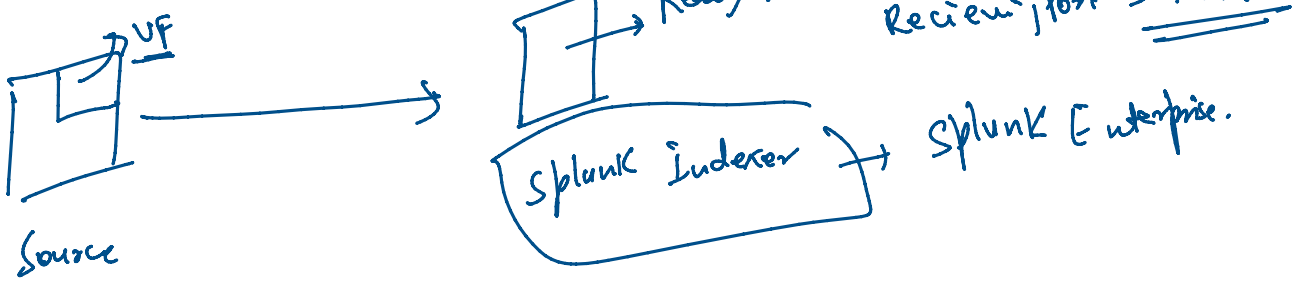
Day - 2

11 August 2024 23:01

1. Ingest data from UF to splunk Indexer



(1) Provision 2 server.
(2) One Server → Install UF
Second Server → Install SE
(3) Enable Reciever port on Indexer.
(4) Conf. on the Source end.
(1) Inputs.conf
(2) Outputs.conf
(5.) Sending default log to splunk
(6.) Sending specific / Custom logs.
(7.) Troubleshooting / Validation part
→ Data is not coming splunk
→ Whether conn. b/w UF & Indexer Successful or not.
splunkd.log
Conn.
Port Communication

(1) UF
(2) HEC Token (Http event Collector)
(3) TCP or UDP
(4) Scripted Input.
(5) Apps & Add-on.

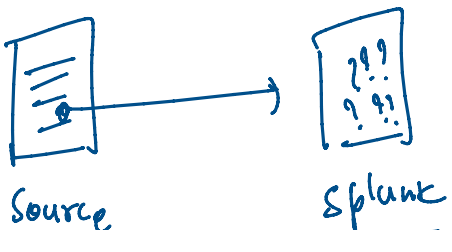
Splunk UF ------> wget -O splunkforwarder-9.3.0-51ccf43db5bd-Linux-x86_64.tgz "https://download.splunk.com/products/universalforwarder/releases/9.3.0/linux/splunkforwarder-9.3.0-51ccf43db5bd-Linux-x86_64.tgz"

Installation of Splunk UF -----

```
1  wget -O splunkforwarder-9.3.0-51ccf43db5bd-Linux-x86_64.tgz "https://download.splunk.com/products/universalforwarder/releases/9.3.0/linux/splunkforwarder-9.3.0-51ccf43db5bd-Linux-x86_64.tgz"
2  ll
3  tar xvzf splunkforwarder-9.3.0-51ccf43db5bd-Linux-x86_64.tgz    ----------> Untaring the package having tar.gz format
4  ll  ----------> Listing the file
5  clear
7  ll
8  cd splunkforwarder/bin/       ----------> cd is for change directory
9  ./splunk start    ------> Starting the splunk service
10  clear
11  history
```

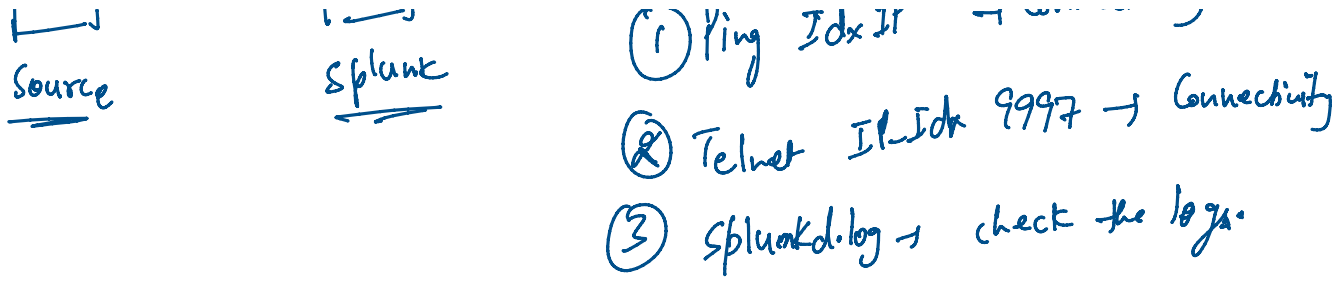
Installation of Splunk Indexer ----

```
1  wget -O splunk-9.3.0-51ccf43db5bd-Linux-x86_64.tgz "https://download.splunk.com/products/splunk/releases/9.3.0/linux/splunk-9.3.0-51ccf43db5bd-Linux-x86_64.tgz"
2  ll
3  tar xvzf splunk-9.3.0-51ccf43db5bd-Linux-x86_64.tgz
4  ll
5  cd splunk/bin/
6  ./splunk start
7  history
```



If the data forwarding is stopped?

(1) Ping Idx IP → Connectivity
→ conn. → Connectivity



SPL Command -----> index=_internal source=*splunkd.log* host="ip-172-31-92-111.ec2.internal" log_level=ERROR

Log Path -----> /home/ec2-user/splunkforwarder/var/log/splunk

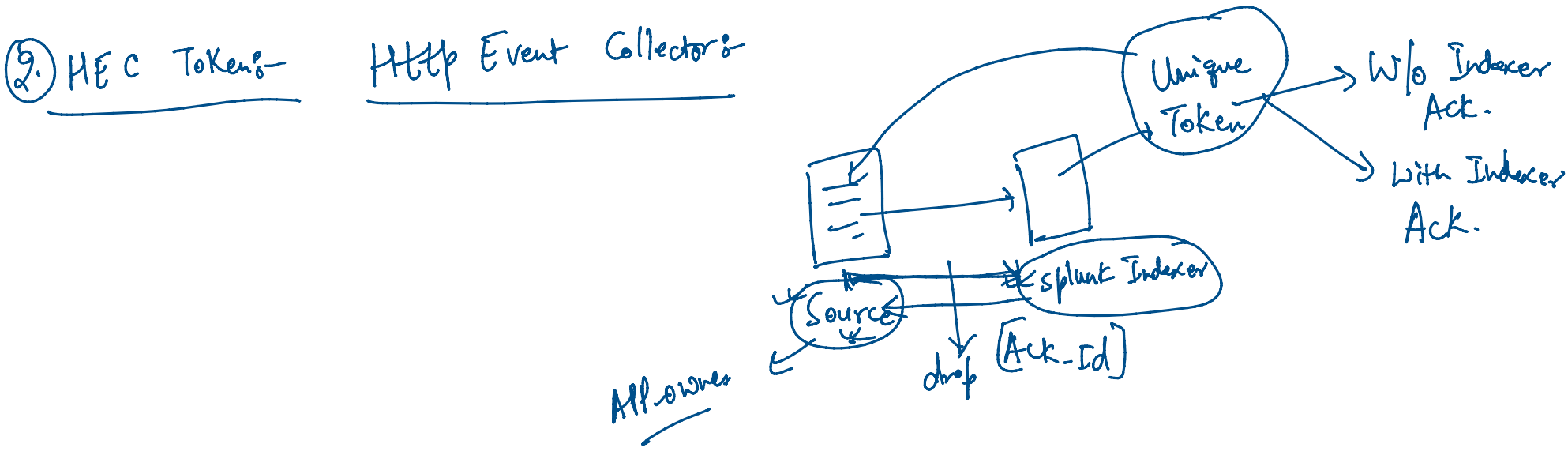
Outputs.conf ----------> This need to be on the Forwarder side (/home/ec2-user/splunkforwarder/etc/system/local)

```
[monitor:///tmp/forward-data/test.txt]
disabled = 0

[monitor:///tmp/forward-data/test1.txt]
index = vk_idx
sourcetype = vk_src
disabled = 0
```

Inputs.conf ----------> This need to be configured on forwarder side (/home/ec2-user/splunkforwarder/etc/system/local)

```
[tcpout]
defaultGroup = default-autolb-group
[tcpout:default-autolb-group]
server = 54.175.14.11:9997

[tcpout-server://54.175.14.11:9997]
```

./splunk enable forward-server 54.175.14.11:9997 [Indexex IP_adress:receiving_port_number] ----------> Connect the forwarder with Indexer
./splunk list forward-server ------> List the indexers connected with forwarder



HEC CODE -----

```
C:\Users\Vivek>curl -k https://127.0.0.1:8088/services/collector -H "Authorization:Splunk f5d5cc47-62de-462a-925f-6c7a71ac06b8" -d "{\"sourcetype\": \"trail\", \"event\":\"hello world\"}"
{"text":"Success","code":0}
C:\Users\Vivek>curl -k https://127.0.0.1:8088/services/collector -H "Authorization:Splunk f5d5cc47-62de-462a-925f-6c7a71ac06b8" -d "{\"sourcetype\": \"trail\", \"event\":\"hello world123\"}"
{"text":"Success","code":0}
C:\Users\Vivek>
C:\Users\Vivek>
C:\Users\Vivek>curl -k https://127.0.0.1:8088/services/collector -H "Authorization:Splunk ad2fe798-6c06-4a34-8edb-04fe0811a758" -d "{\"sourcetype\": \"trail\", \"event\":\"hello world123\"}"
{"text":"Data channel is missing","code":10}
C:\Users\Vivek>
C:\Users\Vivek>
C:\Users\Vivek>curl -k https://127.0.0.1:8088/services/collector/ack?channel=03f3d08c-52b3-4819-9d59-b70fea7f9e62 -H
"Authorization:Splunk ad2fe798-6c06-4a34-8edb-04fe0811a758" -d "{\"sourcetype\": \"trail\", \"event\":\"hello world12
3 with acks\"}"
{"text":"Invalid data format","code":6}
C:\Users\Vivek>curl -k https://127.0.0.1:8088/services/collector?channel=03f3d08c-52b3-4819-9d59-b70fea7f9e62 -H "Authorization:Splunk ad2fe798-6c06-4a34-8edb-04fe0811a758" -d
"{\"sourcetype\": \"trail\", \"event\":\"hello world123 with acks\"}"
{"text":"Success","code":0,"ackId":0}
C:\Users\Vivek>curl -k https://127.0.0.1:8088/services/collector?channel=03f3d08c-52b3-4819-9d59-b70fea7f9e62 -H "Authorization:Splunk ad2fe798-6c06-4a34-8edb-04fe0811a758" -d
"{\"sourcetype\": \"trail\", \"event\":\"hello world1234 with acks\"}"
{"text":"Success","code":0,"ackId":1}
C:\Users\Vivek>curl -k https://127.0.0.1:8088/services/collector?channel=03f3d08c-52b3-4819-9d59-b70fea7f9e62 -H "Authorization:Splunk ad2fe798-6c06-4a34-8edb-04fe0811a758" -d
"{\"sourcetype\": \"trail\", \"event\":\"hello world12345 with acks\"}"
{"text":"Success","code":0,"ackId":2}
C:\Users\Vivek>
C:\Users\Vivek>
C:\Users\Vivek>curl -k https://127.0.0.1:8088/services/collector/ack?channel=03f3d08c-52b3-4819-9d59-b70fea7f9e62 -H
"Authorization:Splunk ad2fe798-6c06-4a34-8edb-04fe0811a758" -d "{\"acks\": [0]}"
{"acks":{"0":true}}
C:\Users\Vivek>curl -k https://127.0.0.1:8088/services/collector/ack?channel=03f3d08c-52b3-4819-9d59-b70fea7f9e62 -H "Authorization:Splunk ad2fe798-6c06-4a34-8edb-04fe0811a758" -d
"{\"acks\": [6]}"
{"acks":{"6":false}}
C:\Users\Vivek>curl -k https://127.0.0.1:8088/services/collector/ack?channel=03f3d08c-52b3-4819-9d59-b70fea7f9e62 -H "Authorization:Splunk ad2fe798-6c06-4a34-8edb-04fe0811a758" -d
"{\"acks\": [2]}"
{"acks":{"2":true}}
C:\Users\Vivek>curl -k https://127.0.0.1:8088/services/collector/ack?channel=03f3d08c-52b3-4819-9d59-b70fea7f9e62 -H "Authorization:Splunk ad2fe798-6c06-4a34-8edb-04fe0811a758" -d
"{\"acks\": [22]}"
{"acks":{"22":false}}
```

C:\Users\Vivek>

Tomorrow's (12th Aug.)

1. App & Add-on.
2. Scripted Input.
3. Syslog (Security Logs)