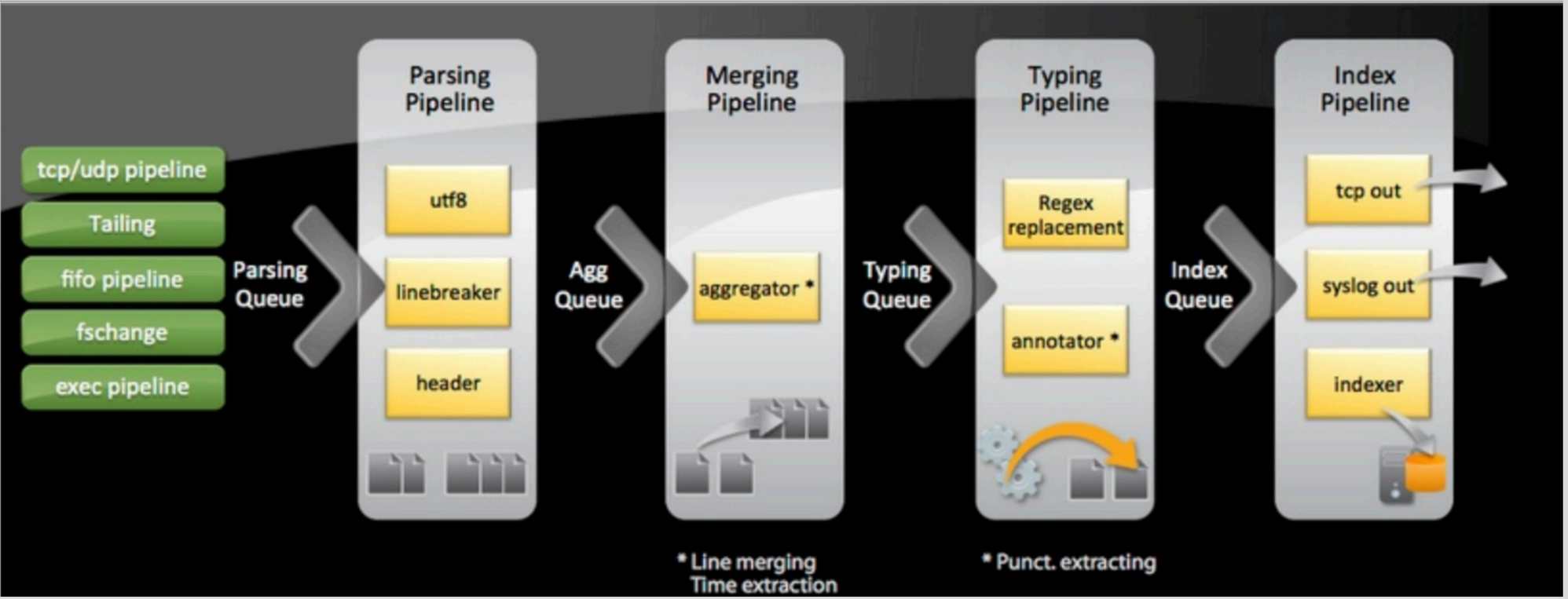

tcp/udp pipeline
Tailing
fifo pipeline
fschange
exec pipeline
Parsing Queue
Parsing Pipeline
utf8
linebreaker
header
Agg Queue
Merging Pipeline
aggregator *
* Line merging
Time extraction
Typing Queue
Typing Pipeline
Regex replacement
annotator *
* Punct. extracting
Index Queue
Index Pipeline
tcp out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

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]#

```
[root@ip-172-31-32-132 monitor]#
[root@ip-172-31-32-132 monitor]# pwd
/opt/monitor
[root@ip-172-31-32-132 monitor]# ls
file1.txt  file2.txt  transform.txt
[root@ip-172-31-32-132 monitor]#
[root@ip-172-31-32-132 monitor]# cat /opt/splunkforwarder/etc/system/local/inputs.con
[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

[monitor:///opt/monitor/transform.txt]
host=uf
index=main
sourcetype=transform_rule
_TCP_ROUTING = indexer
[root@ip-172-31-32-132 monitor]#
[root@ip-172-31-32-132 monitor]#
[root@ip-172-31-32-132 monitor]#
```

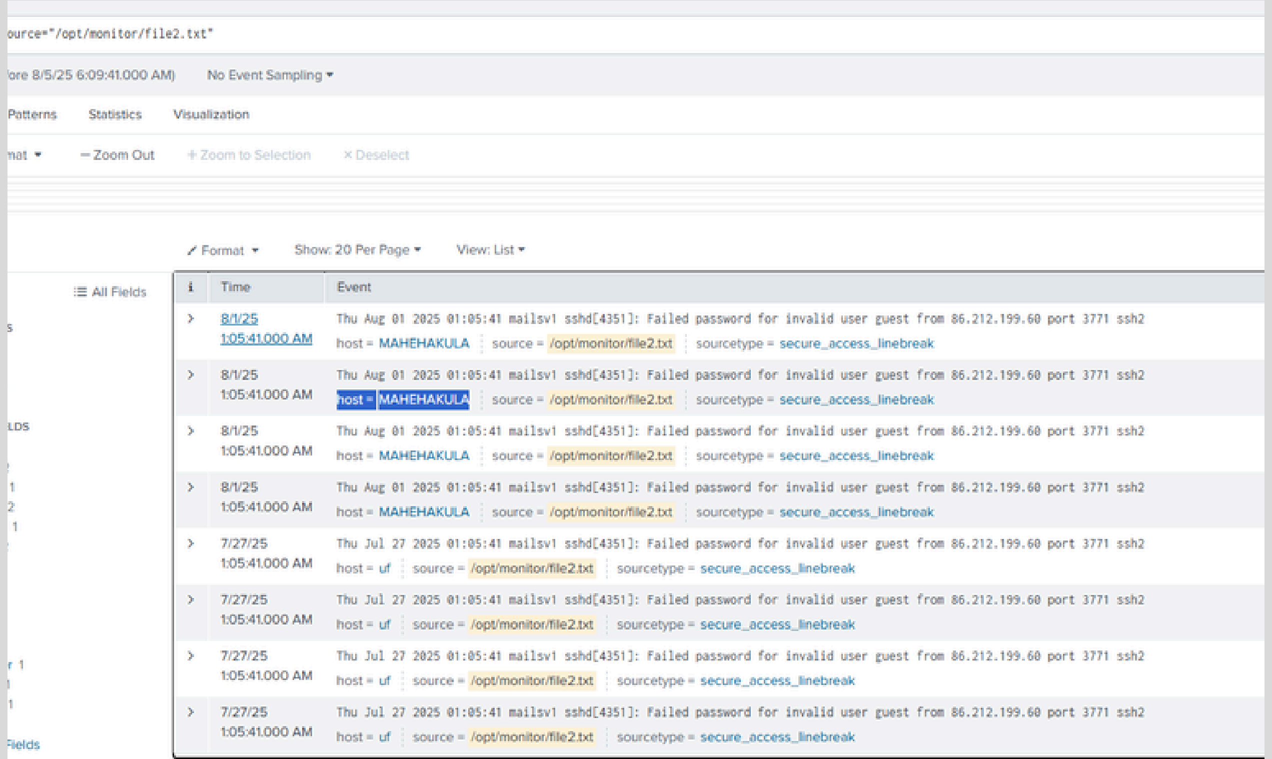
Props.conf

[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

```
[root@ip-172-31-38-148 local]#
[root@ip-172-31-38-148 local]# cat props.conf
[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

[transform_rule]
TRANSFORMS-rule1=renamehost


[root@ip-172-31-38-148 local]#
[root@ip-172-31-38-148 local]# cat transforms.conf
[renamehost]
DEST_KEY = MetaData:Host
REGEX = .*
FORMAT = host::MAHEHAKULA
[root@ip-172-31-38-148 local]#
[root@ip-172-31-38-148 local]# pwd
/opt/splunk/etc/apps/search/local
[root@ip-172-31-38-148 local]#
```

- 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-applttoall = 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

- * NOTE: Keys are case-sensitive. Use the following keys exactly as they
- appear.
-
- queue : Specify which queue to send the event to (can be nullQueue, indexQueue).
- * indexQueue is the usual destination for events going through the
- transform-handling processor.
- * nullQueue is a destination which causes the events to be
- dropped entirely.
- _raw : The raw text of the event.
- _meta : A space-separated list of metadata for an event.
- _time : The timestamp of the event, in seconds since 1/1/1970 UTC.
-
- MetaData:Host : The host associated with the event.
- The value must be prefixed by "host::"
-
- _MetaData:Index : The index where the event should be stored.
-
- MetaData:Source : The source associated with the event.
- The value must be prefixed by "source::"
-
- MetaData:Sourcetype : The source type of the event.
- The value must be prefixed by "sourcetype::"
-
- _TCP_ROUTING : Comma separated list of tcpout group names (from
- outputs.conf)
- Defaults to groups present in 'defaultGroup' for [tcpout].
-
- _SYSLOG_ROUTING : Comma separated list of syslog-stanza names (from
- outputs.conf)
- Defaults to groups present in 'defaultGroup' for [syslog].
-
- * NOTE: Any KEY (field name) prefixed by '_' is not indexed by Splunk software, in general.
-

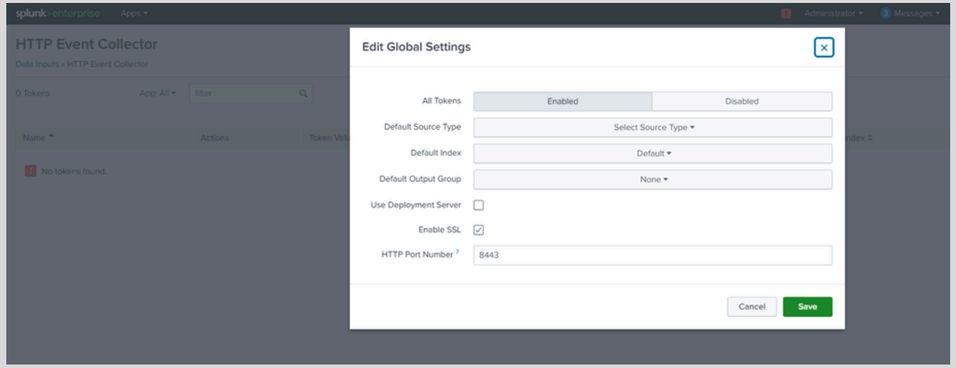
HEC

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]#
```

- masking data
- HEC - acknowledgement

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 be3cc297-83bf-4554-9280-5ef8fb98fddb' \
--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]}'

FILE PRECEDENCE

https://dev.splunk.com/enterprise/docs/developapps/manageknowledge/fileprecedence/

/opt/splunk/{etc,bin,auth}/

filename.conf – configuration file
[stanza] →
attribute1 = value1
attribute2 = value2
host = google1.com → example

File precedence

/opt/splunk/etc/system/local → 1st
filename.conf – configuration file
[stanza] →
attribute1 = value1
attribute2 = value2
host = google1.com

/opt/splunk./etc/apps/ta_nix/local/ → → 3rd
filename.conf – configuration file
[stanza] →
attribute1 = value1
attribute2 = raghu
host = test.com
source = abc_access.log

/opt/splunk./etc/apps/ta_nix/default/→ 5th
filename.conf – configuration file
[stanza] →
attribute1 = mahesh
attribute2 = value2
host = test.com
source = xyz.log

/opt/splunk./etc/apps/00_nix/local/ → 2nd
filename.conf – configuration file
[stanza] →
attribute1 = value1
attribute2 = raghu
host = test.com

/opt/splunk./etc/apps/00_nix/default/→ 4th
filename.conf – configuration file
[stanza] →
attribute1 = mahesh
attribute2 = value2
host = test.com
source = xyz222.log

/opt/splunk/etc/system/default→ LAST – DO NOT EDIT
filename.conf – configuration file
[stanza] →
attribute1 = value1
attribute2 = value2
host = google1.com