SPLUNK DAY 2

UF to INDEXER

Prerequisites:

- **UF**
  - **Install Splunk UF package (untar & start splunk process)**
  - **check connectivity to indexer on port 9997**

- **Indexer**
  - **install Splunk Enterprise (untar & start splunk process)**
  - **Enable 9997 receiving port on this instance**
    to enable receiving port on indexer over 9997

    method1
    UI/web based
    1. Login to SPlunk web
    2. Go to Setttings --> Data(forwarding & receiving)
    enable receiving by clicking on add item --> add 9997 and save it

    method2
    CLI based
    /opt/splunk/bin/splunk enable listen 9997

    method3 (if you follow this method you have restart splunkd)
    config based
    inputs.conf
    [splunktcp://9997]
    connection_host = ip

    check if splunkd is listening on 9997
    netstat -anp|grep :9997
  - **check firewall if indexer is listening on 9997**

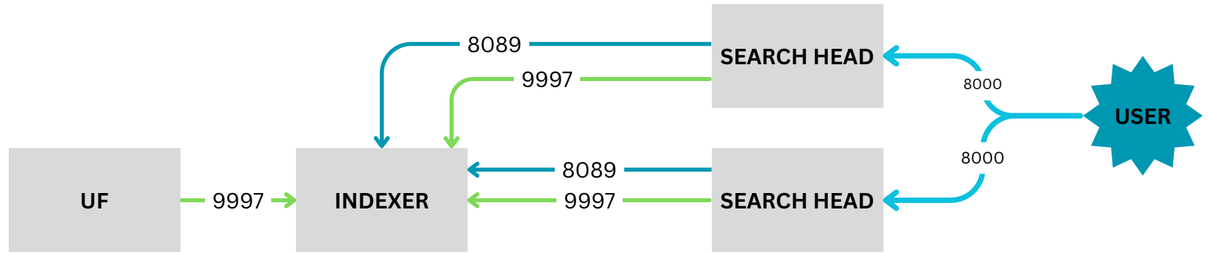
Steps:

1. **Login to UF CLI**
2. **check if splunkd process is running**
   a. **/opt/splunkforwarder/bin/splunk status**

1. **Craete a file outputs.conf in /opt/splunkforwarder/etc/system/local/**
2. **https://help.splunk.com/en/splunk-enterprise/administer/admin-manual/9.4/configuration-file-reference/9.4.4-configuration-file-reference/outputs.conf#outputs.conf.example-0**
   a. **vi /opt/splunkforwarder/etc/system/local/outputs.conf**
   [tcpout]
   defaultGroup = splunksession

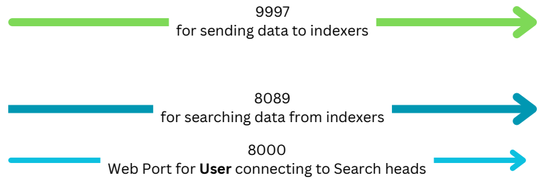
   [tcpout:splunksession]
   server = <indexerIP>:9997

1. **Create a file inputs.conf in /opt/splunkforwarder/etc/system/local/ and a file to monitor the data /opt/splunkforwarder/testfile.log.**
   vi /opt/splunkforwarder/etc/system/local/inputs.conf
   [monitor:///opt/splunkforwarder/testfile.log]
   index = main
   sourcetype=test_access
   #_TCP_ROUTING = splunksession → if you want to send data to specific group.




```
[root@ip-172-31-36-122 local]#
[root@ip-172-31-36-122 local]# /opt/splunk/bin/splunk status
splunkd is running (PID: 3798).
splunk helpers are running (PIDs: 3800 4122 4127 4177 4288 4907).
[root@ip-172-31-36-122 local]# /opt/splunk/bin/splunk enable listen 9997
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServe
rName for details.
Splunk username: admin
Password:
Listening for Splunk data on TCP port 9997.
[root@ip-172-31-36-122 local]#
[root@ip-172-31-36-122 local]#
[root@ip-172-31-36-122 local]#
```

```
[root@ip-172-31-36-122 local]#
[root@ip-172-31-36-122 local]#
[root@ip-172-31-36-122 local]#
[root@ip-172-31-36-122 local]# netstat -anp|grep :9997
tcp        0      0 0.0.0.0:9997            0.0.0.0:*               LISTEN      3798/splunkd
[root@ip-172-31-36-122 local]#
[root@ip-172-31-36-122 local]#
[root@ip-172-31-36-122 local]#
[root@ip-172-31-36-122 local]#
[root@ip-172-31-36-122 local]#
```




```
[root@ip-172-31-34-118 local]# nc -zv 3.108.191.143 9997
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Connected to 3.108.191.143:9997.
Ncat: 0 bytes sent, 0 bytes received in 0.07 seconds.
[root@ip-172-31-34-118 local]#
[root@ip-172-31-34-118 local]#
[root@ip-172-31-34-118 local]#
[root@ip-172-31-34-118 local]#
```

```
[root@ip-172-31-34-118 local]#
[root@ip-172-31-34-118 local]#
[root@ip-172-31-34-118 local]# vi /opt/splunkforwarder/etc/system/local/outputs.conf
[root@ip-172-31-34-118 local]#
[root@ip-172-31-34-118 local]#
[root@ip-172-31-34-118 local]# vi /opt/splunkforwarder/etc/system/local/inputs.conf
[root@ip-172-31-34-118 local]#
[root@ip-172-31-34-118 local]#
[root@ip-172-31-34-118 local]# cat /opt/splunkforwarder/etc/system/local/inputs.conf
[monitor:///opt/splunkforwarder/testfile.log]
index = main
sourcetype=test_access
host = ramesh
[root@ip-172-31-34-118 local]#
[root@ip-172-31-34-118 local]#
[root@ip-172-31-34-118 local]# cat /opt/splunkforwarder/etc/system/local/outputs.conf
[tcpout]
defaultGroup = splunksession

[tcpout:splunksession]
server = 3.108.191.143:9997
[root@ip-172-31-34-118 local]#
[root@ip-172-31-34-118 local]# /opt/splunkforwarder/bin/splunk restart^C
[root@ip-172-31-34-118 local]#
[root@ip-172-31-34-118 local]#
[root@ip-172-31-34-118 local]#
[root@ip-172-31-34-118 local]#
```

```
[root@ip-172-31-34-118 splunkforwarder]#
[root@ip-172-31-34-118 splunkforwarder]# pwd
/opt/splunkforwarder
[root@ip-172-31-34-118 splunkforwarder]#
[root@ip-172-31-34-118 splunkforwarder]#
[root@ip-172-31-34-118 splunkforwarder]# vi testfile.log
[root@ip-172-31-34-118 splunkforwarder]# cat testfile.log
This is a test data for sending text from UF to indexer
[root@ip-172-31-34-118 splunkforwarder]#
[root@ip-172-31-34-118 splunkforwarder]#
```

DEBUG Comands

[root@ip-172-31-46-249 local]# /opt/splunk/bin/splunk btool inputs list --debug
[root@ip-172-31-46-249 local]# ^C
[root@ip-172-31-46-249 local]# ^C
[root@ip-172-31-46-249 local]# /opt/splunk/bin/splunk btool inputs list splunktcp --debug
[root@ip-172-31-46-249 local]# ^C
[root@ip-172-31-46-249 local]# /opt/splunk/bin/splunk show config inputs

```
[root@ip-172-31-46-249 local]# ^C
[root@ip-172-31-46-249 local]# /opt/splunk/bin/splunk btool inputs list splunktcp://9997
[splunktcp://9997]
_rcvbuf = 1572864
connection_host = ip
disabled = 0
host = $decideOnStartup
index = default
[root@ip-172-31-46-249 local]#
[root@ip-172-31-46-249 local]#
[root@ip-172-31-46-249 local]#
[root@ip-172-31-46-249 local]# /opt/splunk/bin/splunk btool inputs list splunktcp://9997 --debug
/opt/splunk/etc/apps/search/local/inputs.conf [splunktcp://9997]
/opt/splunk/etc/system/default/inputs.conf    _rcvbuf = 1572864
/opt/splunk/etc/apps/search/local/inputs.conf connection_host = ip
/opt/splunk/etc/apps/search/local/inputs.conf disabled = 0
/opt/splunk/etc/system/default/inputs.conf    host = $decideOnStartup
/opt/splunk/etc/system/default/inputs.conf    index = default
[root@ip-172-31-46-249 local]#
[root@ip-172-31-46-249 local]#
[root@ip-172-31-46-249 local]#
[root@ip-172-31-46-249 local]#
```

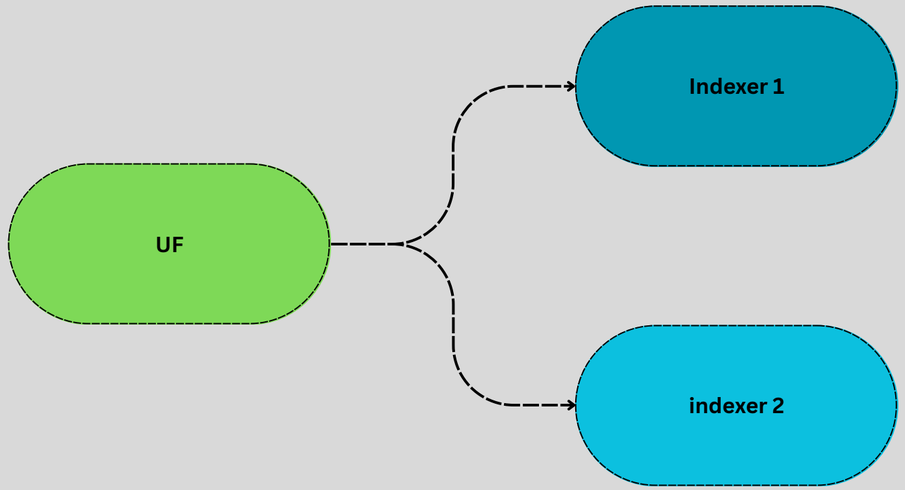
```
[root@ip-172-31-37-21 local]#
[root@ip-172-31-37-21 local]#
[root@ip-172-31-37-21 local]# cat outputs.conf
[tcpout]
defaultGroup = mahesh


[tcpout:mahesh]
server = 13.201.57.159:9997


[tcpout:ramesh]
server = 13.201.86.156:9997

[root@ip-172-31-37-21 local]#
[root@ip-172-31-37-21 local]# cat inputs.conf
[default]
host = uf

[monitor:///opt/mahesh.txt]
index = mah_splunk
sourcetype = alltextfiles
 TCP_ROUTING = ramesh
[root@ip-172-31-37-21 local]#
[root@ip-172-31-37-21 local]#
```



UF configurations

##

Steps:

1. Install UF
2. Start UF accept license
3. configure outputs.conf

   outputs.conf

   [tcpout]

   defaultGroup =

   [tcpout:indexerGroup1]

   server = indexer1IP:9997

   [tcpout:indexerGroup2]

   server = indexer2IP:9997

1. inputs.conf

   vi ...../local/inputs.conf

   [monitor:///opt/montiorfiles1/*]

   host=uf

   index=main

   sourcetype=montiorfiles1

   _TCP_ROUTING = indexerGroup1

   [monitor:///opt/montiorfiles2/*]

   host=uf

   index=main

   sourcetype=montiorfiles2

   _TCP_ROUTING = indexerGroup2

   - After configuring above config file, Restart splunkd

https://help.splunk.com/en/splunk-enterprise/administer/admin-manual/9.4/configuration-file-reference/9.4.4-configuration-file-reference/inputs.conf

Indexer Configurations

##

###

Steps:

1. Install SPlunk enterprise
2. start and accept license
3. enable 9997 port using any one of 3 methods

   /opt/splunk/bin/splunk enable listen 9997
4.

Todays Topics

Bootstarting splunk
inputs.conf (crcSalt,initCrcLength, ignoreOlderthan)
props.conf
transforms.conf
Renaming hostname using transforms.conf

Bootstarting splunk
/opt/splunkforwarder/bin/splunk **enable boot-start** -user root
cat /etc/systemd/system/SplunkForwarder.service
systemctl status SplunkForwarder
systemctl start SplunkForwarder
systemctl status SplunkForwarder
systemctl restart SplunkForwarder

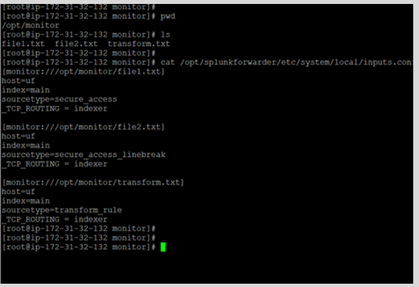
inputs.conf

[monitor://<PATH>]
host = google.com
sourcetype = google_access
crcSalt = <SOURCE>
initCrcLength = 256 bytes
#Cannot be less than 256 or more than 1048576
ignoreOlderthan = 1d

[root@ip-172-31-32-132 local]# cat inputs.conf
[monitor:///opt/monitor/file1.txt]
host=uf
index=main
sourcetype=secure_access
_TCP_ROUTING = indexer

[monitor:///opt/monitor/file2.txt]
host=uf
index=main
sourcetype=secure_access_linebreak
_TCP_ROUTING = indexer

##################################
[root@ip-172-31-32-132 local]# cat outputs.conf
[tcpout:indexer]
server = 15.206.159.98:9997
[root@ip-172-31-32-132 local]#



Props.conf

[secure_access]
SHOULD_LINEMERGE=false
LINE_BREAKER=([\r\n]+)
BREAK_ONLY_BEFORE_DATE=null
NO_BINARY_CHECK=true
CHARSET=UTF-8
MAX_TIMESTAMP_LOOKAHEAD=50
TIME_FORMAT=%a %b %d %Y %H:%M:%S
TIME_PREFIX=^
TZ=Asia/Kolkata
description=this is for tutorial

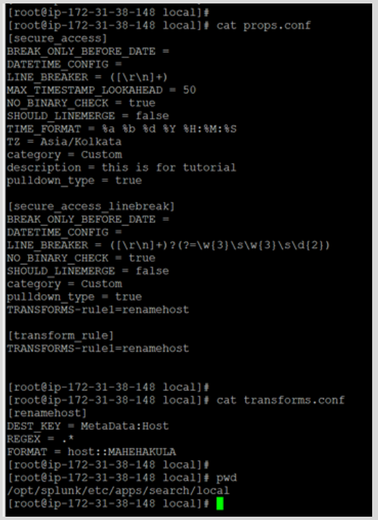
[secure_access]
BREAK_ONLY_BEFORE_DATE =
DATETIME_CONFIG =
LINE_BREAKER = ([\r\n]+)
MAX_TIMESTAMP_LOOKAHEAD = 50
NO_BINARY_CHECK = true
SHOULD_LINEMERGE = false
TIME_FORMAT = %a %b %d %Y %H:%M:%S
TZ = Asia/Kolkata
category = Custom
description = this is for tutorial
pulldown_type = true

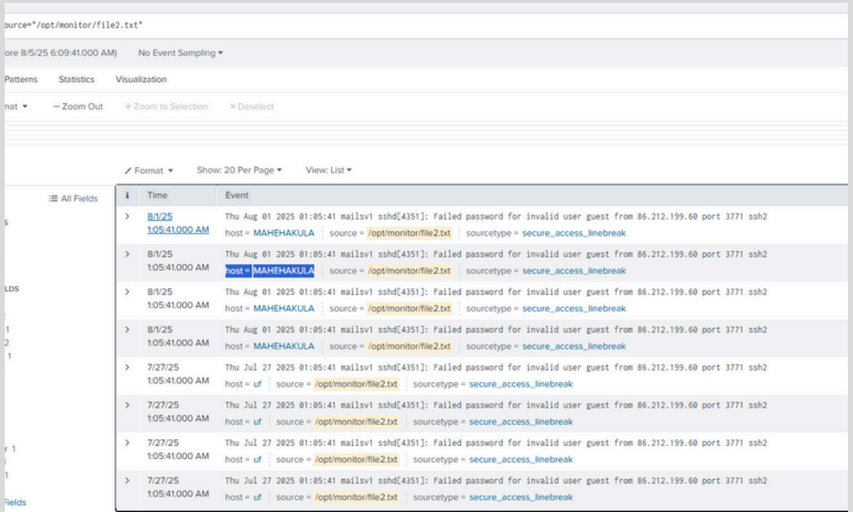
[secure_access_linebreak]
BREAK_ONLY_BEFORE_DATE =
DATETIME_CONFIG =
LINE_BREAKER = ([\r\n]+)?(?=\w{3}\s\w{3}\s\d{2})
NO_BINARY_CHECK = true
SHOULD_LINEMERGE = false
category = Custom
pulldown_type = true
TRANSFORMs-rule1=renamehost

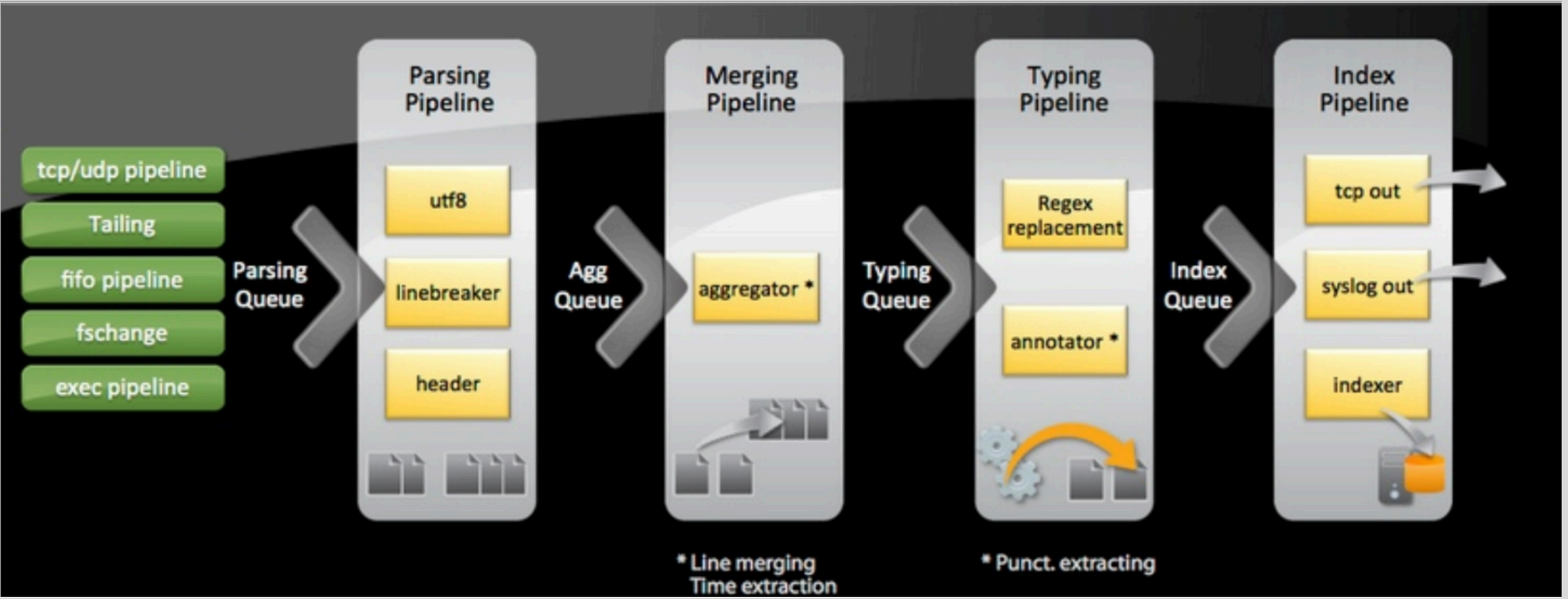
TRANSFORMS-<class> = <transform_stanza_name>, <transform_stanza_name2>

transforms.conf

[renamehost]
DEST_KEY = MetaData:Host
REGEX = .*
FORMAT = host::UniversalForwarder
##Renaming host name during parsing stage






tcp/udp pipeline
Tailing
fifo pipeline
fschange
exec pipeline
Parsing Queue
Parsing Pipeline
utf8
linebreaker
header
Agg Queue
Merging Pipeline
aggregator *
* Line merging
Time extraction
Typing Queue
Typing Pipeline
Regex replacement
annotator *
* Punct. extracting
Index Queue
Index Pipeline
tcp out
syslog out
indexer

Todays Topics

- How data is processed in Splunk?
- Stages - Pipelines & Queues
-
- How to add metadata Fields for all events in splunk?
- How to send redundant data to NullQueue?
- How to send data to a specific tcpout group/indexergroup?
- HTTP event Collector –
  - Token Generation
  - Port configuration
  - send sample data to main index

4 phases

- input
- parsing
- indexing
- searching

During Parsing phase

- Parsing queue → Parsing Pipeline → Agg queue → Merging Pipeline → Typing queue--> Typing Pipeline → Index Queue → Index Pipeline

https://docs.splunk.com/Documentation/Splunk/9.4.2/Admin/Propsconf
https://docs.splunk.com/Documentation/Splunk/9.4.2/Admin/Inputsconf
https://docs.splunk.com/Documentation/Splunk/9.4.2/Admin/Transformsconf#transforms.conf
https://help.splunk.com/en/splunk-enterprise/search/spl-search-reference/9.1/time-format-variables-and-modifiers/date-and-time-format-variables
https://help.splunk.com/en/splunk-enterprise/get-started/get-data-in/9.3/get-data-with-http-event-collector/use-curl-to-manage-http-event-collector-tokens-events-and-services

outputs.conf
[tcpout:indexer]
server = 15.206.159.98:9997, idx2:9997, idx3:9997

How to add metadata Fields for all events in splunk?
################### INDEXER ######################
props.conf
[default]
TRANSFORMS-appIttoall = apply_to_all

transforms.conf
[apply_to_all]
REGEX = .
FORMAT = processed_by::SplunkSessionIndexer1
WRITE_META = true

To sent data to Null queue when ever there is an event with (Code=F)
props.conf
[source::/opt/monitorlogs/nullQueuelogs.txt]
TRANSFORMS-nullQueue = send_to_nullqueue

transforms.conf
[send_to_nullqueue]
REGEX = Code\=F
DEST_KEY = queue
FORMAT = nullQueue

To sent data toa specific tcp group when ever there is an event with (Code=F)
[source::/opt/monitorlogs/nullQueuelogs.txt]
TRANSFORMS-TCPGrpp= send_to_Group

transforms.conf
[send_to_nullqueue]
REGEX = Code\=F
DEST_KEY = _TCP_ROUTING
FORMAT = indexer ---> Outputs.conf tcpgroup

To send code=f to a specific index
[source::/opt/monitorlogs/indexlogs.txt]
TRANSFORMS-index = send_to_index

transforms.conf
[send_to_index]
REGEX = Code\=F
DEST_KEY = _MetaData:Index
FORMAT = apple

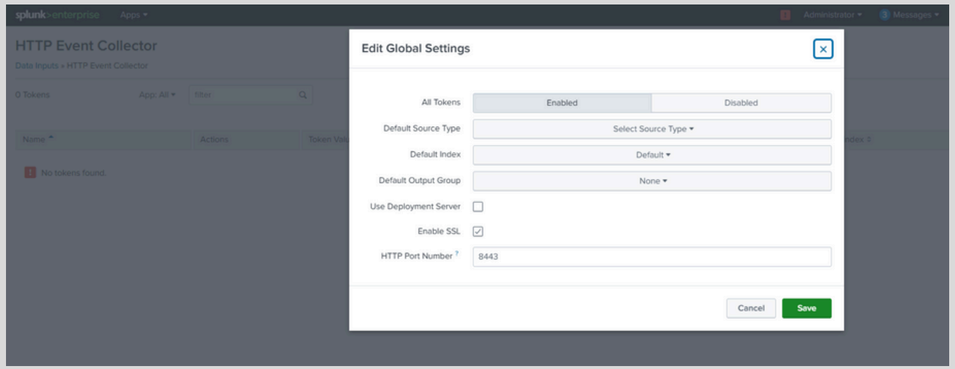
HEC

Go to WEb → Settings → Data(Data inputs) → HTTP Event Collector

Go to global settings → Enable it (you can change port as needed)

Generate a token

{"text":"Success","code":0}



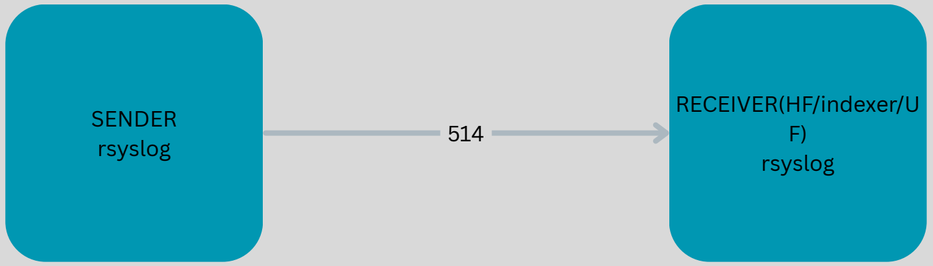

```
[root@ip-172-31-46-101 local]# cd /opt/splunk/etc/apps/search/local/
[root@ip-172-31-46-101 local]# ls
indexes.conf  inputs.conf
[root@ip-172-31-46-101 local]# cat in
cat: in: No such file or directory
[root@ip-172-31-46-101 local]# cat inputs.conf
[splunktcp://9997]
connection_host = ip

[http://apple_index]
disabled = 0
host = ip-172-31-46-101.ap-south-1.compute.internal
index = apple
indexes = apple
token = 2745dc24-e308-4f0d-8f0a-4f05914d6ba6
[root@ip-172-31-46-101 local]#
[root@ip-172-31-46-101 local]#
[root@ip-172-31-46-101 local]#
[root@ip-172-31-46-101 local]#
[root@ip-172-31-46-101 local]#
[root@ip-172-31-46-101 local]#
[root@ip-172-31-46-101 local]#
```

Todays topic (Aug 7th)

where does GUID is saved – instance.cfg, server.conf
masking data
HEC - acknowledgement
rsyslog data

```
[root@ip-172-31-42-5 ~]# cd /opt/splunkforwarder/etc/
[root@ip-172-31-42-5 etc]# ls
apps           deployment-apps  licenses              lo
auth           disabled-apps    log-btool-debug.cfg   lo
copyright.txt  init.d           log-btool.cfg         lo
datetime.xml   instance.cfg     log-cmdline-debug.cfg lo
[root@ip-172-31-42-5 etc]# cat instance.cfg
[general]
guid = CFBEEB03-A182-490C-9D10-8770D7DB615B
[root@ip-172-31-42-5 etc]#
[root@ip-172-31-42-5 etc]#
[root@ip-172-31-42-5 etc]# pwd
/opt/splunkforwarder/etc
[root@ip-172-31-42-5 etc]#
[root@ip-172-31-42-5 etc]#
[root@ip-172-31-42-5 etc]#
[root@ip-172-31-42-5 etc]#
```



Installation:(install rsyslog on both servers sender & receiver)
yum install rsyslog -y

Sender side:
vi /etc/rsyslog.conf
. @@<SYSLOG_LISTENER_IP>:514

Listener Side:
uncomment 31,32 OR 36,37 lines
vi /etc/rsyslog.conf

```
29 # Provides UDP syslog reception
30 # for parameters see http://www.rsyslog.com/doc/imudp.html
31 #module(load="imudp") # needs to be done just once
32 #input(type="imudp" port="514")
33
34 # Provides TCP syslog reception
35 # for parameters see http://www.rsyslog.com/doc/imtcp.html
36 module(load="imtcp") # needs to be done just once
37 input(type="imtcp" port="514")
```

Add below lines
vi /etc/rsyslog.d/splunk.conf

```
$template SplunkFile, "/opt/testfile.log"
*.* ?SplunkFile
```

if $msg contains 'error' then /opt/error.log

commands:
service rsyslog start
service rsyslog stop
service rsyslog restart

props.conf

[<SOURCETYPE>]

[**source**::<SOURCE>]

[**host**::<HOST>]

How to mask the sensitive info
on indexer/hf

props.conf
[access_log]
SEDCMD-maskCreditcard = s/(\d{12,16})/XXXXXXXXXX/g

props.conf

[access_transforms]
TRANSFORMS-maskdata = maskcarddata

transforms.conf
[maskcarddata]
REGEX = (\d{12,16})
FORMAT = $1::XXXXXXXXX
DEST_KEY = _raw

HEC ACK:
https://help.splunk.com/en/splunk-enterprise/get-started/get-data-in/9.3/get-data-with-http-event-collector/use-curl-to-manage-http-event-collector-tokens-events-and-services

```
curl --location 'https://43.205.111.108:8443/services/collector/raw?channel=00872DC6-AC83-4EDE-8AFE-8413C3825C21&sourcetype=mydata' \
--header 'Authorization: Splunk f26f5849-00c1-41b8-923b-65e46b1622f5' \
--header 'Content-Type: application/json' \
--data '"hello World"'
```

```
curl --location 'https://43.205.111.108:8443/services/collector/ack?channel=00872DC6-AC83-4EDE-8AFE-8413C3825C4C' \
--header 'Authorization: Splunk f26f5849-00c1-41b8-923b-65e46b1622f5' \
--header 'Content-Type: application/json' \
--data '{"acks": [1,3,4]}'
```