

## 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 -an|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

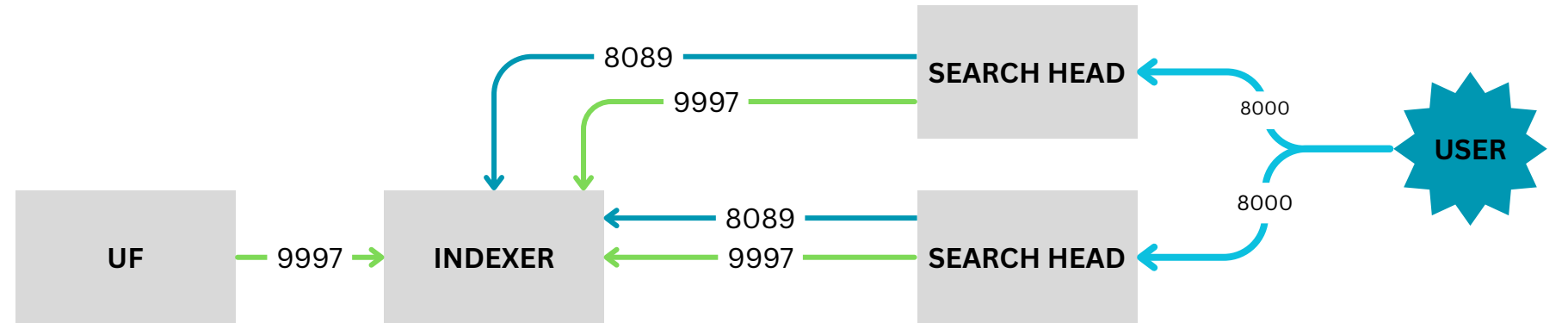
[tcpout]

defaultGroup = splunksession

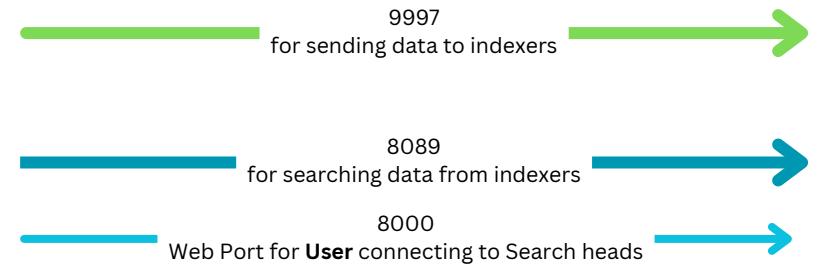
[tcpout:splunksession]

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]# netstat -an|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-172-31-36-122 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]# vi /opt/splunkforwarder/etc/system/local/inputs.conf
[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]# 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 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

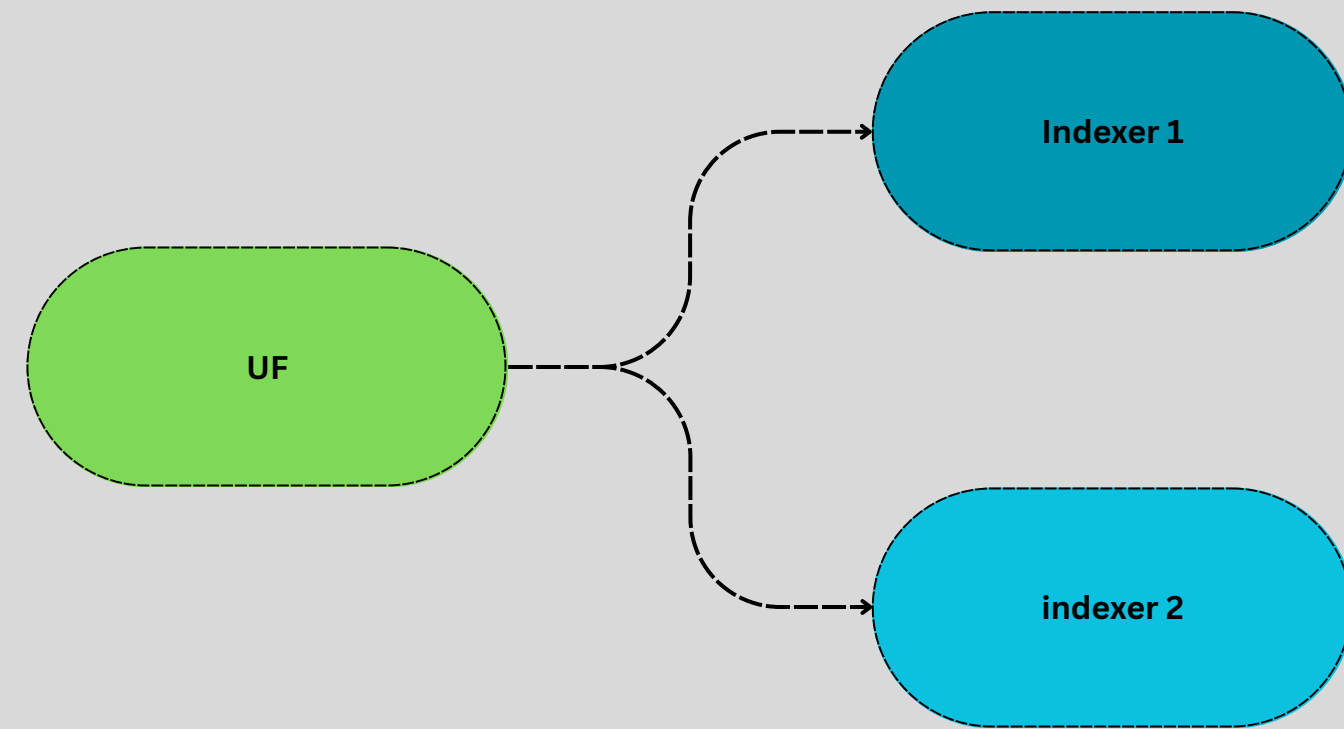
[root@ip-172-31-46-249 local]# /opt/splunk/bin/splunk btool inputs list **splunktcp** --debug

[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.

Today's 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]#
```

```
[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.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

[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

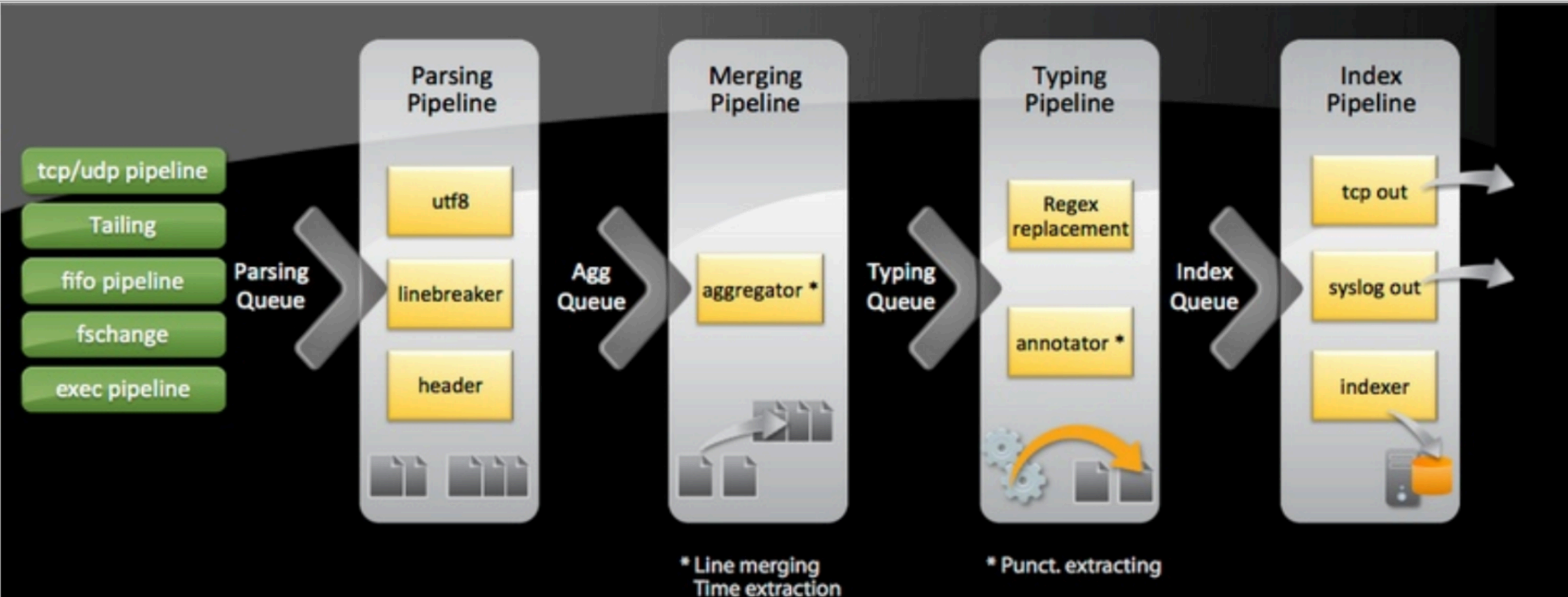
[secure_access_linebreak]
BREAK_ONLY_BEFORE_DATE =
DATETIME_CONFIG =
LINE_BREAKER = ([\\r\\n]+)?(?:\\w{3}\\s\\w{3}\\s\\d{2})
NO_BINARY_CHECK = true
SHOULD_LINEMERGE = false
category = Custom
pulldown_type = true
TRANSFORMS-rule1=renamehost

[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]#
```

source="/opt/monitor/file2.txt"	
ore 8/5/25 6:09:41.000 AM] No Event Sampling	
Patterns	Statistics Visualization
nat	Zoom Out Zoom to Selection Deselect
Format Show: 20 Per Page View: List	
All Fields	Time Event
	8/1/25 10:05:41.000 AM Thu Aug 01 2025 01:05:41 mailsv1 sshd[4351]: Failed password for invalid user guest from 86.212.199.60 port 3771 ssh2
	host = MAHEHAKULA source = /opt/monitor/file2.txt sourcetype = secure_access_linebreak
	8/1/25 1:05:41.000 AM Thu Aug 01 2025 01:05:41 mailsv1 sshd[4351]: Failed password for invalid user guest from 86.212.199.60 port 3771 ssh2
	host = MAHEHAKULA source = /opt/monitor/file2.txt sourcetype = secure_access_linebreak
	8/1/25 1:05:41.000 AM Thu Aug 01 2025 01:05:41 mailsv1 sshd[4351]: Failed password for invalid user guest from 86.212.199.60 port 3771 ssh2
	host = MAHEHAKULA source = /opt/monitor/file2.txt sourcetype = secure_access_linebreak
	8/1/25 1:05:41.000 AM Thu Aug 01 2025 01:05:41 mailsv1 sshd[4351]: Failed password for invalid user guest from 86.212.199.60 port 3771 ssh2
	host = MAHEHAKULA source = /opt/monitor/file2.txt sourcetype = secure_access_linebreak
	7/27/25 1:05:41.000 AM Thu Jul 27 2025 01:05:41 mailsv1 sshd[4351]: Failed password for invalid user guest from 86.212.199.60 port 3771 ssh2
	host = uf source = /opt/monitor/file2.txt sourcetype = secure_access_linebreak
	7/27/25 1:05:41.000 AM Thu Jul 27 2025 01:05:41 mailsv1 sshd[4351]: Failed password for invalid user guest from 86.212.199.60 port 3771 ssh2
	host = uf source = /opt/monitor/file2.txt sourcetype = secure_access_linebreak
	7/27/25 1:05:41.000 AM Thu Jul 27 2025 01:05:41 mailsv1 sshd[4351]: Failed password for invalid user guest from 86.212.199.60 port 3771 ssh2
	host = uf source = /opt/monitor/file2.txt sourcetype = secure_access_linebreak
	7/27/25 1:05:41.000 AM Thu Jul 27 2025 01:05:41 mailsv1 sshd[4351]: Failed password for invalid user guest from 86.212.199.60 port 3771 ssh2
	host = uf source = /opt/monitor/file2.txt sourcetype = secure_access_linebreak







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

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
```

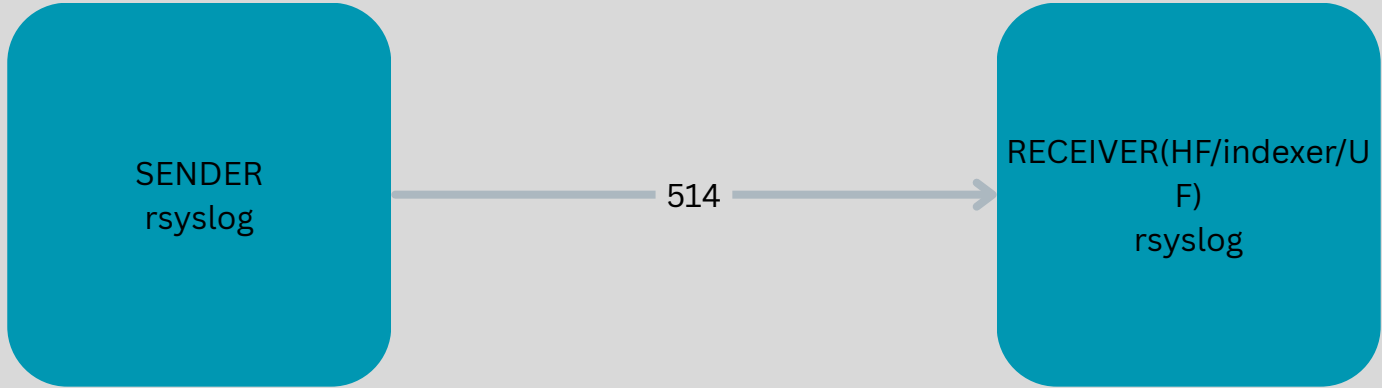
```
transforms.conf
[maskcarddata]
REGEX = (\\d{12,16})
FORMAT = $1::XXXXXXXXXX
DEST_KEY = _raw
```

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]}'
```

```
[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

what is app and addon.

Splunk DB connect

Regex

<https://splunkbase.splunk.com/app/2686>

<https://docs.splunk.com/Documentation/DBX/3.8.0/DeployDBX/AboutSplunkDBConnect>

<https://docs.splunk.com/Documentation/DBX/3.8.0/DeployDBX/Installdatabasedrivers>

addons (inputs and setup config) and Apps (KOs)

Addons types

TA - Technology Addon

SA - Supporting addon

DA - Domain Addon

#### Addon:

- Data collection
- (inputs/scripts...)
- Field extractions
- No UI (very minimal UI)
- No Dashboards, reports, alerts (KOs)
- on indexers, Hfs, Ufs
- SH only for field extractions

#### App:

- All KOs (Knowledge Objects)
- It has UI
- only on Search Head

Splunk DB connect:

Steps:

1. Download/install DB connect from splunk base on HF/indexer

Prerequisites:

- jre 17/21

1. Install Java 21 on splunk instance
2. Check java --version
3. Get the jre location
4. configure in splunk db connect app
5. install mysql addon (Splunk DBX Add-on for MySQL JDBC) MySQL





## Splunk Add-on for Unix and Linux | Splunkbase

\*\*\* Important: Read upgrade Instructions and test add-on update before deploying to production \*\*\*...

 splunk.com

Install splunk-add-on-for-unix-and-linux\_1010.tgz app on UF and Indexer

Create a local folder in /opt/splunkforwarder/etc/apps/Splunk\_TA\_nix

vi /opt/splunkforwarder/etc/apps/Splunk\_TA\_nix/local/inputs.conf

inputs.conf

[monitor:///var/log]  
disabled = false  
host=UF

[script:///bin/netstat.sh]  
disabled = false  
interval = 30  
host=UF

[script:///bin/cpu\_metric.sh]  
disabled = false  
index = os\_metrics  
#you have to create above index in indexer as metric type  
host=UF

```
[ec2-user@ip-172-31-47-134 ~]$ pwd
/home/ec2-user
[ec2-user@ip-172-31-47-134 ~]$ ls
splunk-add-on-for-unix-and-linux_1010.tgz
[ec2-user@ip-172-31-47-134 ~]$ sudo su -
[root@ip-172-31-47-134 ~]# /opt/splunkforwarder/bin/splunk status
splunkd is running (PID: 2463).
splunk helpers are running (PIDs: 2464).
[root@ip-172-31-47-134 ~]#
[root@ip-172-31-47-134 ~]#
[root@ip-172-31-47-134 ~]# /opt/splunkforwarder/bin/splunk stop
Stopping splunkd...
Shutting down. Please wait, as this may take a few minutes.
. [ OK ]
Stopping splunk helpers...
[ OK ]

Done.
[root@ip-172-31-47-134 ~]# ls
[root@ip-172-31-47-134 ~]# cd /home/ec2-user/
[root@ip-172-31-47-134 ec2-user]# ls
splunk-add-on-for-unix-and-linux_1010.tgz
[root@ip-172-31-47-134 ec2-user]# tar -xzf splunk-add-on-for-unix-and-linux_1010.tgz -C /opt/splunkforwarder/e
tc/apps/
[root@ip-172-31-47-134 ec2-user]# cd /opt/splunkforwarder/etc/apps/
[root@ip-172-31-47-134 apps]# ls
SplunkUniversalForwarder introspection_generator_addon search
Splunk_TA_nix journald_input splunk_httpinput
audit_trail learned splunk_internal_metrics
[root@ip-172-31-47-134 apps]# pwd
/opt/splunkforwarder/etc/apps
[root@ip-172-31-47-134 apps]# cd Splunk_TA_nix
[root@ip-172-31-47-134 Splunk_TA_nix]# ls
LICENSES README.txt VERSION appserver default metadata
README THIRDPARTY app.manifest bin lookups static
```