 1.00 -1.214e-04  4.676e-04  4.238e-06  2.136e-04  1.221e-04 A9FEA97A 4B K K
                            host = ip-172-31-86-68.ec2.internal  source = /var/log/chrony/measurements.log  sourcetype = measurements
>  06/11/2024               2024-11-06 09:11:28 169.254.169.123  4      8.959      0.057 -1.311e-06 N  1  8.716e-06 -1.444e-06  4.363e-04  1.394e-04  3.921e-04
```

Testing the splunk

Install httpd in splunk server

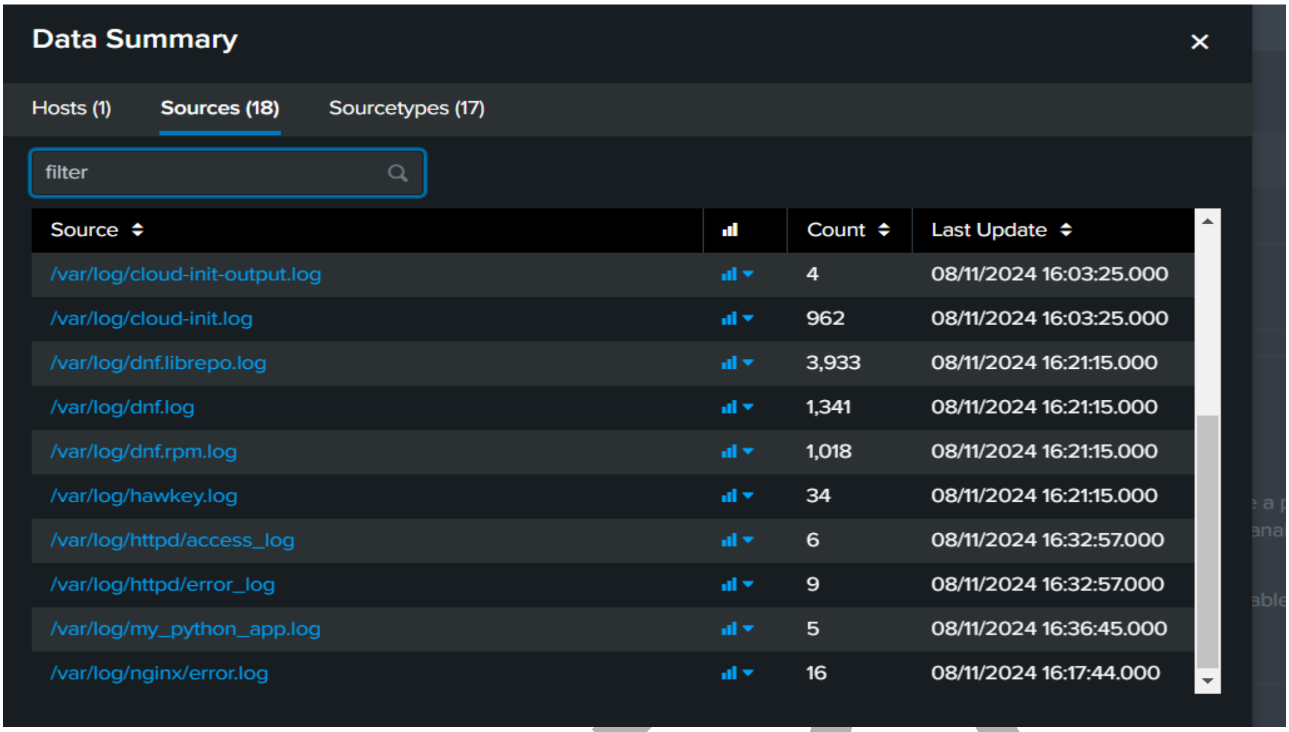
yum install httpd -y

systemctl strat httpd

- Then search your public ip in browser

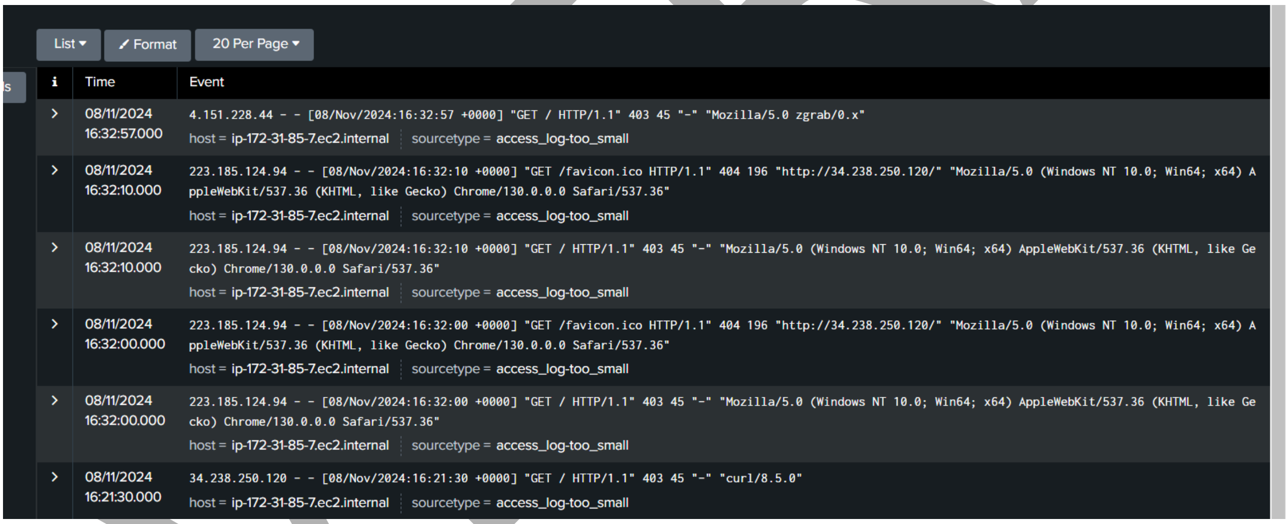
Next go to splunk click on data summery select sources

- Click on httpd/accesslog



Source		Count	Last Update
/var/log/cloud-init-output.log		4	08/11/2024 16:03:25.000
/var/log/cloud-init.log		962	08/11/2024 16:03:25.000
/var/log/dnf.librepo.log		3,933	08/11/2024 16:21:15.000
/var/log/dnf.log		1,341	08/11/2024 16:21:15.000
/var/log/dnf.rpm.log		1,018	08/11/2024 16:21:15.000
/var/log/hawkey.log		34	08/11/2024 16:21:15.000
/var/log/httpd/access_log		6	08/11/2024 16:32:57.000
/var/log/httpd/error_log		9	08/11/2024 16:32:57.000
/var/log/my_python_app.log		5	08/11/2024 16:36:45.000
/var/log/nginx/error.log		16	08/11/2024 16:17:44.000

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



i	Time	Event
>	08/11/2024 16:32:57.000	4.151.228.44 - - [08/Nov/2024:16:32:57 +0000] "GET / HTTP/1.1" 403 45 "-" "Mozilla/5.0 zgrab/0.x" host = ip-172-31-85-7.ec2.internal sourcetype = access_log-too_small
>	08/11/2024 16:32:10.000	223.185.124.94 - - [08/Nov/2024:16:32:10 +0000] "GET /favicon.ico HTTP/1.1" 404 196 "http://34.238.250.120/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.0.0 Safari/537.36" host = ip-172-31-85-7.ec2.internal sourcetype = access_log-too_small
>	08/11/2024 16:32:10.000	223.185.124.94 - - [08/Nov/2024:16:32:10 +0000] "GET / HTTP/1.1" 403 45 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.0.0 Safari/537.36" host = ip-172-31-85-7.ec2.internal sourcetype = access_log-too_small
>	08/11/2024 16:32:00.000	223.185.124.94 - - [08/Nov/2024:16:32:00 +0000] "GET /favicon.ico HTTP/1.1" 404 196 "http://34.238.250.120/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.0.0 Safari/537.36" host = ip-172-31-85-7.ec2.internal sourcetype = access_log-too_small
>	08/11/2024 16:32:00.000	223.185.124.94 - - [08/Nov/2024:16:32:00 +0000] "GET / HTTP/1.1" 403 45 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.0.0 Safari/537.36" host = ip-172-31-85-7.ec2.internal sourcetype = access_log-too_small
>	08/11/2024 16:21:30.000	34.238.250.120 - - [08/Nov/2024:16:21:30 +0000] "GET / HTTP/1.1" 403 45 "-" "curl/8.5.0" host = ip-172-31-85-7.ec2.internal sourcetype = access_log-too_small

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:
```

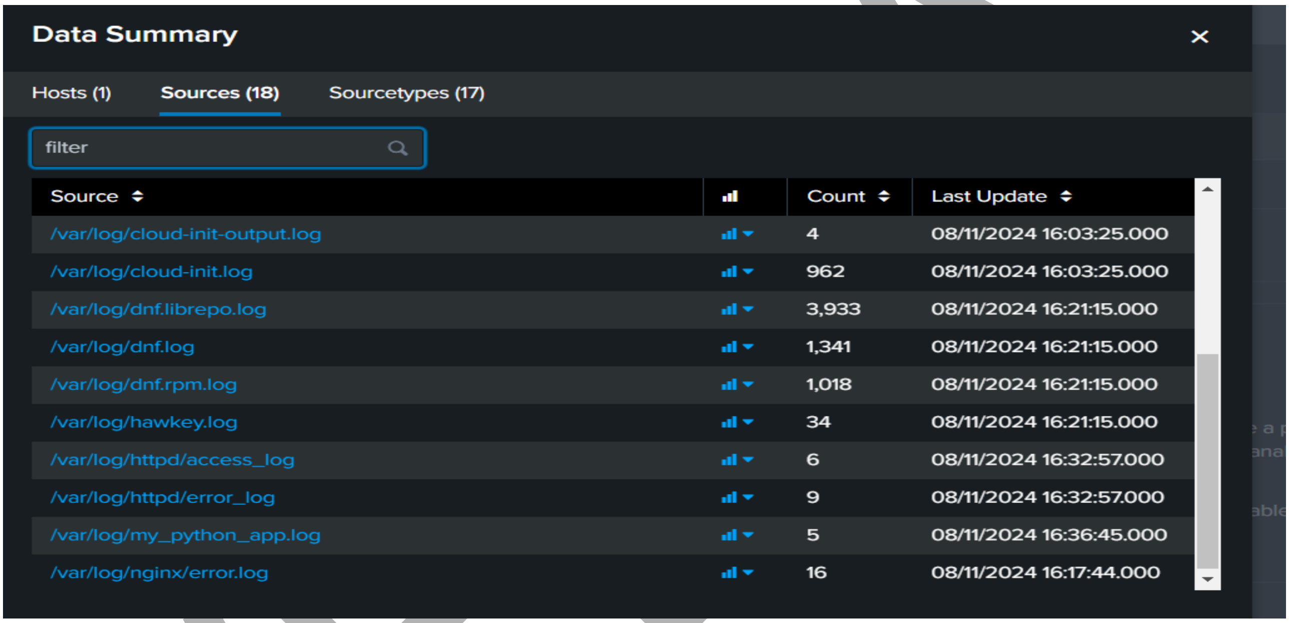
    # Log the error with stack trace

    logging.error("An error occurred: %s", e, exc_info=True)

# Additional success log

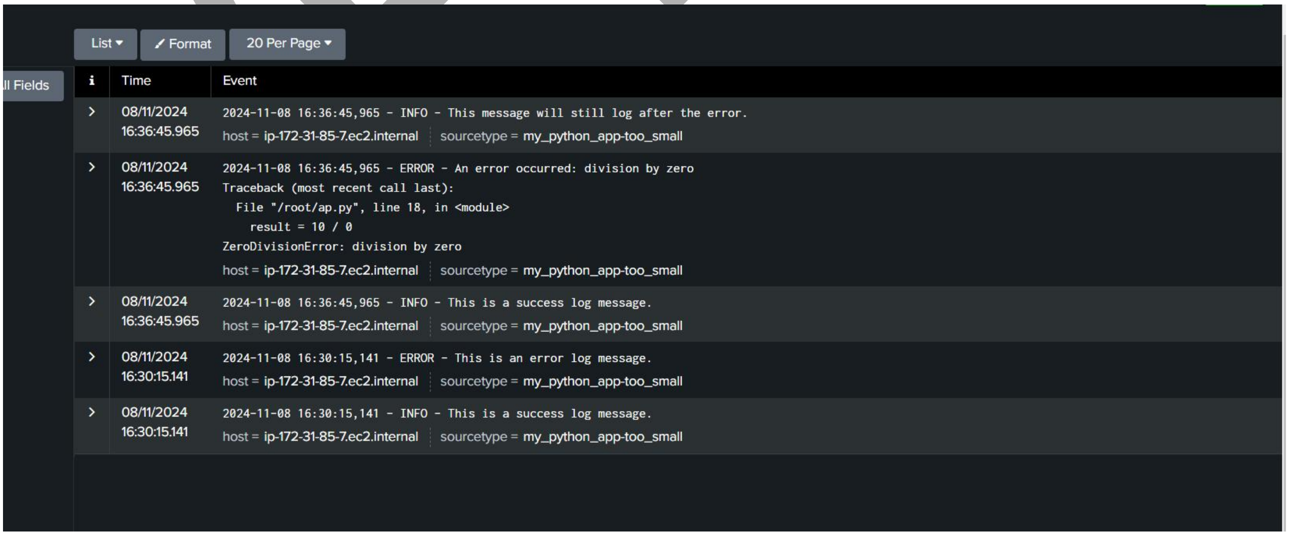
logging.info("This message will still log after the error.")

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



Data Summary

Source		Count	Last Update
/var/log/cloud-init-output.log		4	08/11/2024 16:03:25.000
/var/log/cloud-init.log		962	08/11/2024 16:03:25.000
/var/log/dnf.librepo.log		3,933	08/11/2024 16:21:15.000
/var/log/dnf.log		1,341	08/11/2024 16:21:15.000
/var/log/dnf.rpm.log		1,018	08/11/2024 16:21:15.000
/var/log/hawkey.log		34	08/11/2024 16:21:15.000
/var/log/httpd/access_log		6	08/11/2024 16:32:57.000
/var/log/httpd/error_log		9	08/11/2024 16:32:57.000
/var/log/my_python_app.log		5	08/11/2024 16:36:45.000
/var/log/nginx/error.log		16	08/11/2024 16:17:44.000



i	Time	Event
>	08/11/2024 16:36:45.965	2024-11-08 16:36:45,965 - INFO - This message will still log after the error. host = ip-172-31-85-7.ec2.internal sourcetype = my_python_app-too_small
>	08/11/2024 16:36:45.965	2024-11-08 16:36:45,965 - ERROR - An error occurred: division by zero Traceback (most recent call last): File "/root/ap.py", line 18, in <module> result = 10 / 0 ZeroDivisionError: division by zero host = ip-172-31-85-7.ec2.internal sourcetype = my_python_app-too_small
>	08/11/2024 16:36:45.965	2024-11-08 16:36:45,965 - INFO - This is a success log message. host = ip-172-31-85-7.ec2.internal sourcetype = my_python_app-too_small
>	08/11/2024 16:30:15.141	2024-11-08 16:30:15,141 - ERROR - This is an error log message. host = ip-172-31-85-7.ec2.internal sourcetype = my_python_app-too_small
>	08/11/2024 16:30:15.141	2024-11-08 16:30:15,141 - INFO - This is a success log message. host = ip-172-31-85-7.ec2.internal sourcetype = my_python_app-too_small

These are the python application logs