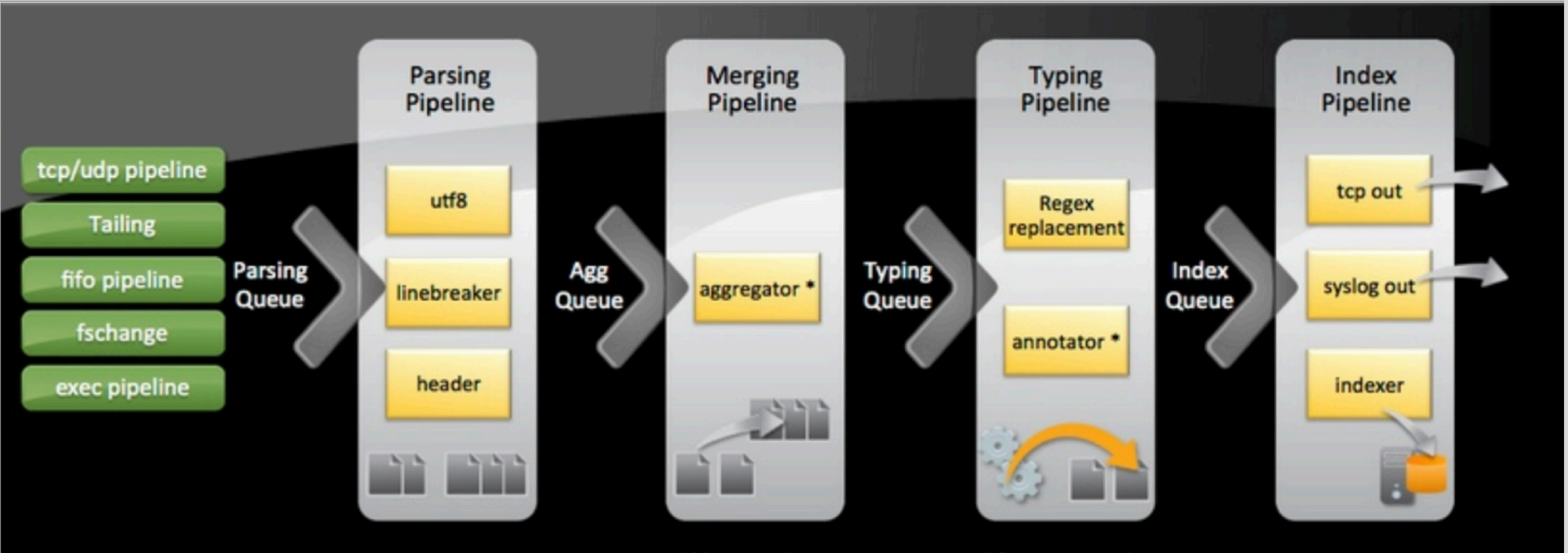


tcp/udp pipeline

Tailing

fifo pipeline

fschange

exec pipeline

Parsing Queue

Parsing Pipeline

utf8

linebreaker

header

Agg Queue

Merging Pipeline

aggregator *

Typing Queue

Typing Pipeline

Regex replacement

annotator *

Index Queue

Index Pipeline

tcp out

syslog out

indexer

* Line merging
Time extraction

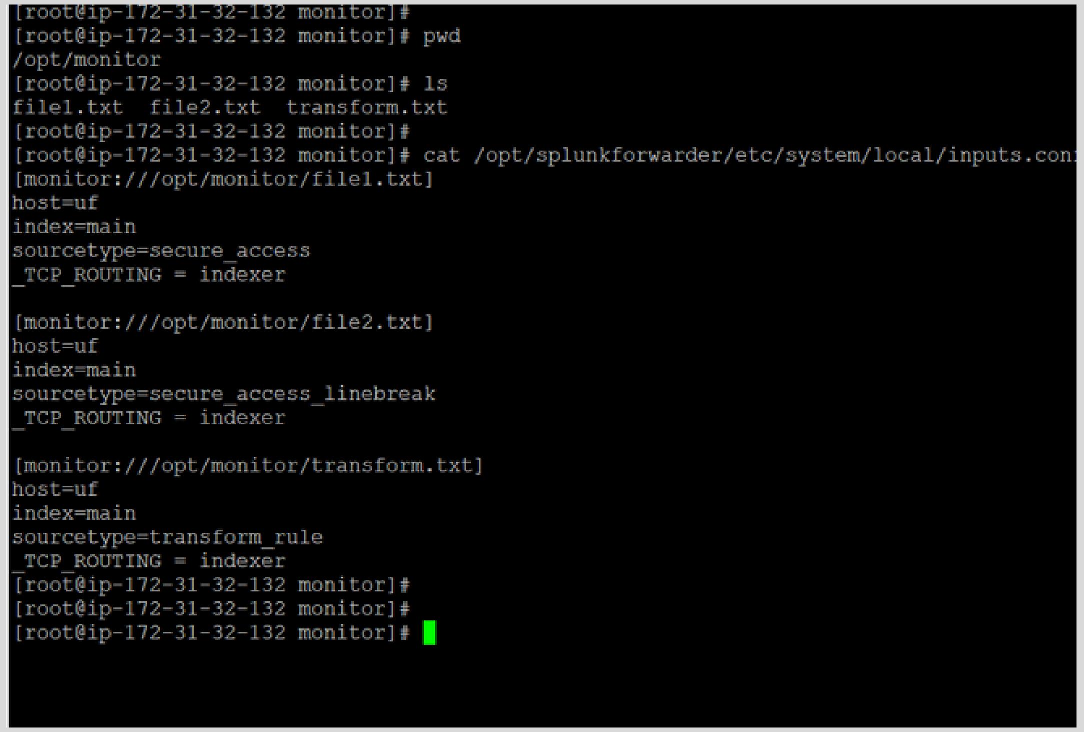
* Punct. extracting

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

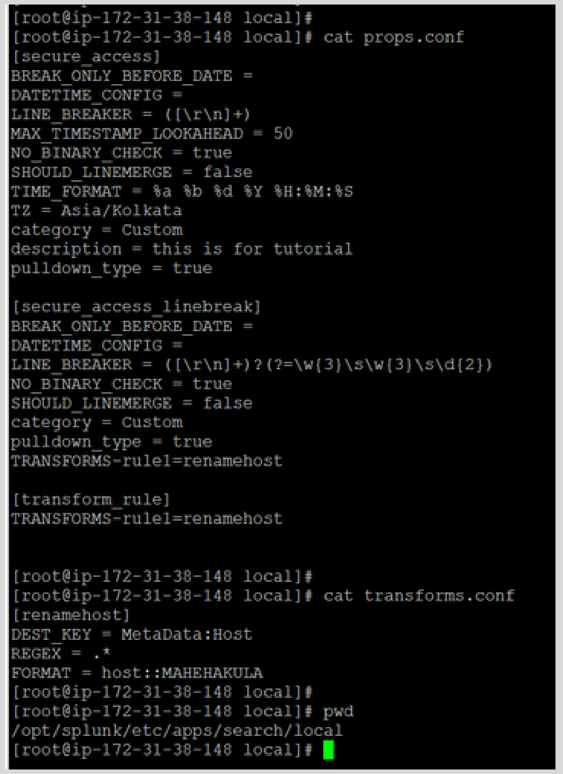
```
[ secure_access ]
SHOULD_LINEMERGE=false
LINE_BREAKER=([\r\n]+)
BREAK_ONLY_BEFORE_DATE=null
NO_BINARY_CHECK=true
CHARSET=UTF-8
MAX_TIMESTAMP_LOOKAHEAD=50
TIME_FORMAT=%a %b %d %Y %H:%M:%S
TIME_PREFIX=^
TZ=Asia/Kolkata
description=this is for tutorial
```

```
[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
```

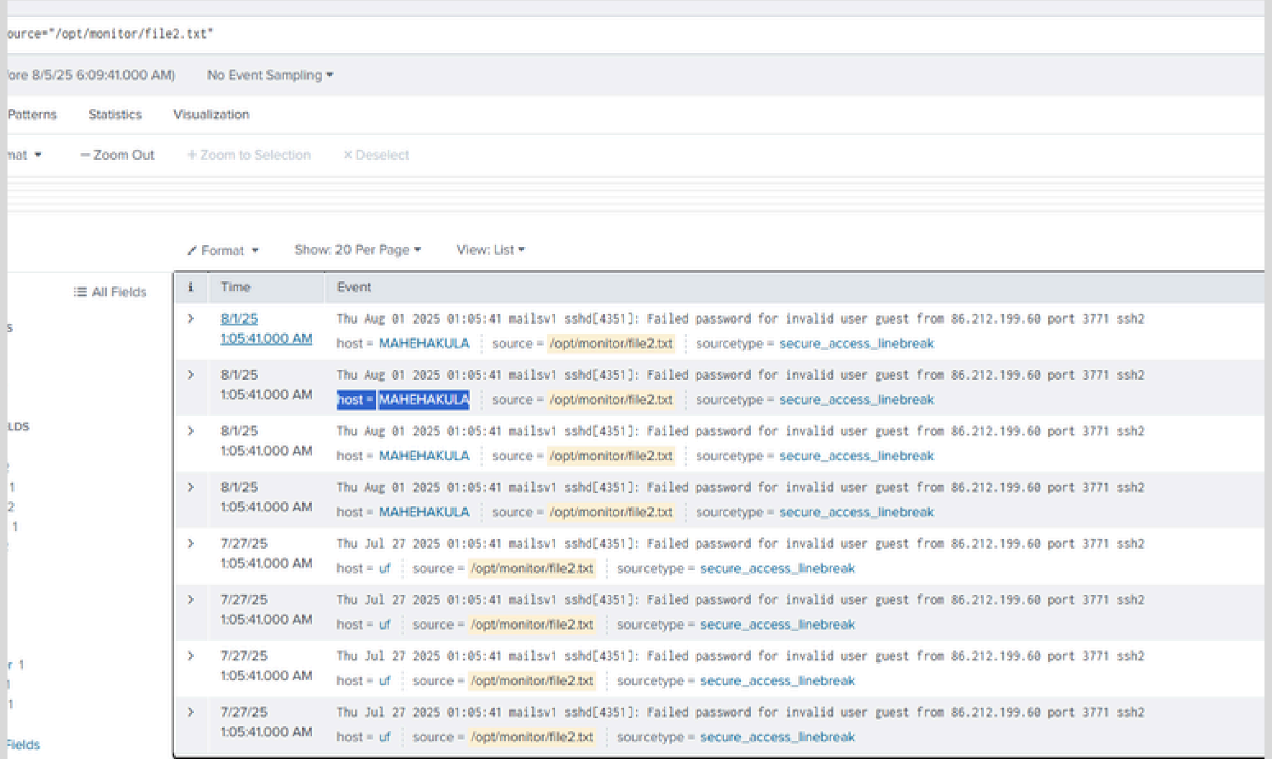
TRANSFORMS-<class> = <transform_stanza_name>, <transform_stanza_name2>

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]#
```



i	Time	Event
>	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
>	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

- 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-appltoall = 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
```

transforms.conf | Splunk Enterprise (last updated 2025-07-04T13:09:40.897Z)

The following are the spec and example files for transforms.conf.

splunk.com

```
• * 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.
•
```

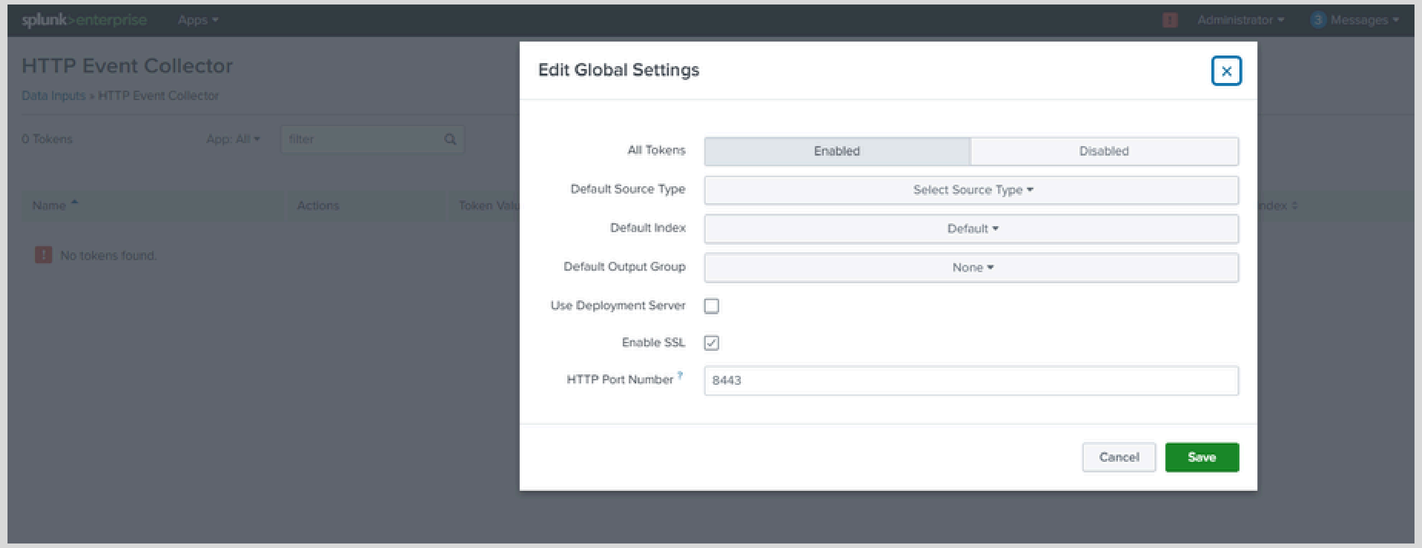
HEC

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

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

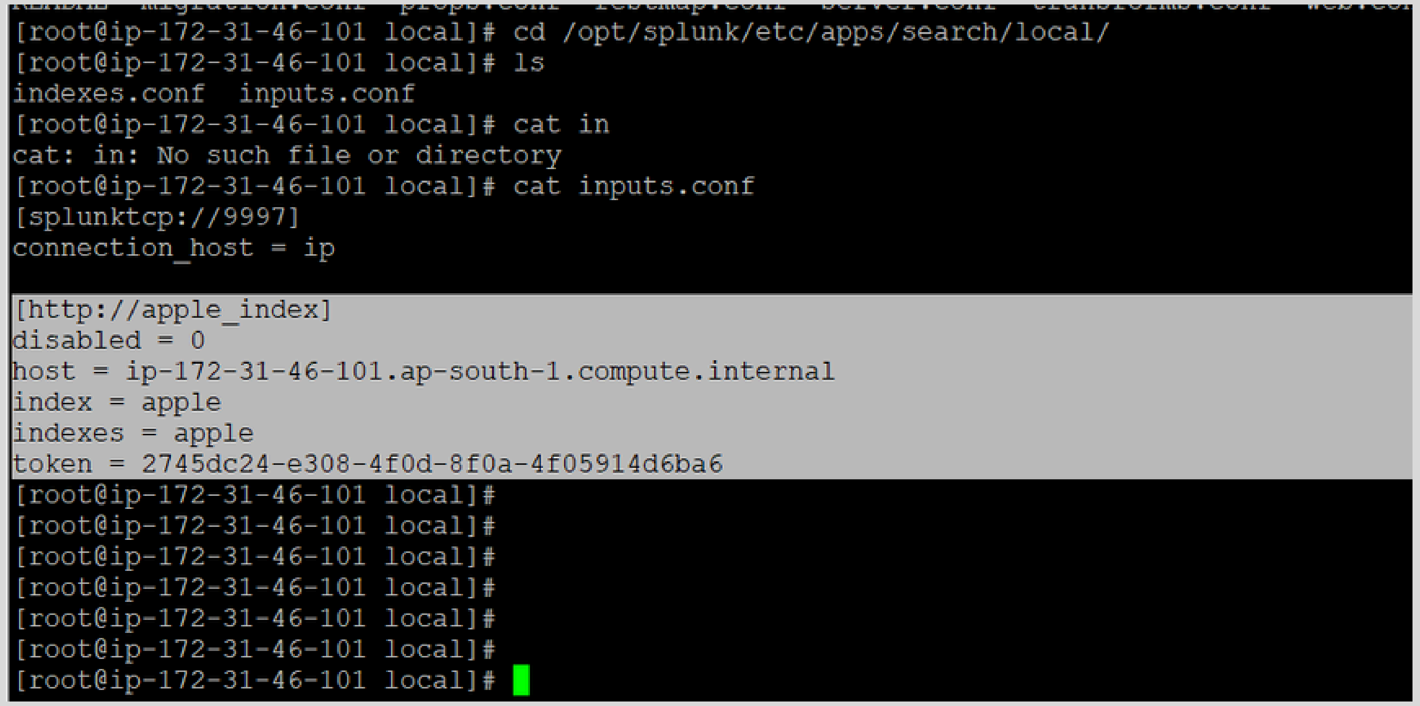
Generate a token

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



Edit Global Settings

All Tokens	Enabled / Disabled
Default Source Type	Select Source Type ▾
Default Index	Default ▾
Default Output Group	None ▾
Use Deployment Server	□
Enable SSL	☑
HTTP Port Number ?	8443



```
README  migration.conf  props.conf  restmap.conf  server.conf  transforms.conf  web.con
[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]}'
```

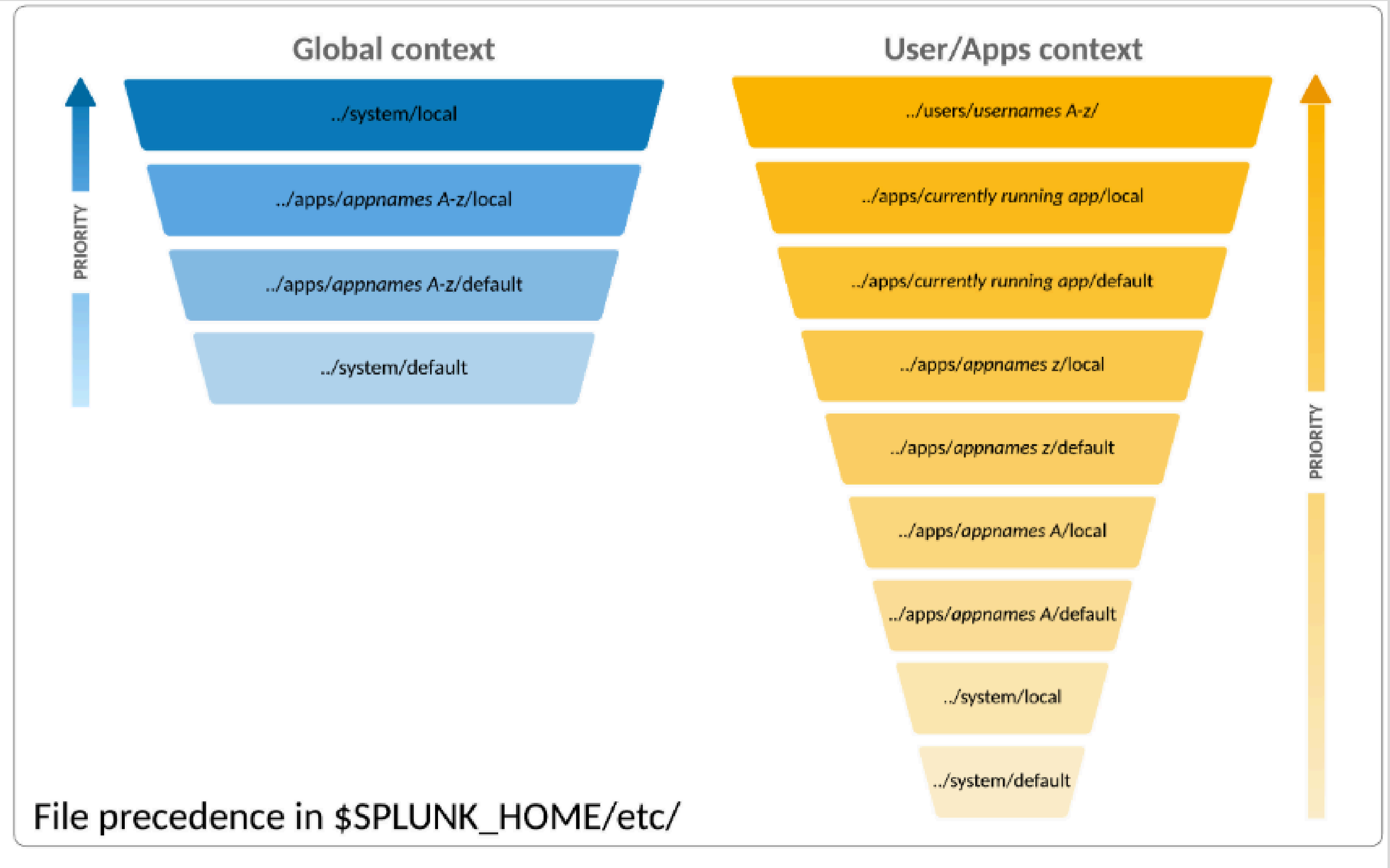
FILE PRECEDENCE

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


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

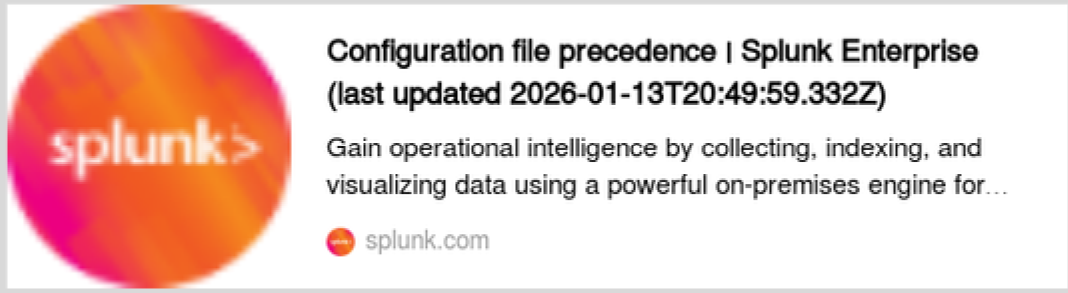
File precedence

```
/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
```

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



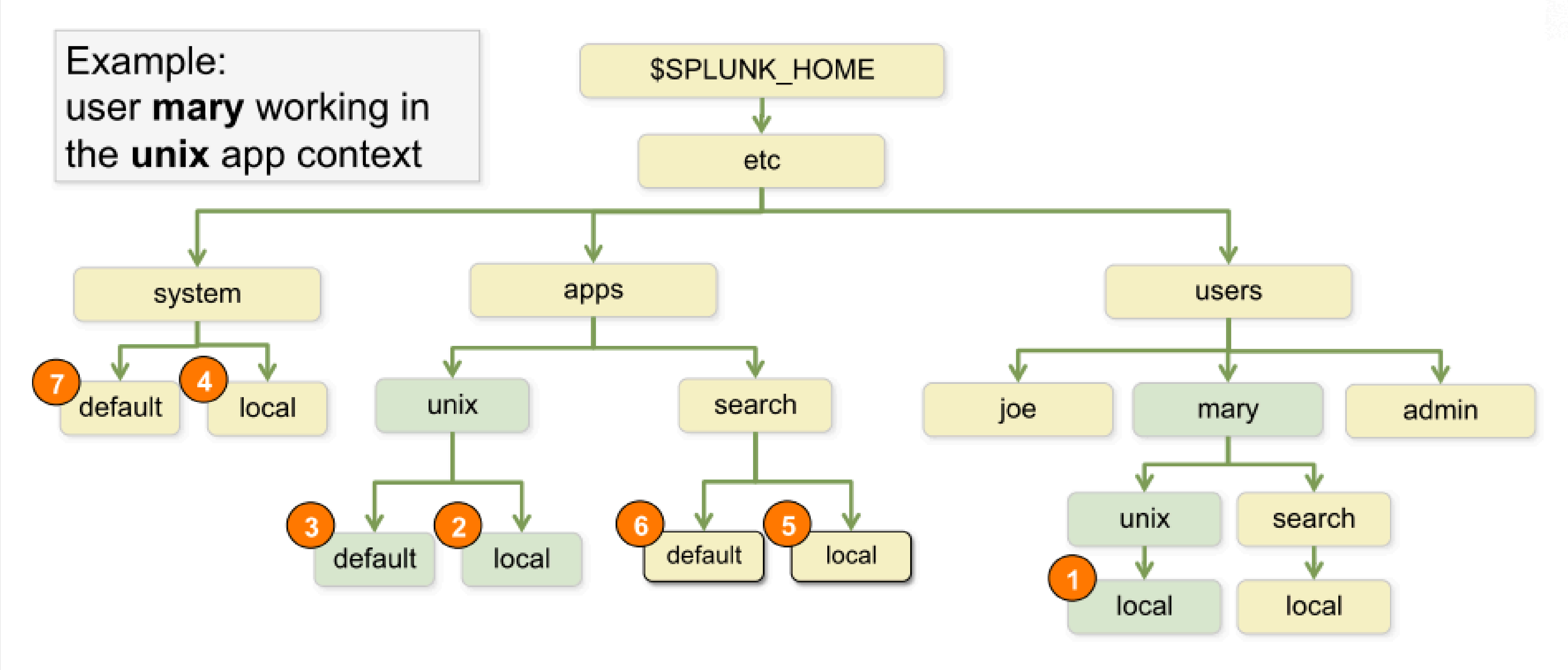
File precedence in $SPLUNK_HOME/etc/



Configuration file precedence | Splunk Enterprise (last updated 2026-01-13T20:49:59.332Z)

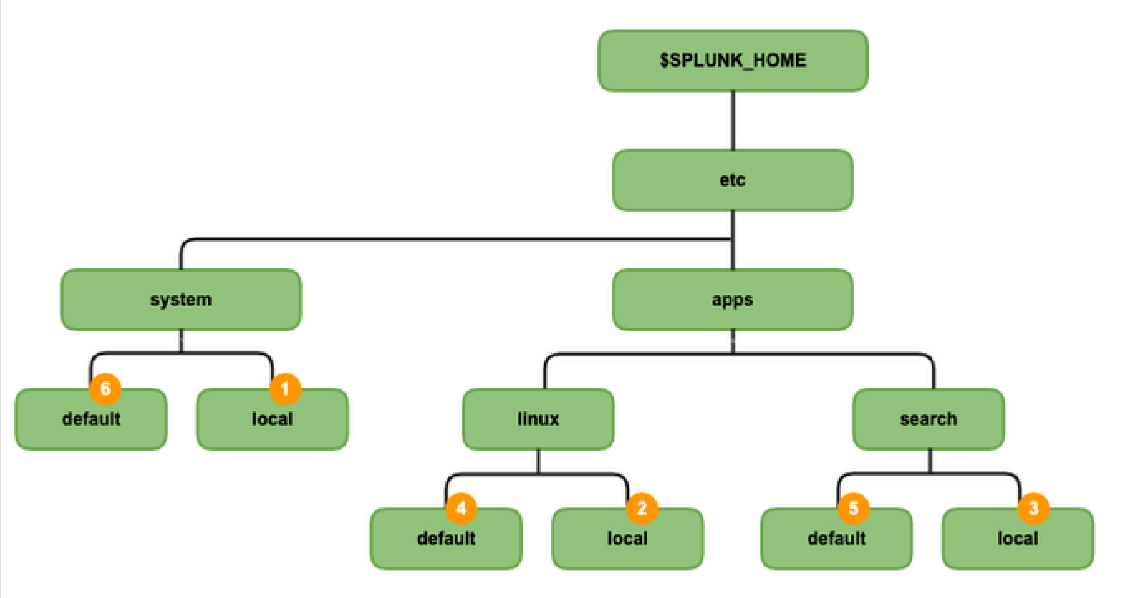
Gain operational intelligence by collecting, indexing, and visualizing data using a powerful on-premises engine for…

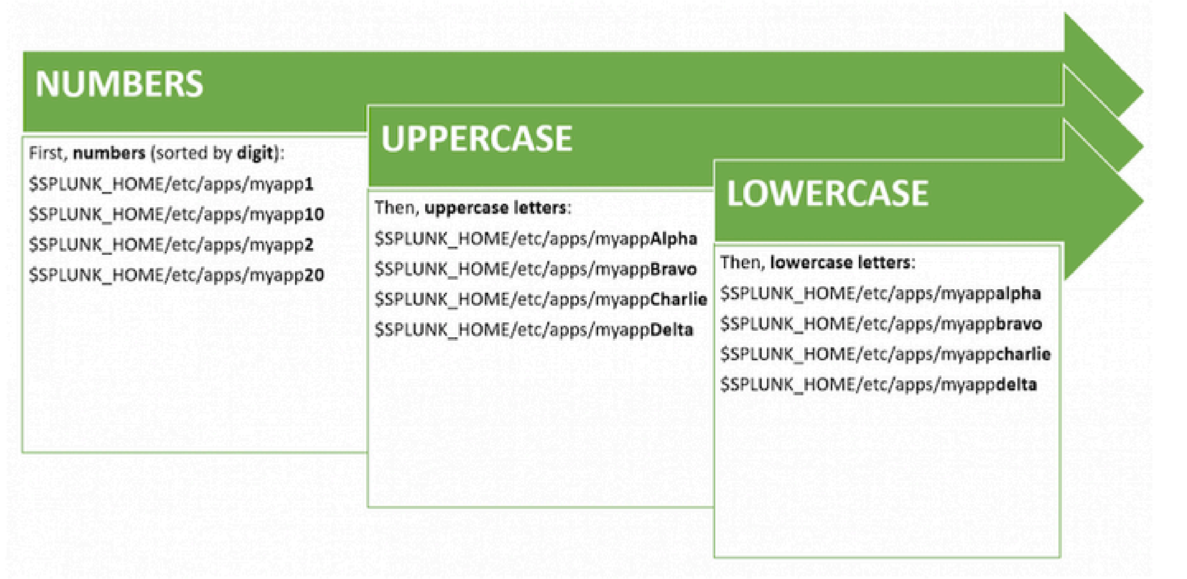
splunk.com



Example:
user **mary** working in the **unix** app context

https://www.alasta.com/splunk/2019/11/09/splunk-precedence.html





NUMBERS

First, **numbers** (sorted by **digit**):
$SPLUNK_HOME/etc/apps/myapp**1**
$SPLUNK_HOME/etc/apps/myapp**10**
$SPLUNK_HOME/etc/apps/myapp**2**
$SPLUNK_HOME/etc/apps/myapp**20**

UPPERCASE

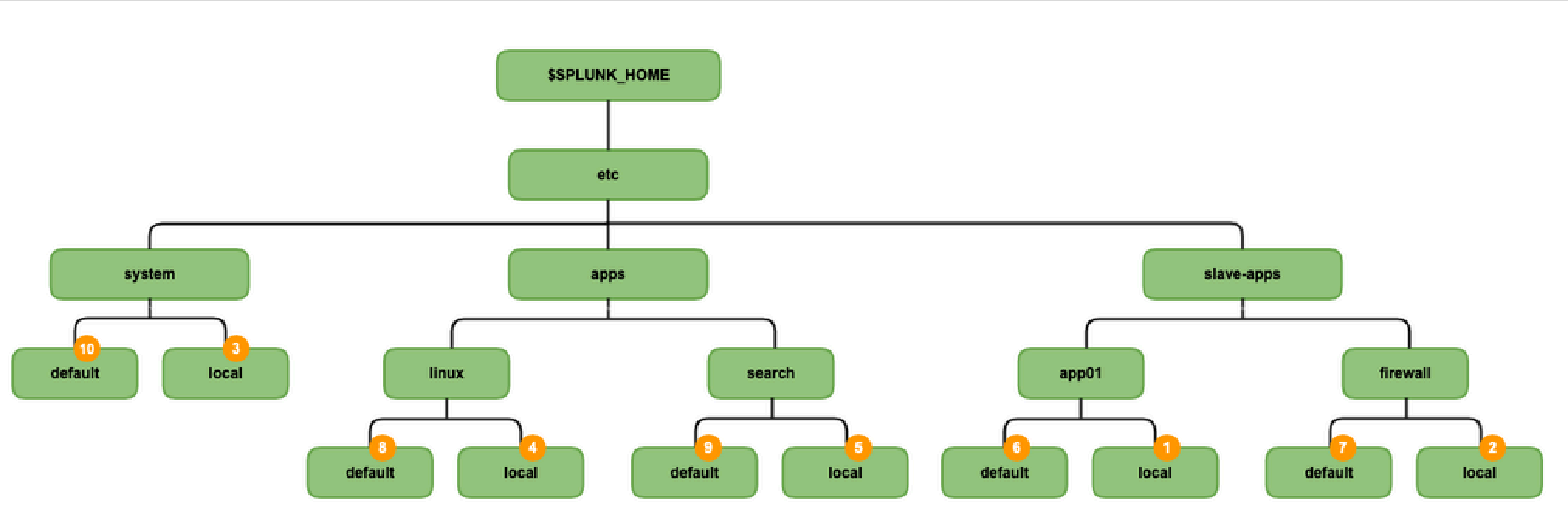
Then, **uppercase letters**:
$SPLUNK_HOME/etc/apps/myapp**Alpha**
$SPLUNK_HOME/etc/apps/myapp**Bravo**
$SPLUNK_HOME/etc/apps/myapp**Charlie**
$SPLUNK_HOME/etc/apps/myapp**Delta**

LOWERCASE

Then, **lowercase letters**:
$SPLUNK_HOME/etc/apps/myapp**alpha**
$SPLUNK_HOME/etc/apps/myapp**bravo**
$SPLUNK_HOME/etc/apps/myapp**charlie**
$SPLUNK_HOME/etc/apps/myapp**delta**

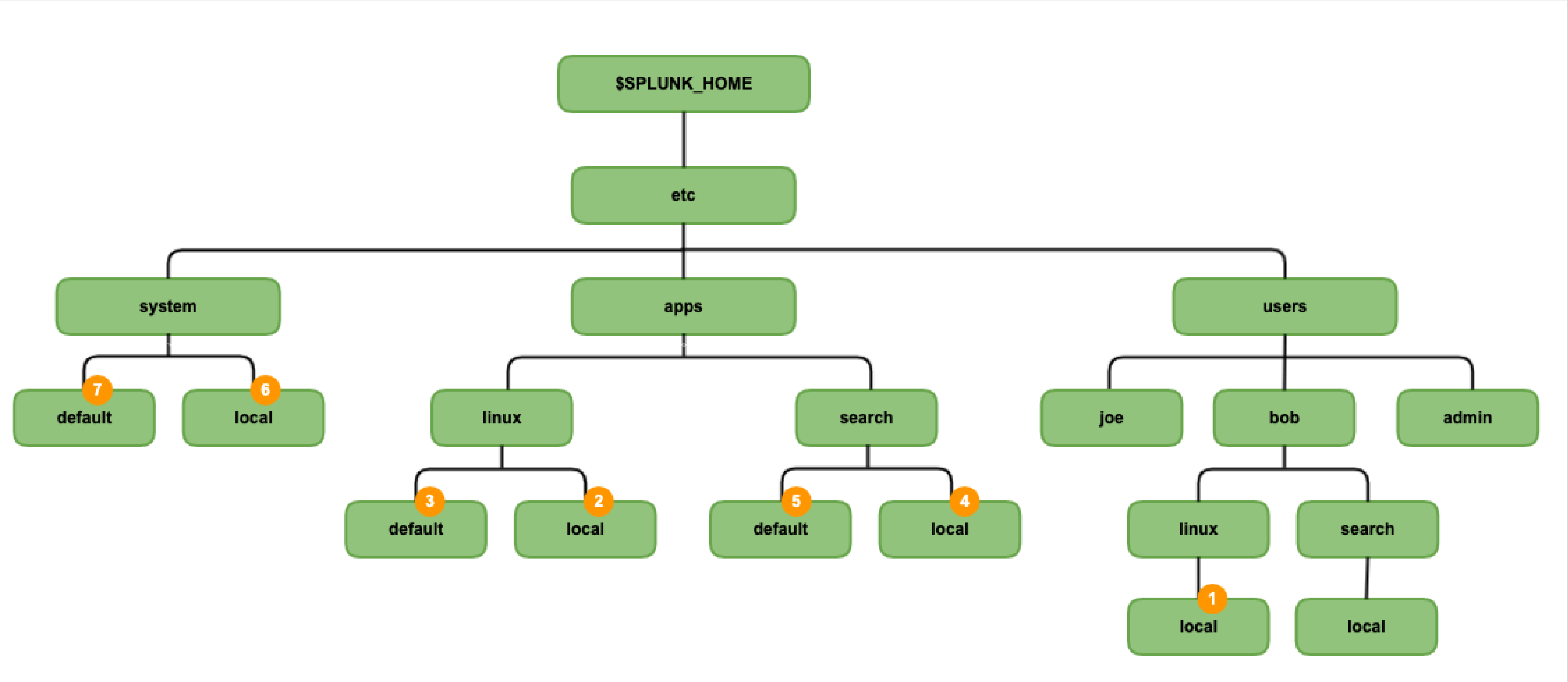
Precedence: (indexer cluster)

Slave-app local : $SPLUNK_HOME/etc/slave-apps/local/
System local : $SPLUNK_HOME/etc/system/local/
App local : $SPLUNK_HOME/etc/apps//local/
Slave-app default : $SPLUNK_HOME/etc/slave-apps/default/
App default : $SPLUNK_HOME/etc/apps//default/
System default : $SPLUNK_HOME/etc/system/default/



Precedence Search time :

User app local : $SPLUNK_HOME/etc///local/
App local current app : $SPLUNK_HOME/etc/apps//local/
App default current app : $SPLUNK_HOME/etc/apps//default/
Others app local : $SPLUNK_HOME/etc/apps//local/
Others app default : $SPLUNK_HOME/etc/apps//default/
System local : $SPLUNK_HOME/etc/system/local/
System default : $SPLUNK_HOME/etc/system/default/


$SPLUNK_HOME
etc
system
apps
users
7
default
6
local
linux
search
joe
bob
admin
3
default
2
local
5
default
4
local
linux
search
1
local
local