SPLUNK DAY 2

UF to INDEXER

Prerequisites:

- UF
 - Install Splunk UF package (untar & start splunk process)
 - check connectivity to indexer on port 9997
- Indexer
 - o 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 -anplgrep: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.

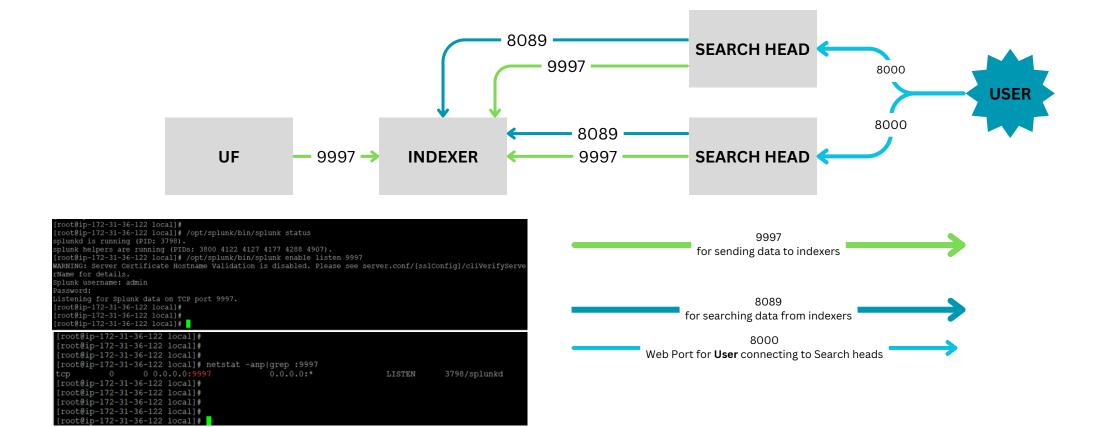
vi /opt/splunkforwarder/etc/system/local/inputs.conf

[monitor:///opt/splunkforwarder/testfile.log]

index = main

sourcetype=test_access

#_TCP_ROUTING = splunksession → if you want to send data to specific group.



```
[root@ip-172-31-34-118 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]#
```

```
[root8ip-1/2-3i-34-1i8 local]#
[root8ip-172-3i-34-1i8 local]#
[root8ip-172-3i-34-1i8 local]# vi /opt/splunkforwarder/etc/system/local/outputs.conf
[root8ip-172-3i-34-1i8 local]# vi /opt/splunkforwarder/etc/system/local/inputs.conf
[root8ip-172-3i-34-1i8 local]# vi /opt/splunkforwarder/etc/system/local/inputs.conf
[root8ip-172-3i-34-1i8 local]# [root8ip-172-3i-34-1i8 splunkforwarder]# [root8ip-172-3i-34-1i8 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

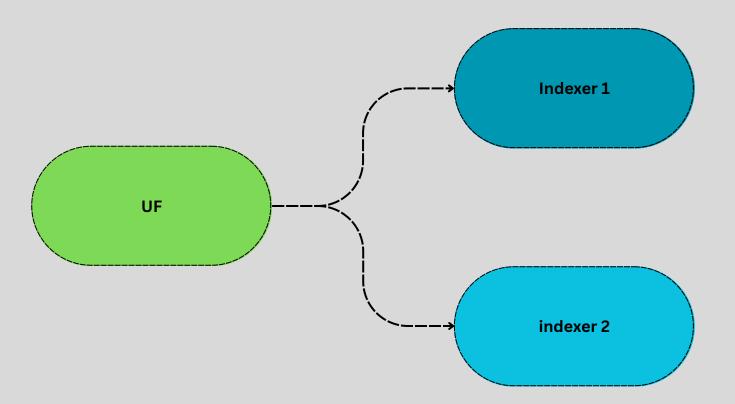
[root@ip-172-31-46-249 local]# ^C

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

[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
rovbuf = 1572864
connection_host = ip
disabled = 0
dost = $decideOnStartup
dost = 1572864
dost = 152886
dost
```

```
[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/splunkenterprise/administer/adminmanual/9.4/configuration-file-reference/9.4.4configuration-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

host=uf index=main sourcetype=secure_access_linebreak _TCP_ROUTING = indexer

[monitor:///opt/monitor/file2.txt]

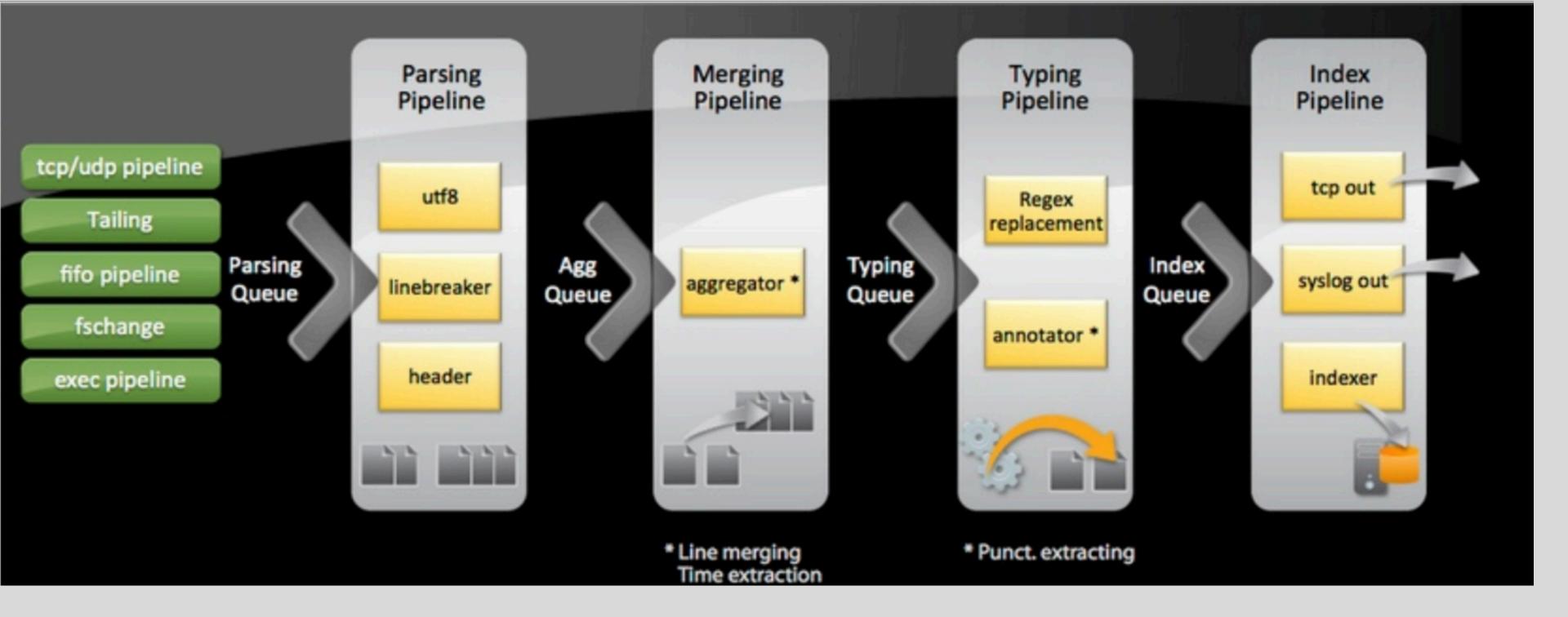
################################## [root@ip-172-31-32-132 local]# cat outputs.conf [tcpout:indexer] server = 15.206.159.98:9997 [root@ip-172-31-32-132 local]#

Props.conf transforms.conf

```
[secure_access]
                                                                            [renamehost]
SHOULD_LINEMERGE=false
                                                                            DEST_KEY = MetaData:Host
LINE_BREAKER=([\r\n]+)
                                                                            REGEX = .*
BREAK_ONLY_BEFORE_DATE=null
                                                                            FORMAT = host::UniversalForwarder
NO_BINARY_CHECK=true
                                                                            ##Renaming host name during parsing stage
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>
```

ot@ip-172-31-38-148 local]# ot@ip-172-31-38-148 local]# cat props.conf ecure_access] EAK ONLY BEFORE DATE = NE_BREAKER = ([\r\n]+)
X TIMESTAMP LOOKAHEAD = 50 OULD_LINEMERGE = false ME_FORMAT = %a %b %d %Y %H:%M:%S egory = Custom cription = this is for tutorial ldown type = true ecure_access_linebreak] EAK_ONLY_BEFORE_DATE = TETIME_CONFIG = NE_BREAKER = ([\r\n]+)?(?=\w{3}\s\w{3}\s\d{2}) BINARY CHECK = true JLD_LINEMERGE = false egory = Custom ransform rule] oot@ip-172-31-38-148 local]#
oot@ip-172-31-38-148 local]# cat transforms.conf KEY = MetaData:Host RMAT = host::MAHEHAKULA ot@ip-172-31-38-148 local]# ot@ip-172-31-38-148 local]# pwd /splunk/etc/apps/search/loca t@ip-172-31-38-148 local]#

```
ource="/opt/monitor/file2.txt"
ore 8/5/25 6:09:41.000 AM) No Event Sampling *
Patterns Statistics Visualization
        - Zoom Out + Zoom to Selection × Deselect
                       ✓ Format ▼ Show: 20 Per Page ▼ View: List ▼
                       i Time
        :≡ All Fields
                                           Thu Aug 01 2025 01:05:41 mailsv1 sshd[4351]: Failed password for invalid user guest from 86.212.199.60 port 3771 ssh2
                            1:05:41.000 AM host = MAHEHAKULA source = /opt/monitor/file2.txt sourcetype = secure_access_linebreak
                           8/U25 Thu Aug 01 2025 01:05:41 mailsv1 sshd[4351]: Failed password for invalid user guest from 86.212.199.60 port 3771 ssh2
                            1:05:41.000 AM host = MAHEHAKULA source = /opt/monitor/file2.txt sourcetype = secure_access_linebreak
                                           Thu Aug 01 2025 01:05:41 mailsv1 sshd[4351]: Failed password for invalid user guest from 86.212.199.60 port 3771 ssh2
                           1:05:41.000 AM host = MAHEHAKULA source = /opt/monitor/file2.txt sourcetype = secure_access_linebreak
                            8/V25 Thu Aug 01 2025 01:05:41 mailsv1 sshd[4351]: Failed password for invalid user guest from 86.212.199.60 port 3771 ssh2
                            1:05:41.000 AM host = MAHEHAKULA source = /opt/monitor/file2.txt sourcetype = secure_access_linebreak
                                          Thu Jul 27 2025 01:05:41 mailsv1 sshd[4351]: Failed password for invalid user guest from 86.212.199.60 port 3771 ssh2
                            1:05:41.000 AM host = uf source = /opt/monitor/file2.txt sourcetype = secure_access_linebreak
                          7/27/25 Thu Jul 27 2025 01:05:41 mailsv1 sshd[4351]: Failed password for invalid user guest from 86.212.199.60 port 3771 ssh2
                           1:05:41.000 AM host = uf | source = /opt/monitor/file2.txt | sourcetype = secure_access_linebreak
                                         Thu Jul 27 2025 01:05:41 mailsv1 sshd[4351]: Failed password for invalid user guest from 86.212.199.60 port 3771 ssh2
                            1:05:41.000 AM host = uf | source = /opt/monitor/file2.txt | sourcetype = secure_access_linebreak
                          7/27/25 Thu Jul 27 2025 01:05:41 mailsv1 sshd[4351]: Failed password for invalid user guest from 86.212.199.60 port 3771 ssh2
                           1:05:41.000 AM host = uf | source = /opt/monitor/file2.txt | sourcetype = secure_access_linebreak
```



- How data is processed in Splunk?
- Stages Pipelines & Queues
- How to add metadata Fields for all events in splunk?

Todays Topics

- . How to send redundant data to NullOueue?
- How to send data to a specific topout group/indexergroup?
- HTTP event Collector -
- o Token Generation
- Port configuration o 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-variablesand-modifiers/date-and-time-format-variables

https://help.splunk.com/en/splunk-enterprise/get-started/get-data-in/9.3/get-data-with-http-eventcollector/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?

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 to a specific tcp group when ever there is an event with (Code=F)

TRANSFORMS-TCPGrpp= send_to_Group

DEST_KEY = _TCP_ROUTING

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

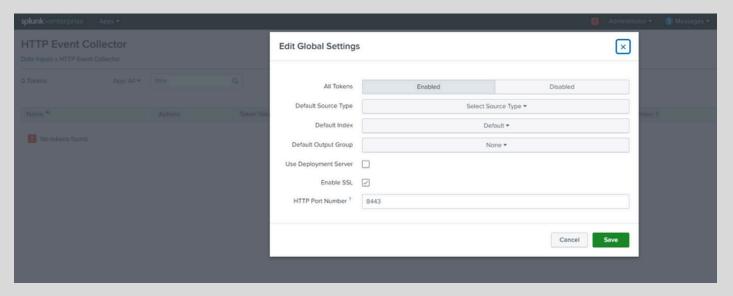
HEC

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]
 onnection 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]#
```