Training – Day #6

15 June 2023 05:03

#Universal Forwarder

(1) Install Putty

(2) splunk.ppk (key)

(3) Install Universal Forwarder

(4) start Splunk

(5) configuration at UF end (Splunk indexer IP, Port = 9997[default]) => ***Note*** : by default (without any configuration) all the internal data of UF will be forwarded to splunk _internal index

(6) Validate the connection : 2 ways (1) On UF level : through command (2) On Indexer level : through SPL

(7) Define custom logs

(8) Troubleshooting (splunkd.log)

(9) HEC token concept

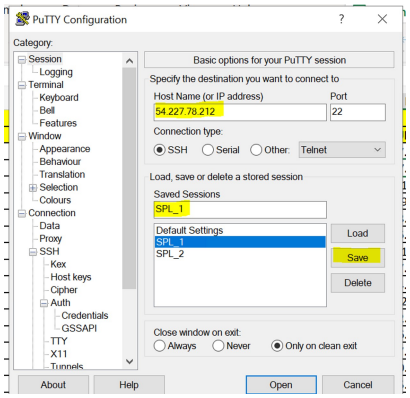
(10) Apps/Add-on

(11) Index-time extraction

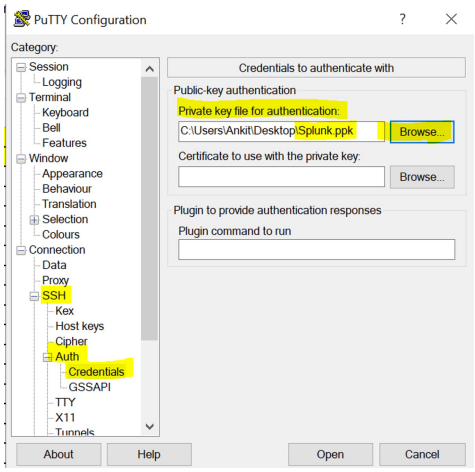
(12) Create Custom source type/line-breaking/event-breaking

Step#1 : Add host-name to putty

SPLK URL 1	SPLK URL 2
54.227.78.212	3.83.207.175



Download splunk.ppk from share-point



Username => **ec2-user**

```
ec2-user@ip-172-31-95-137:~
login as: ec2-user
Authenticating with public key "imported-openssh-key"
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-172-31-95-137 ~]$
```

#Download and Installation of Universal Forwarder :

Step #1 : Download UF on first server (54.227.78.212)

Splunk UF ---- wget -O splunkforwarder-9.0.5-e9494146ae5c-Linux-x86_64.tgz "https://download.splunk.com/products/universalforwarder/releases/9.0.5/linux/splunkforwarder-9.0.5-e9494146ae5c-Linux-x86_64.tgz"

Splunk Enterprise - wget -O splunk-9.0.5-e9494146ae5c-Linux-x86_64.tgz "https://download.splunk.com/products/splunk/releases/9.0.5/linux/splunk-9.0.5-e9494146ae5c-Linux-x86_64.tgz"

Step #2 : untar and unzip => *tar -xvzf <filename>.tgz*

Step #3 : Start the UF and check status =>

cd /splunk forwarder/bin

./splunk start

```
[ec2-user@ip-172-31-95-137 ~]$ cd splunkforwarder/bin/
[ec2-user@ip-172-31-95-137 bin]$ pwd
/home/ec2-user/splunkforwarder/bin
[ec2-user@ip-172-31-95-137 bin]$ ./splunk start
```

Please enter an administrator username: ***splunkufadmin***

Password must contain at least:

* 8 total printable ASCII character(s).

Please enter a new password: ***splunkufadmin***

```
Please enter an administrator username: splunkufadmin
Password must contain at least:
   * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
Creating unit file...
Current splunk is running as non root, which cannot operate systemd unit files.
```

./splunk status

```
[ec2-user@ip-172-31-95-137 bin]$ ./splunk status
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R ec2-user /home/ec2-user/splunkforwarder"
splunkd is running (PID: 25128).
splunk helpers are running (PIDs: 25132).
[ec2-user@ip-172-31-95-137 bin]$
```

#Download and Installation of Splunk Enterprise :

Step #1 : Download Splunk Enterprise on second server (3.83.207.175)

Splunk Enterprise - wget -O splunk-9.0.5-e9494146ae5c-Linux-x86_64.tgz "https://download.splunk.com/products/splunk/releases/9.0.5/linux/splunk-9.0.5-e9494146ae5c-Linux-x86_64.tgz"

Step #2 : untar and unzip => *tar -xvzf <filename>.tgz*

Step #3 : Start the Splunk enterprise and check status =>

cd /home/ec2-user/splunk/bin

./splunk start

```
[ec2-user@ip-172-31-86-162 bin]$ pwd
/home/ec2-user/splunk/bin
[ec2-user@ip-172-31-86-162 bin]$ ./splunk start
```

Please enter an administrator username: ***splunkenadmin***

Password must contain at least:

** 8 total printable ASCII character(s).*

Please enter a new password: ***splunkenadmin***

Please confirm new password: ***splunkenadmin***

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

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

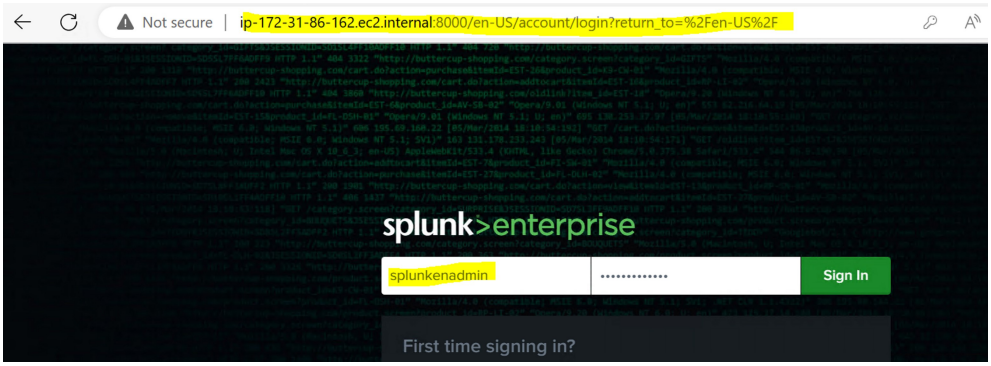
The Splunk web interface is at http://ip-172-31-86-162.ec2.internal:8000

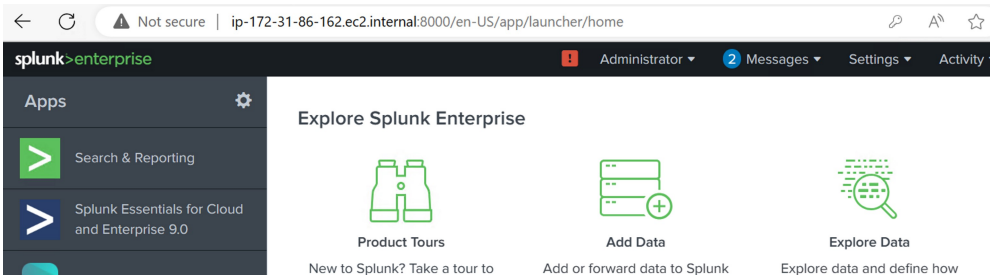
```
Done
                                                           [  OK  ]

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-172-31-86-162.ec2.internal:8000
```

./splunk status

```
[ec2-user@ip-172-31-86-162 bin]$ ./splunk status
splunkd is running (PID: 24820).
splunk helpers are running (PIDs: 24825 24988 25028 25052 25100).
```

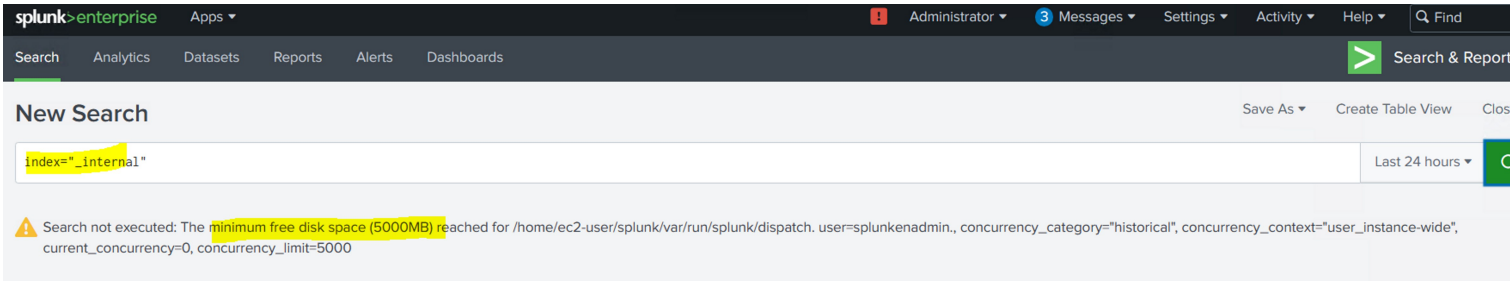
Step #4 : Log into URL => *http://ip-172-31-86-162.ec2.internal:8000*

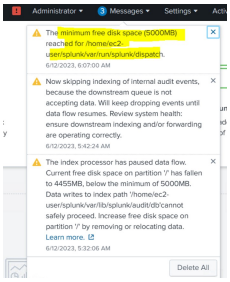




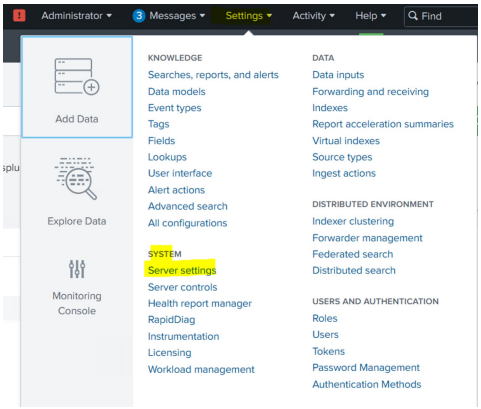
#Fixing Search query by increasing space:

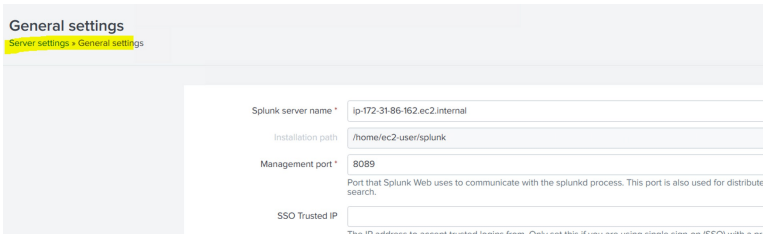
If free disk space is lower than default 5000MB, any search query will not work.





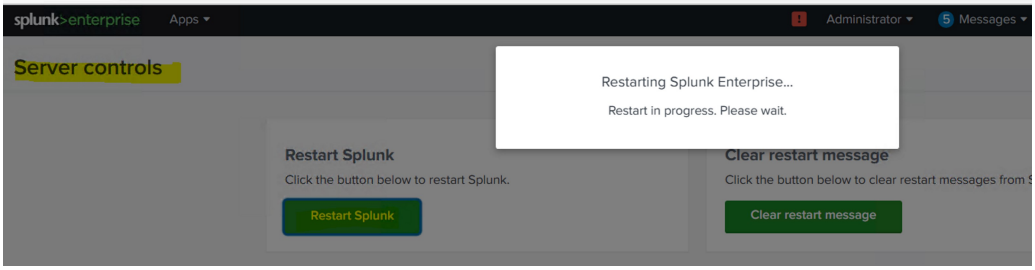
Solution : lower the required space from 5000 MB to 2000 MB.

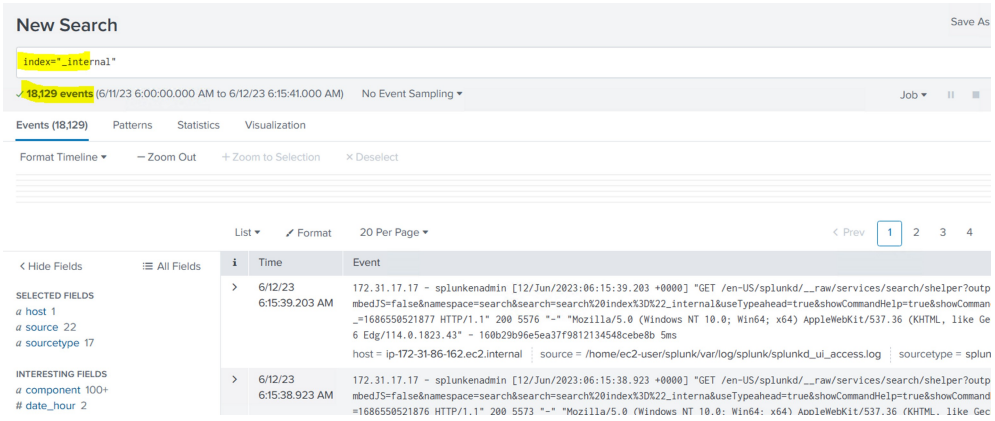




Change it from Default 5000 to 2000

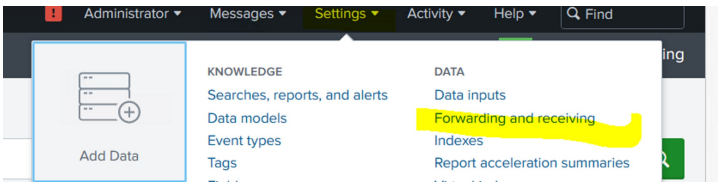
Restart Splunk => Settings > Server Controls => Restart Splunk

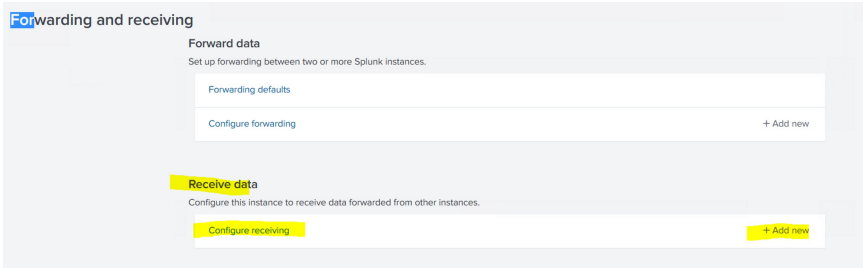


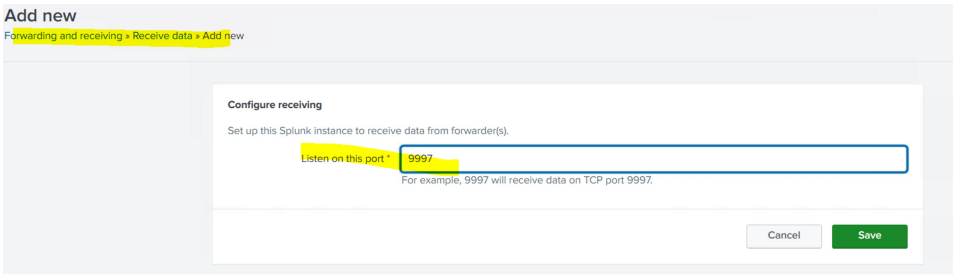


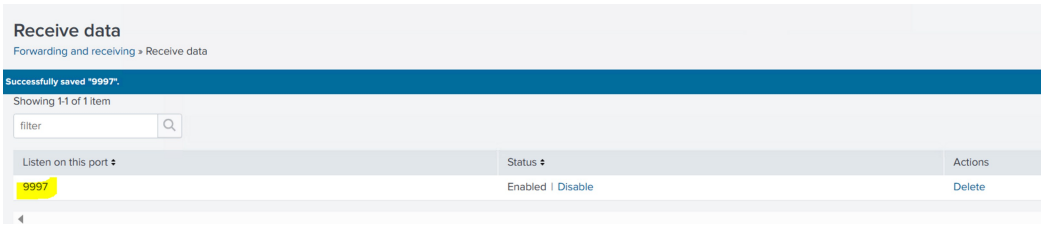
#Enable Port 9997 on Splunk Enterprise and configure UF to communicate on 9997 :

Settings => Forwarding and Receiving => Receiving Data => Add New









#Add forwarder in UF with Indexer Public-IP (Splunk-2)

[ec2-user@ip-172-31-95-137 bin]$ pwd

/home/ec2-user/splunkforwarder/bin

[ec2-user@ip-172-31-95-137 bin]$

[ec2-user@ip-172-31-95-137 bin]$ ./splunk add forward-server 3.83.207.175:9997

```
[ec2-user@ip-172-31-95-137 bin]$ ./splunk add forward-server 3.83.207.175:9997
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R ec2-user /home/ec2-user/splunkforwarder"
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.
Splunk username: splunkufadmin
Password:
Added forwarding to: 3.83.207.175:9997.
[ec2-user@ip-172-31-95-137 bin]$
```

NOTE : Adding forwarder at UF end, does not need restart.

#Check connectivity from Splunk UF end through command:

[ec2-user@ip-172-31-95-137 bin]$ ***./splunk list forward-server***

Warning: Attempting to revert the SPLUNK_HOME ownership

Warning: Executing "chown -R ec2-user /home/ec2-user/splunkforwarder"

WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.

Active forwards:

3.83.207.175:9997

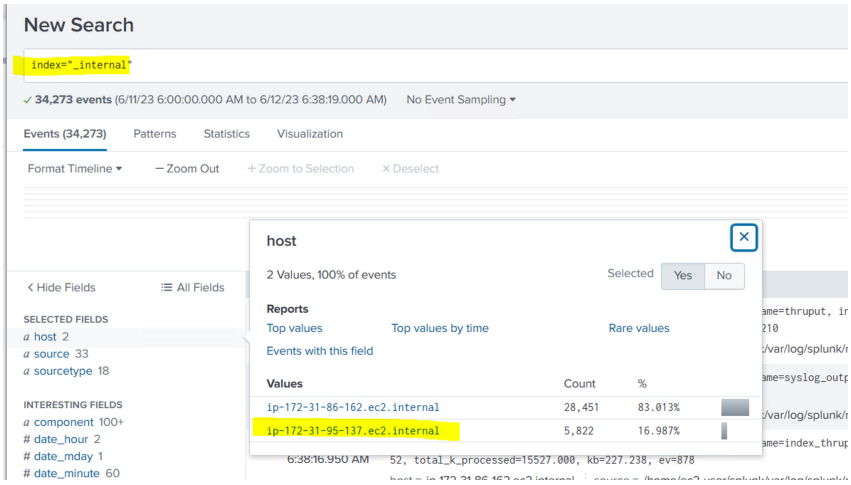
Configured but inactive forwards:

None

[ec2-user@ip-172-31-95-137 bin]$

```
[ec2-user@ip-172-31-95-137 bin]$ ./splunk list forward-server
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R ec2-user /home/ec2-user/splunkforwarder"
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.
Active forwards:
        3.83.207.175:9997
Configured but inactive forwards:
        None
[ec2-user@ip-172-31-95-137 bin]$
```

#Check connectivity from Splunk Enterprise end through SPL :



#Create Custom Log and forward its data to splunk.

Step #1 : create a sample file test.txt with few line in /tmp on UF server.

```
[ec2-user@ip-172-31-95-137 bin]$ cd /tmp/
[ec2-user@ip-172-31-95-137 tmp]$ vi test.txt
[ec2-user@ip-172-31-95-137 tmp]$ more test.txt
Hi, This is the 1st line.
Hi, This is the 2nd line.
```

Step #2: create input.conf with required in for and restart UF.

```
/home/ec2-user/splunkforwarder/etc/system/local
[ec2-user@ip-172-31-95-137 local]$
[ec2-user@ip-172-31-95-137 local]$
[ec2-user@ip-172-31-95-137 local]$ ls
README  outputs.conf  server.conf
```

cd /home/ec2-user/splunkforwarder/etc/system/local

vi inputs.conf

[monitor:///tmp/test.txt]

disabled = 0

README inputs.conf outputs.conf server.conf

[ec2-user@ip-172-31-95-137 local]$ more inputs.conf

[monitor:///tmp/test.txt]

disabled = 0

```
[ec2-user@ip-172-31-95-137 local]$ vi inputs.conf
[ec2-user@ip-172-31-95-137 local]$ more inputs.conf
[monitor:///tmp/test.txt]
disabled = 0
```

```
[ec2-user@ip-172-31-95-137 local]$ ls
README  inputs.conf  outputs.conf  server.conf
```

Restart UF =>

[ec2-user@ip-172-31-95-137 local]$ **cd /home/ec2-user/splunkforwarder**

[ec2-user@ip-172-31-95-137 splunkforwarder]$ **cd bin/**

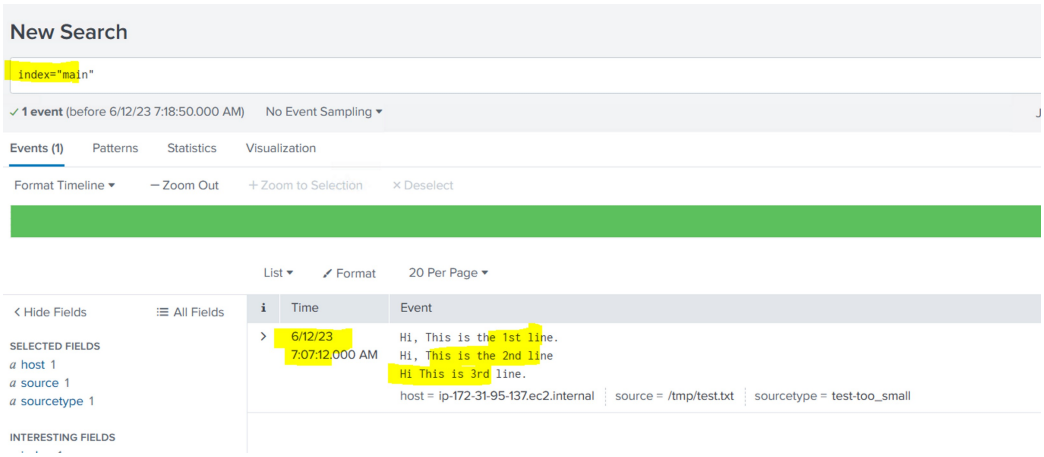
[ec2-user@ip-172-31-95-137 bin]$ pwd

/home/ec2-user/splunkforwarder/bin

[ec2-user@ip-172-31-95-137 bin]$

[ec2-user@ip-172-31-95-137 bin]$ ./**splunk restart**

Check the data in => index="main"



outputs.conf

cd /home/ec2-user/splunkforwarder/etc/system/local/

[ec2-user@ip-172-31-95-137 local]$ ls

README input.conf inputs.conf outputs.conf server.conf

[ec2-user@ip-172-31-95-137 local]$ more outputs.conf

[tcpout]

defaultGroup = default-autolb-group

[tcpout:default-autolb-group]

server = 3.83.207.175:9997

[tcpout-server://3.83.207.175:9997]

[ec2-user@ip-172-31-95-137 local]$

server.conf

[ec2-user@ip-172-31-95-137 local]$ more server.conf

[general]

serverName = ip-172-31-95-137.ec2.internal

pass4SymmKey = 7hEs+I0R6C0/ifi8ryCelkuWlNDeVNq7KbChA78nQ6qfpO6cuoM7oCA==

[sslConfig]

sslPassword = 7ptmqRUEmka2o59j4u7+tM4caP86ho9guU5rtadk6RNcylYflzcjFjA==

[lmpool:auto_generated_pool_forwarder]

description = auto_generated_pool_forwarder

*peers = **

quota = MAX

stack_id = forwarder

[lmpool:auto_generated_pool_free]

description = auto_generated_pool_free

*peers = **

quota = MAX

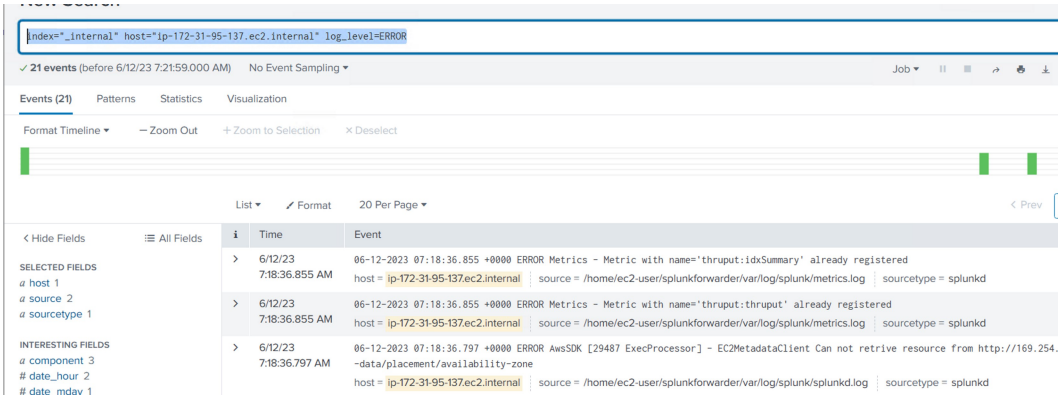
stack_id = free

#Troubleshooting:

(1) ping

(2) tcpdump

(3) SPL => ***index="_internal" host="ip-172-31-95-137.ec2.internal" log_level=ERROR***


index="_internal" host="ip-172-31-95-137.ec2.internal" log_level=ERROR
21 events (before 6/12/23 7:21:59.000 AM)
No Event Sampling
Job
Events (21)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
List
Format
20 Per Page
Prev
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 2
a sourcetype 1
INTERESTING FIELDS
a component 3
date_hour 2
date_mday 1
Time
Event
6/12/23 7:18:36.855 AM
06-12-2023 07:18:36.855 +0000 ERROR Metrics - Metric with name='thruput:idxSummary' already registered
host = ip-172-31-95-137.ec2.internal
source = /home/ec2-user/splunkforwarder/var/log/splunk/metrics.log
sourcetype = splunkd
6/12/23 7:18:36.855 AM
06-12-2023 07:18:36.855 +0000 ERROR Metrics - Metric with name='thruput:thruput' already registered
host = ip-172-31-95-137.ec2.internal
source = /home/ec2-user/splunkforwarder/var/log/splunk/metrics.log
sourcetype = splunkd
6/12/23 7:18:36.797 AM
06-12-2023 07:18:36.797 +0000 ERROR AwsSDK [29487 ExecProcessor] - EC2MetadataClient Can not retrive resource from http://169.254.
-data/placement/availability-zone
host = ip-172-31-95-137.ec2.internal
source = /home/ec2-user/splunkforwarder/var/log/splunk/splunkd.log
sourcetype = splunkd