How to Troubleshoot Blocked Ingestion Pipeline Queues with Indexers and Forwarders

Harendra Rawat
Senior Principal Software Engineer | Splunk Inc.

splunk> .conf19

Harendra Rawat

Senior Principal Software Engineer | Splunk Inc.

Gaurav Gupta

Senior Software Engineer | Splunk Inc.

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or plans of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only, and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Turn Data Into Doing, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2019 Splunk Inc. All rights reserved.

How to troubleshoot blocked ingestion pipeline queues with Indexers and Forwarders

Troubleshoot blocked ingestion pipeline queues

splunk> .conf19

Agenda

Troubleshoot blocked ingestion pipeline queues

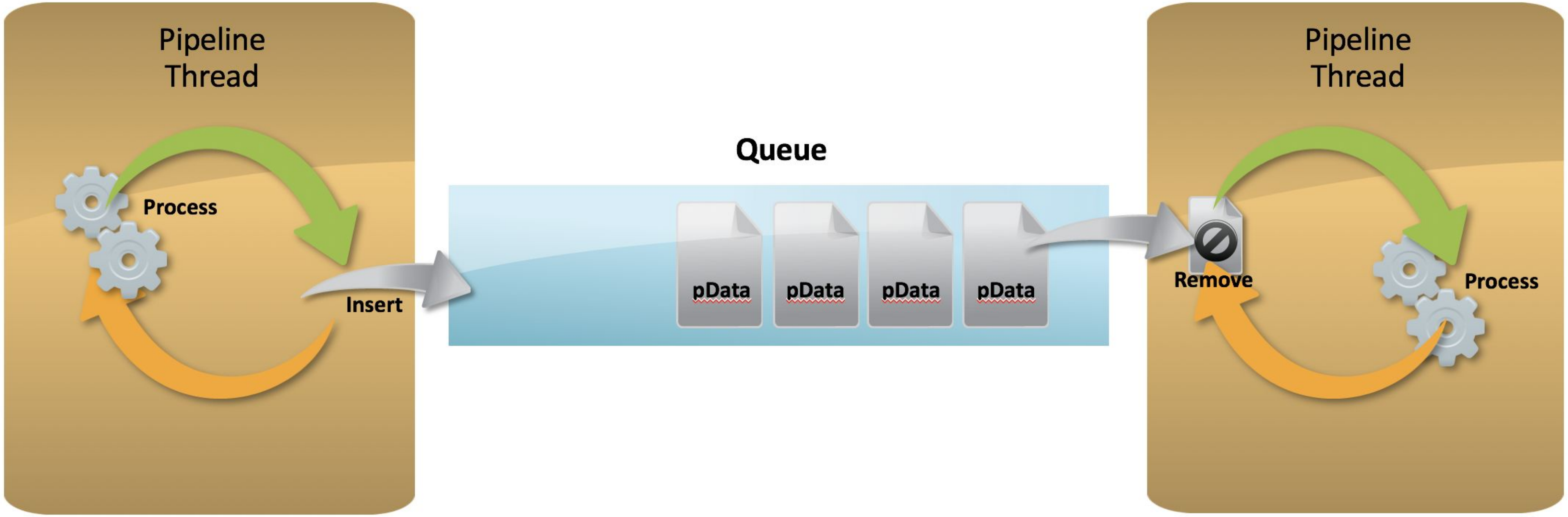
- Introduction to Splunk ingestion pipeline queues
- Typical problems associated with queues
  - Blocked queues, low ingestion thruput and broken/orphaned events
- How to find problematic queue
- Debugging problematic queue
- How to fix problematic queue

Splunk Ingestion Pipeline Queues

Forwarder pipeline queues

Splunk Ingestion Pipeline Queues

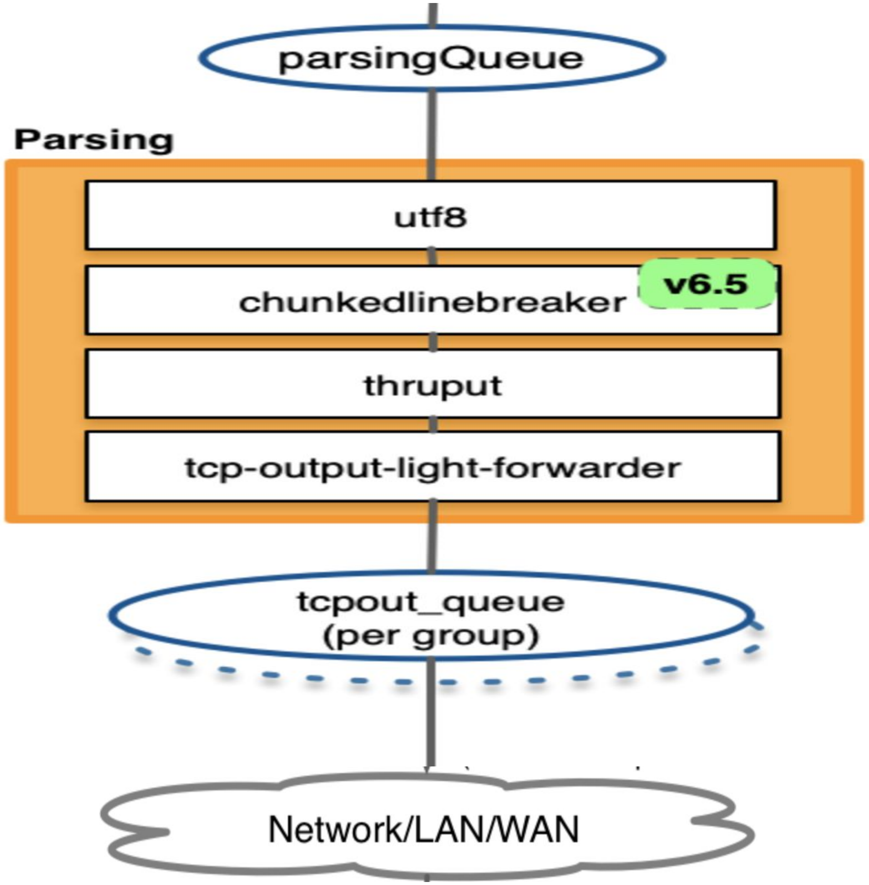
Queue



- Queue size bounded by memory
- Holds variable sized Pipeline Data

Forwarder Ingestion Pipeline

Forwarder ingestion pipeline queues

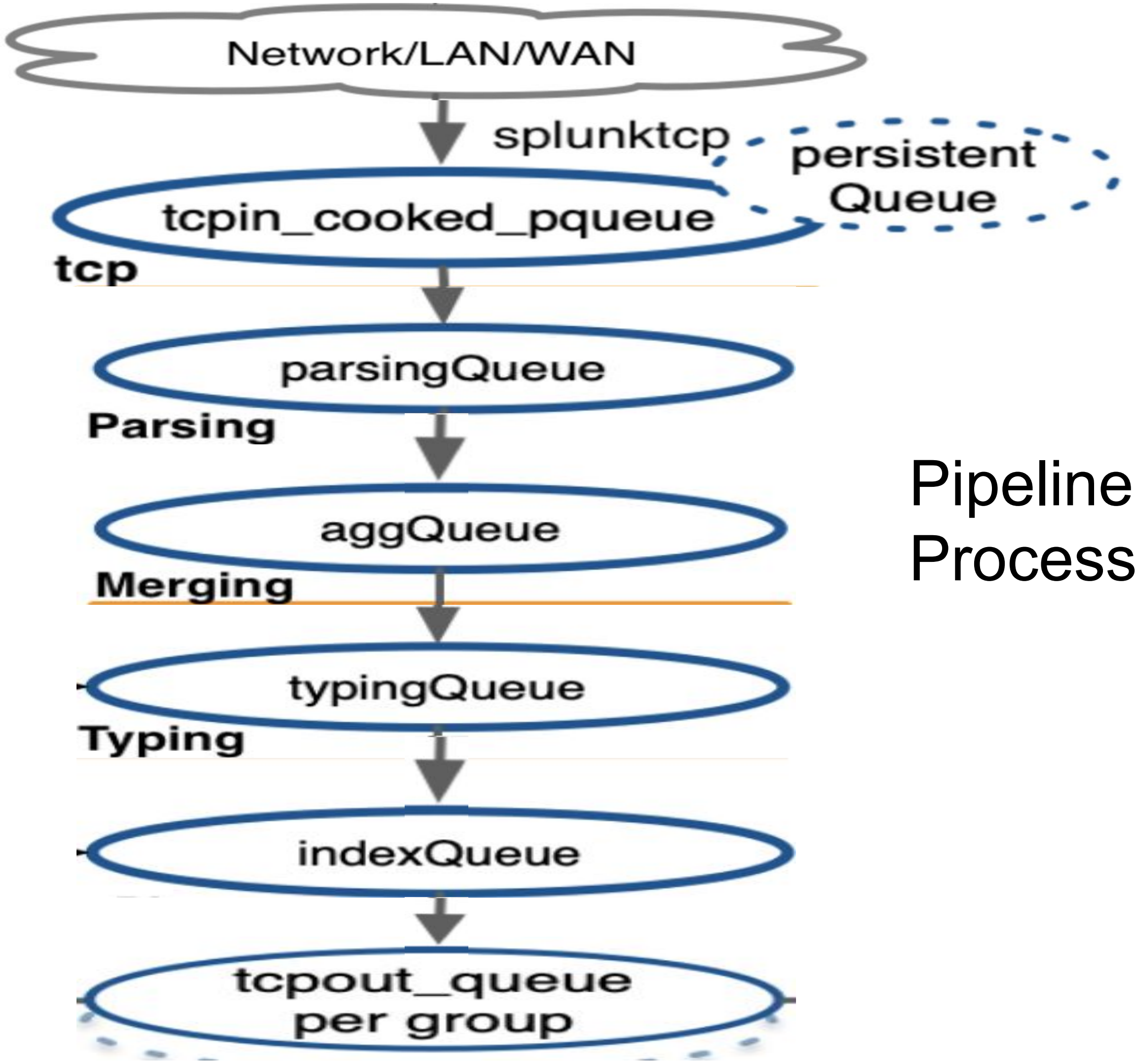


- Remember the order of queues and processor in the pipeline.

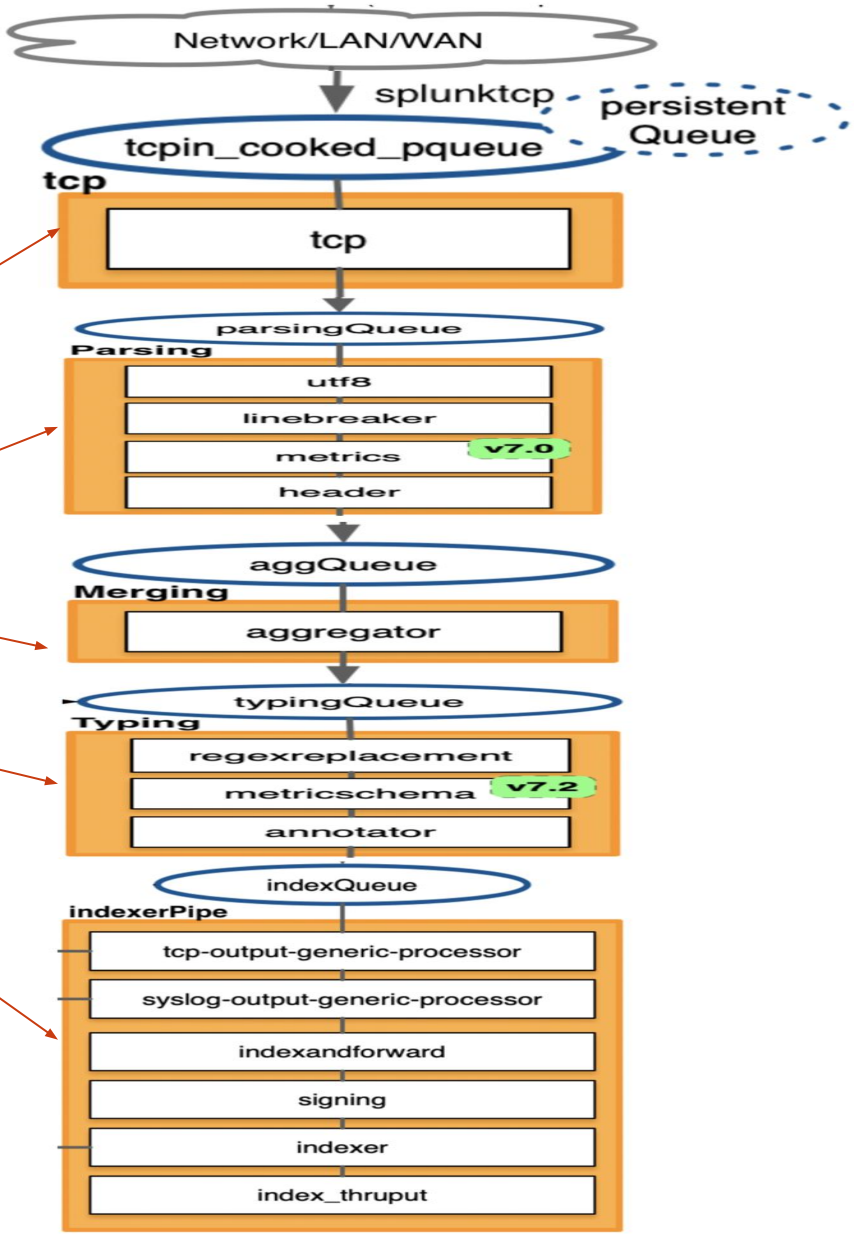
Indexer Ingestion Pipeline

Indexer pipeline queues

Indexer Ingestion Pipeline



Pipeline
Processor threads



- Remember the order of queues and processor in the pipeline.

Typical Problems Associated with Queues

Problems with ingestion pipeline queues

Typical Problems Associated with Queues

Problems with queues

Blocked queue

Low ingestion thruput

Missing Broken/Orphaned Events

How to Find Problematic Queue

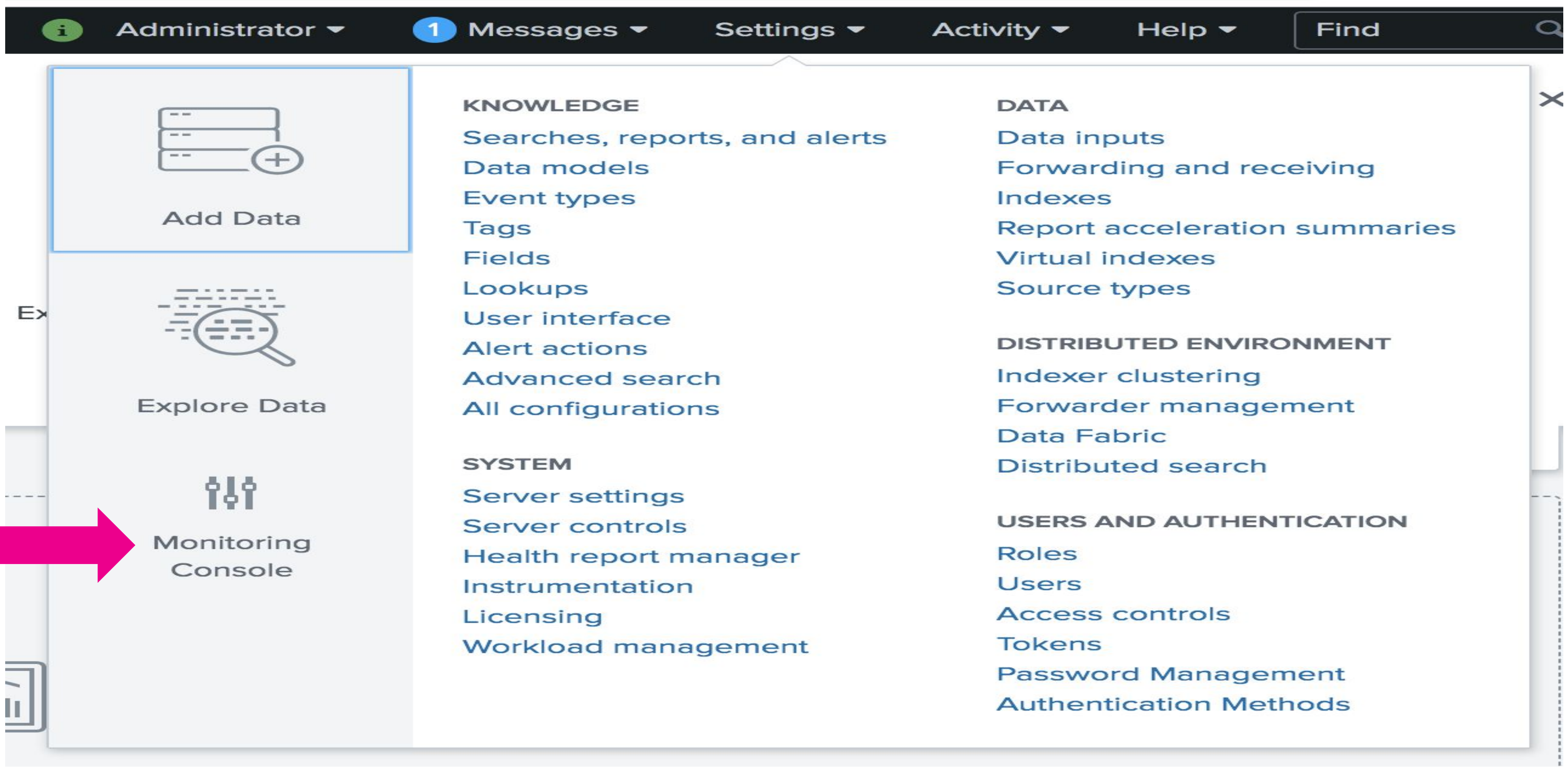
Identifying the queue causing blocked ingestion pipeline

splunk> .conf19

How to Find Problematic Queue With

Identifying the queue responsible for blocked ingestion pipeline

- Click on >Monitoring Console(MC)



KNOWLEDGE
Searches, reports, and alerts
Data models
Event types
Tags
Fields
Lookups
User interface
Alert actions
Advanced search
All configurations

SYSTEM
Server settings
Server controls
Health report manager
Instrumentation
Licensing
Workload management

DATA
Data inputs
Forwarding and receiving
Indexes
Report acceleration summaries
Virtual indexes
Source types

DISTRIBUTED ENVIRONMENT
Indexer clustering
Forwarder management
Data Fabric
Distributed search

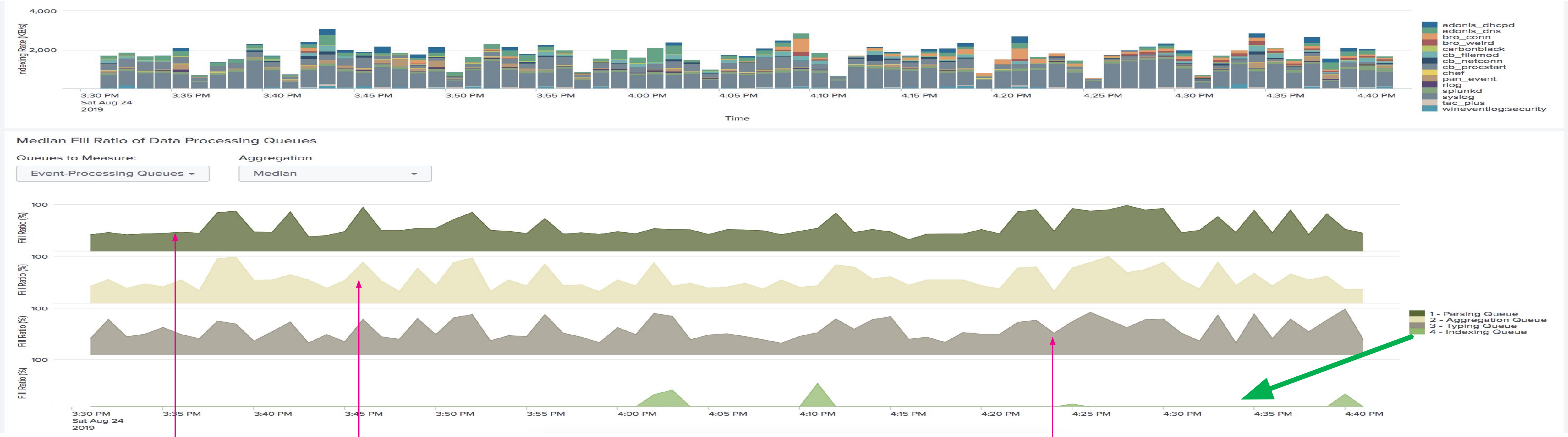
USERS AND AUTHENTICATION
Roles
Users
Access controls
Tokens
Password Management
Authentication Methods

- Remember MC.

How to Find Problematic Queue

Identifying the queue responsible for blocked ingestion pipeline

- Click on >(MC)Indexing->Performance->Indexing Performance : Instance.



Median Fill Ratio of Data Processing Queues

Queues to Measure: Event-Processing Queues

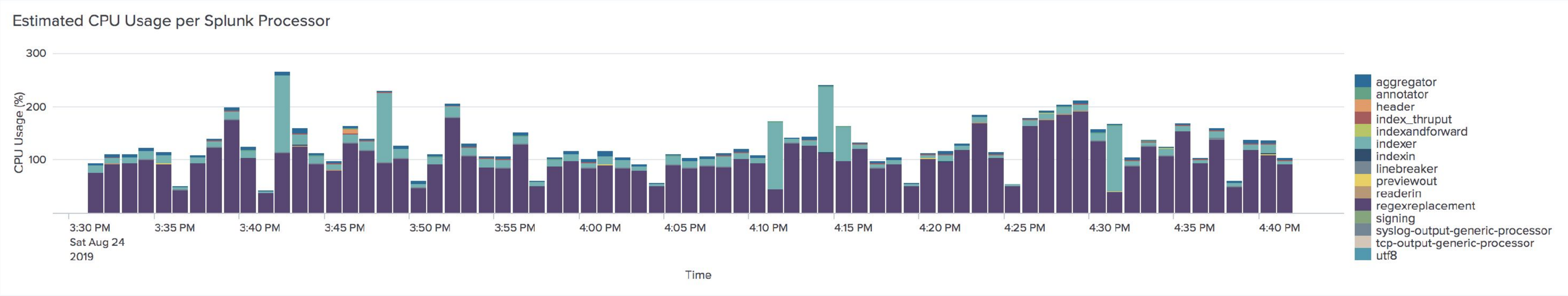
Aggregation: Median

- Remember the order of queues in the pipeline
- Parsing/Aggregation queues are blocked due to Typing queue
- Typing Queue is the bottleneck

How to Find Problematic Queue

Identifying the queue responsible for blocked ingestion pipeline

- Click on >(MC)Indexing->Performance->Indexing Performance : Advanced.



Estimated CPU Usage per Splunk Processor

- In limits.conf add [default]
  regex_cpu_profiling = true
- Restart splunk

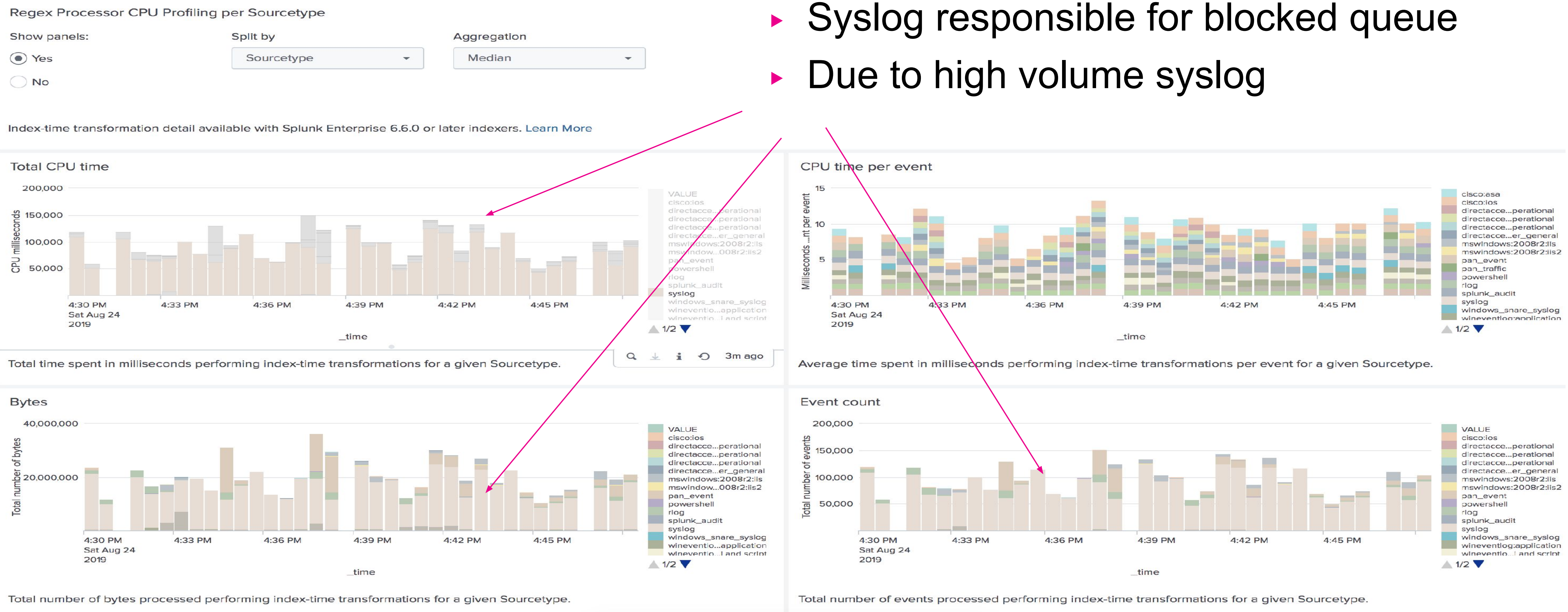
- How to enable identify CPU usage using MC
- How to enable regex cpu profiling

Debugging Blocked Queue

Troubleshooating typing queue

Click on >(MC)Indexing->Performance->Indexing Performance : Advanced.

- Syslog responsible for blocked queue
- Due to high volume syslog



Regex Processor CPU Profiling per Sourcetype

Show panels: ● Yes ○ No

Split by: Sourcetype

Aggregation: Median

Index-time transformation detail available with Splunk Enterprise 6.6.0 or later indexers. Learn More

Total CPU time

Total time spent in milliseconds performing index-time transformations for a given Sourcetype.

CPU time per event

Average time spent in milliseconds performing index-time transformations per event for a given Sourcetype.

Bytes

Total number of bytes processed performing index-time transformations for a given Sourcetype.

Event count

Total number of events processed performing index-time transformations for a given Sourcetype.

- Take away> Use MC to find offending source/sourcetype causing blocked typing queue.

splunk> .conf19

How to Find Problematic Queue

Identify the queue responsible for blocked ingestion pipeline

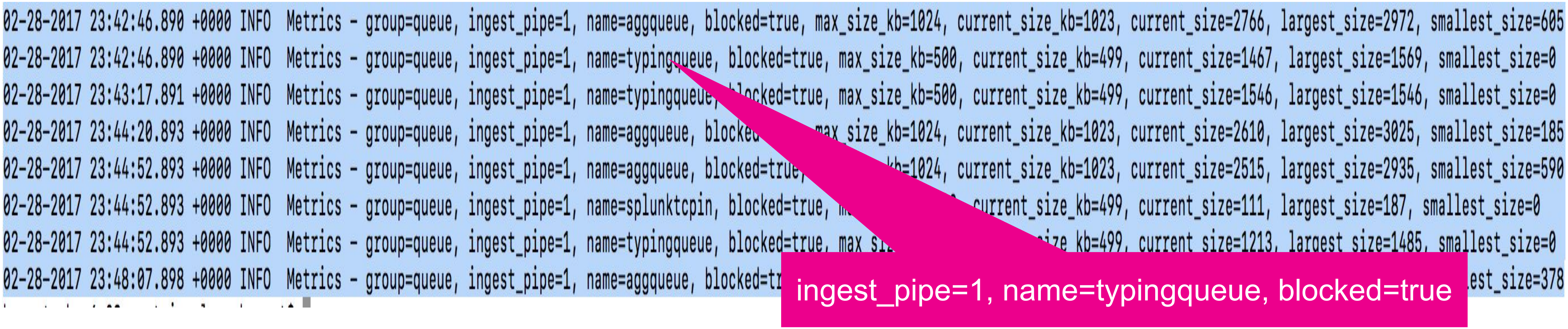
How to Find Problematic Queue

Identifying the queue responsible for blocked ingestion pipeline

Using “grep” cli command

ingest_pipe=1, name=aggqueue, blocked=true

```
>grep blocked metrics.log
```



```
02-28-2017 23:42:46.890 +0000 INFO  Metrics - group=queue, ingest_pipe=1, name=aggqueue, blocked=true, max_size_kb=1024, current_size_kb=1023, current_size=2766, largest_size=2972, smallest_size=605
02-28-2017 23:42:46.890 +0000 INFO  Metrics - group=queue, ingest_pipe=1, name=typingqueue, blocked=true, max_size_kb=500, current_size_kb=499, current_size=1467, largest_size=1569, smallest_size=0
02-28-2017 23:43:17.891 +0000 INFO  Metrics - group=queue, ingest_pipe=1, name=typingqueue, blocked=true, max_size_kb=500, current_size_kb=499, current_size=1546, largest_size=1546, smallest_size=0
02-28-2017 23:44:20.893 +0000 INFO  Metrics - group=queue, ingest_pipe=1, name=aggqueue, blocke          max_size_kb=1024, current_size_kb=1023, current_size=2610, largest_size=3025, smallest_size=185
02-28-2017 23:44:52.893 +0000 INFO  Metrics - group=queue, ingest_pipe=1, name=aggqueue, blocked=true,              kb=1024, current_size_kb=1023, current_size=2515, largest_size=2935, smallest_size=590
02-28-2017 23:44:52.893 +0000 INFO  Metrics - group=queue, ingest_pipe=1, name=splunktcpin, blocked=true, m               current_size_kb=499, current_size=111, largest_size=187, smallest_size=0
02-28-2017 23:44:52.893 +0000 INFO  Metrics - group=queue, ingest_pipe=1, name=typingqueue, blocked=true, max si              ize_kb=499, current_size=1213, largest_size=1485, smallest_size=0
02-28-2017 23:48:07.898 +0000 INFO  Metrics - group=queue, ingest_pipe=1, name=aggqueue, blocked=tr                                                                                        est_size=378
```

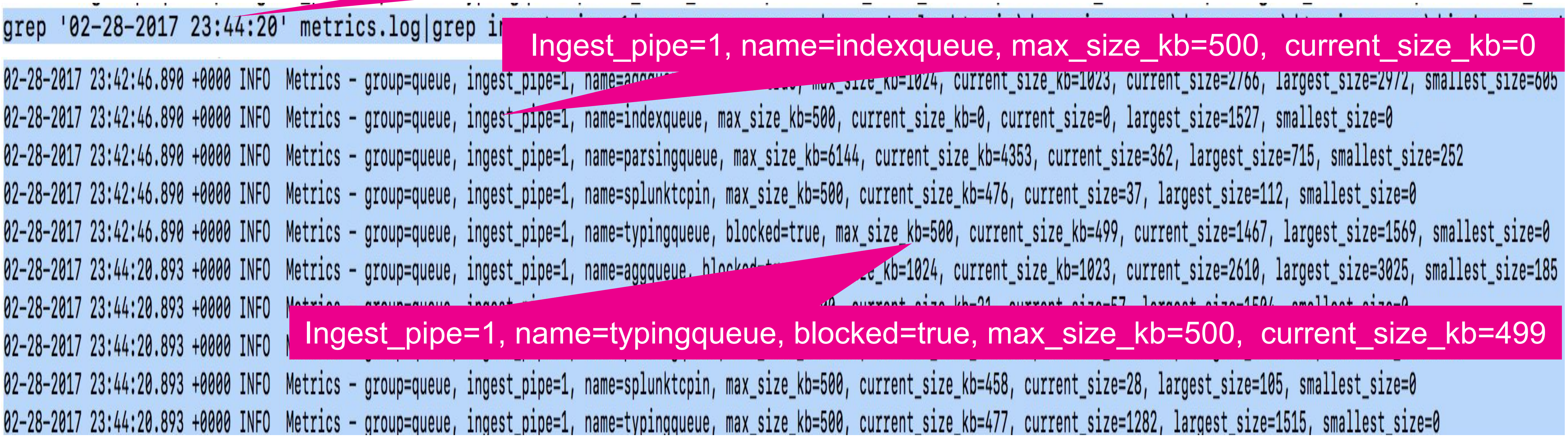
ingest_pipe=1, name=typingqueue, blocked=true

- Parsing/Aggregation queues are blocked due to Typing queue.
- Typing Queue is the bottleneck
- Using ‘grep’ cli find blocked queues.

How to Find Problematic Queue

Identifying the queue responsible for blocked ingestion pipeline

```
>grep ‘02-28-2017 23:44:20’ metrics.log| grep ingest_pipe=1|grep group=queue
```



```
grep '02-28-2017 23:44:20' metrics.log|grep i
02-28-2017 23:42:46.890 +0000 INFO  Metrics - group=queue, ingest_pipe=1, name=agg      max_size_kb=1024, current_size_kb=1023, current_size=2766, largest_size=2972, smallest_size=605
02-28-2017 23:42:46.890 +0000 INFO  Metrics - group=queue, ingest_pipe=1, name=indexqueue, max_size_kb=500, current_size_kb=0, current_size=0, largest_size=1527, smallest_size=0
02-28-2017 23:42:46.890 +0000 INFO  Metrics - group=queue, ingest_pipe=1, name=parsingqueue, max_size_kb=6144, current_size_kb=4353, current_size=362, largest_size=715, smallest_size=252
02-28-2017 23:42:46.890 +0000 INFO  Metrics - group=queue, ingest_pipe=1, name=splunktcpin, max_size_kb=500, current_size_kb=476, current_size=37, largest_size=112, smallest_size=0
02-28-2017 23:42:46.890 +0000 INFO  Metrics - group=queue, ingest_pipe=1, name=typingqueue, blocked=true, max_size_kb=500, current_size_kb=499, current_size=1467, largest_size=1569, smallest_size=0
02-28-2017 23:44:20.893 +0000 INFO  Metrics - group=queue, ingest_pipe=1, name=aggqueue,             kb=1024, current_size_kb=1023, current_size=2610, largest_size=3025, smallest_size=185
02-28-2017 23:44:20.893 +0000 INFO
02-28-2017 23:44:20.893 +0000 INFO
02-28-2017 23:44:20.893 +0000 INFO  Metrics - group=queue, ingest_pipe=1, name=splunktcpin, max_size_kb=500, current_size_kb=458, current_size=28, largest_size=105, smallest_size=0
02-28-2017 23:44:20.893 +0000 INFO  Metrics - group=queue, ingest_pipe=1, name=typingqueue, max_size_kb=500, current_size_kb=477, current_size=1282, largest_size=1515, smallest_size=0
```

Ingest_pipe=1, name=indexqueue, max_size_kb=500, current_size_kb=0

Ingest_pipe=1, name=typingqueue, blocked=true, max_size_kb=500, current_size_kb=499

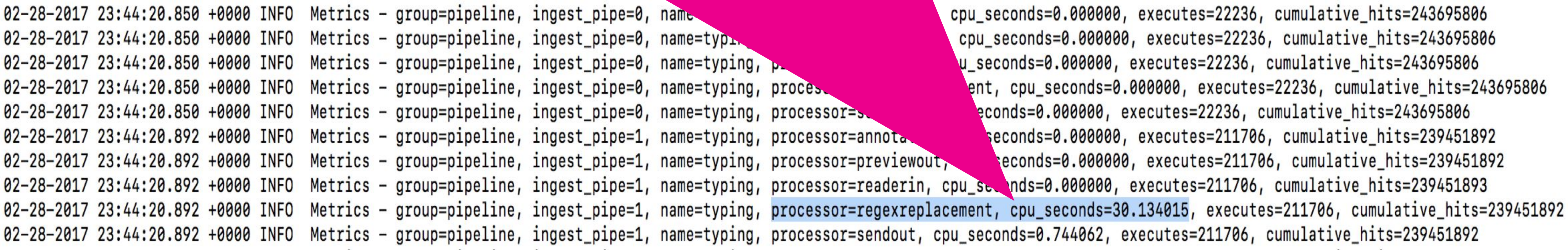
- Remember the order of queues in the pipeline.
- Parsing/Aggregation queues are blocked due to Typing queue.
- Using ‘grep’ cli find blocked queues for a specific time range. Find the queues that are not blocked.

Finding processor causing blocked queue

Troubleshooting typing queue

grep name=typing metrics.log |grep ”

Processor=reegexreeplacement, cpu_seconds=30.134015



```
02-28-2017 23:44:20.850 +0000 INFO  Metrics - group=pipeline, ingest_pipe=0, name                    cpu_seconds=0.000000, executes=22236, cumulative_hits=243695806
02-28-2017 23:44:20.850 +0000 INFO  Metrics - group=pipeline, ingest_pipe=0, name=typi                cpu_seconds=0.000000, executes=22236, cumulative_hits=243695806
02-28-2017 23:44:20.850 +0000 INFO  Metrics - group=pipeline, ingest_pipe=0, name=typing, p             u_seconds=0.000000, executes=22236, cumulative_hits=243695806
02-28-2017 23:44:20.850 +0000 INFO  Metrics - group=pipeline, ingest_pipe=0, name=typing, proce            ent, cpu_seconds=0.000000, executes=22236, cumulative_hits=243695806
02-28-2017 23:44:20.850 +0000 INFO  Metrics - group=pipeline, ingest_pipe=0, name=typing, processor=s        econds=0.000000, executes=22236, cumulative_hits=243695806
02-28-2017 23:44:20.892 +0000 INFO  Metrics - group=pipeline, ingest_pipe=1, name=typing, processor=annota     seconds=0.000000, executes=211706, cumulative_hits=239451892
02-28-2017 23:44:20.892 +0000 INFO  Metrics - group=pipeline, ingest_pipe=1, name=typing, processor=previewout,   econds=0.000000, executes=211706, cumulative_hits=239451892
02-28-2017 23:44:20.892 +0000 INFO  Metrics - group=pipeline, ingest_pipe=1, name=typing, processor=readerin, cpu_se  nds=0.000000, executes=211706, cumulative_hits=239451893
02-28-2017 23:44:20.892 +0000 INFO  Metrics - group=pipeline, ingest_pipe=1, name=typing, processor=regexreplacement, cpu_seconds=30.134015, executes=211706, cumulative_hits=239451892
02-28-2017 23:44:20.892 +0000 INFO  Metrics - group=pipeline, ingest_pipe=1, name=typing, processor=sendout, cpu_seconds=0.744062, executes=211706, cumulative_hits=239451892
```

- Remember the processors of typing queue.
- Search cpu usage(cpu_seconds) in metrics.log for name=typing.
- Typing Queue is blocked due to regexreplacement

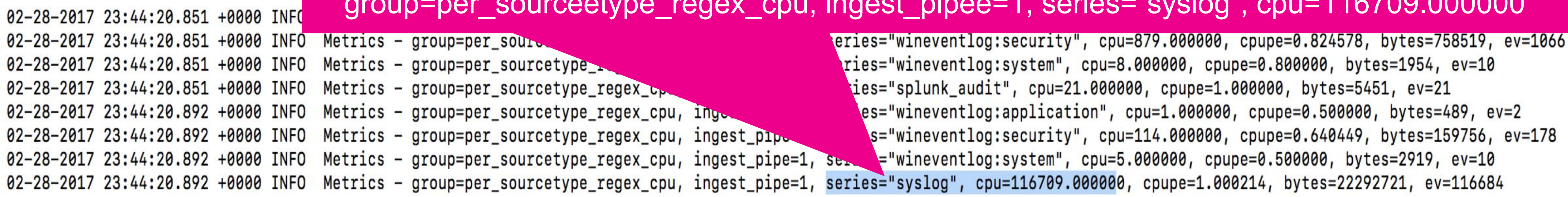
- Using ‘grep name=typing metrics.log |grep ”02-28-2017 23:44:20”’ find all processors associated with typing queue.
- Find the processor consuming most of the cpu seconds.

Finding sourcetype causing blocked queue

Using regexreplacement processor cpu profiling

- In limits.conf add following and Restart splunk
- [default]
  regex_cpu_profiling = true

grep group=per_sourcetype_regex_cpu metrics.log |grep ”02-28-2017 23:44:20”



group=per_sourceetype_regex_cpu, ingest_pipee=1, series=“syslog”, cpu=116709.000000

```
02-28-2017 23:44:20.851 +0000 INFO
02-28-2017 23:44:20.851 +0000 INFO  Metrics - group=per_sou                              eries="wineventlog:security", cpu=879.000000, cpupe=0.824578, bytes=758519, ev=1066
02-28-2017 23:44:20.851 +0000 INFO  Metrics - group=per_sourcetype_                       ries="wineventlog:system", cpu=8.000000, cpupe=0.800000, bytes=1954, ev=10
02-28-2017 23:44:20.851 +0000 INFO  Metrics - group=per_sourcetype_regex_c                 ies="splunk_audit", cpu=21.000000, cpupe=1.000000, bytes=5451, ev=21
02-28-2017 23:44:20.892 +0000 INFO  Metrics - group=per_sourcetype_regex_cpu, in             es="wineventlog:application", cpu=1.000000, cpupe=0.500000, bytes=489, ev=2
02-28-2017 23:44:20.892 +0000 INFO  Metrics - group=per_sourcetype_regex_cpu, ingest_pip      s="wineventlog:security", cpu=114.000000, cpupe=0.640449, bytes=159756, ev=178
02-28-2017 23:44:20.892 +0000 INFO  Metrics - group=per_sourcetype_regex_cpu, ingest_pipe=1, se    ="wineventlog:system", cpu=5.000000, cpupe=0.500000, bytes=2919, ev=10
02-28-2017 23:44:20.892 +0000 INFO  Metrics - group=per_sourcetype_regex_cpu, ingest_pipe=1, series="syslog", cpu=116709.000000, cpupe=1.000214, bytes=22292721, ev=116684
```

- ▸ Breakdown total time spent by regexreplacement processor.
- ▸ Search ‘per_sourcetype_regex_cpu’ in metrics.log
- ▸ ‘syslog’ is the reason typing Queue is blocked.
- ▸ Using ‘grep group=per_sourcetype_regex_cpu metrics.log |grep ”02-28-2017 23:44:20”’
  find total regex cpu usage for each sourcetype for a given time range.
- ▸ Find the sourcetype consuming most of the cpu in milliseconds.

splunk> .conf19

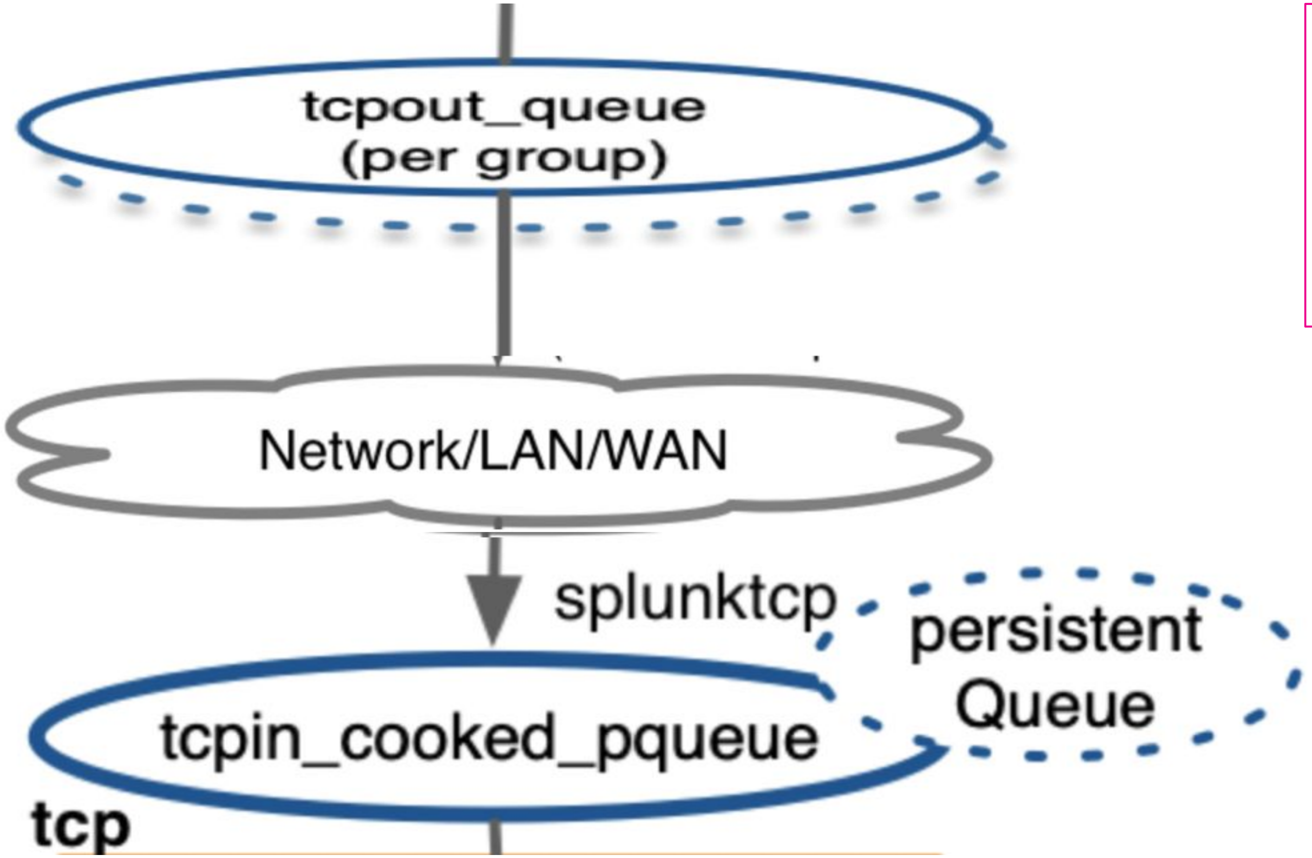
Debugging blocked tcpout queue

Troubleshoot blocked ingestion pipeline queues

.conf19
splunk>

TcpoutQ to TcpinQ

Troubleshooting Blocked Tcpout queue



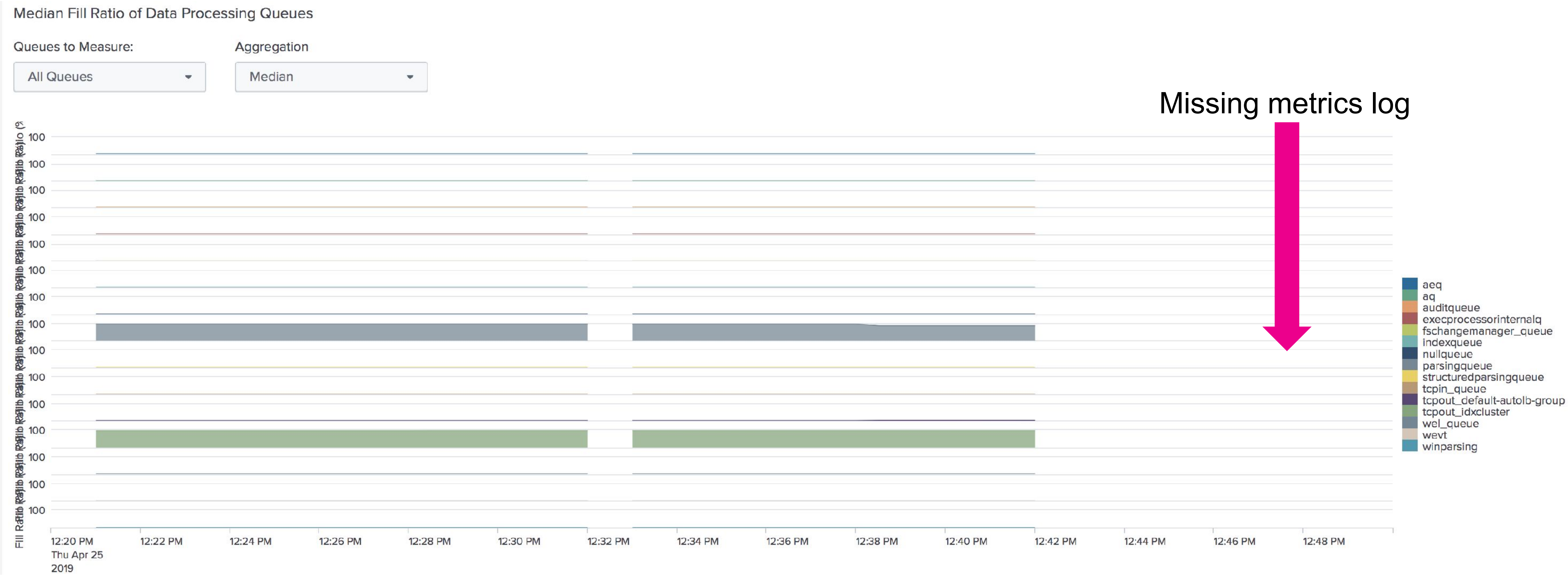
- netstat
- ping
- metrics.log

- Tools/log possibly needed to narrow down the cause of TcpoutQ blockage

Check TcpoutQ status on Monitoring Console

Troubleshooting Blocked Tcpout queue

- Click on >(MC)Indexing->Performance->Indexing Performance : Instance.



Median Fill Ratio of Data Processing Queues

Queues to Measure: All Queues

Aggregation: Median

Missing metrics log

- Monitoring console indicates TcpoutQ is blocked.
- There is missing metrics.log data due to indexing latency caused by blocked TcpoutQ

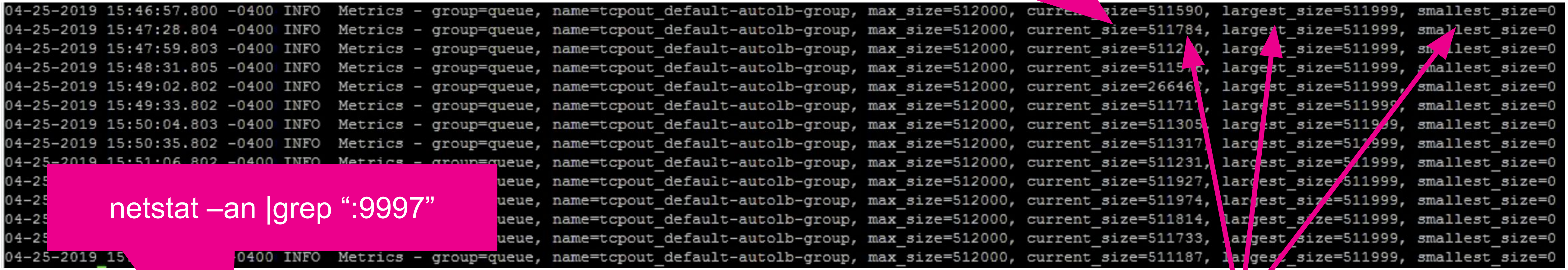
splunk> .conf19

Live troublesho

current_size=511590, largest_size=511999, smallest_size=0
current_size=511784, largest_size=511999, smallest_size=0

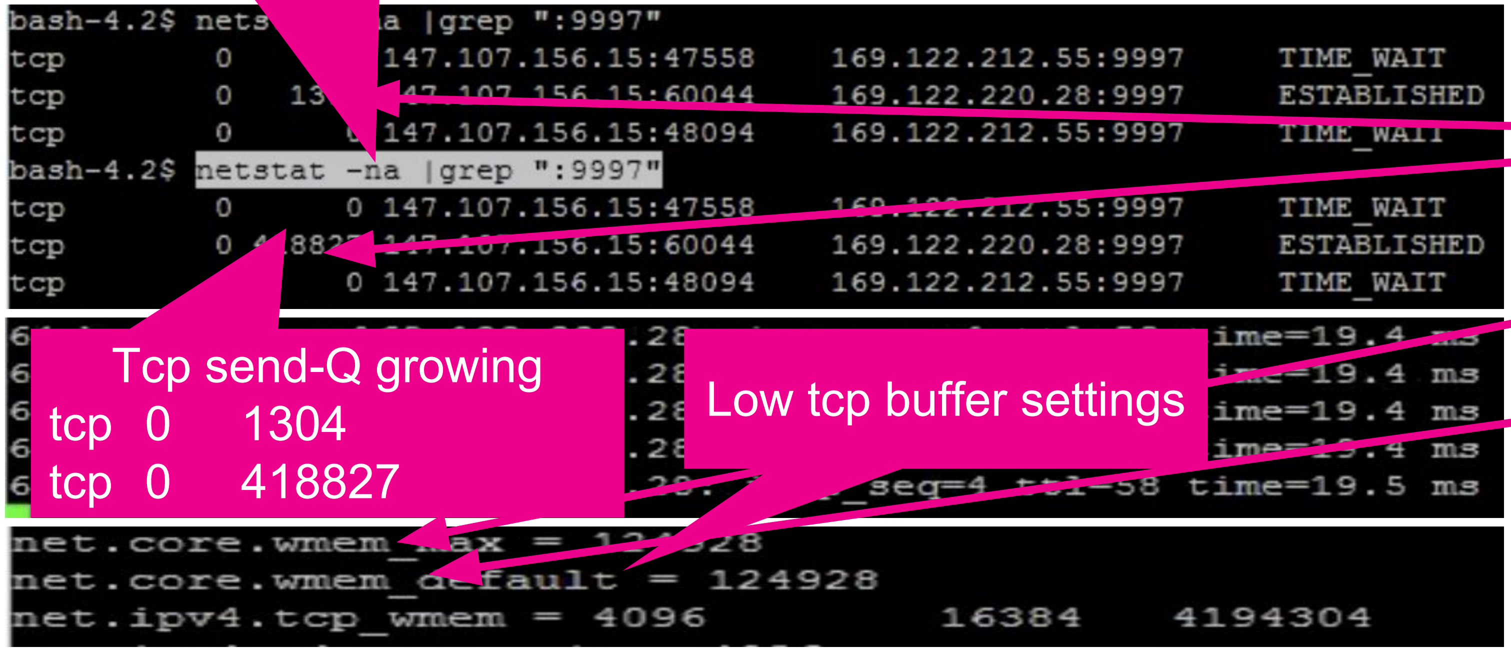
With metrics.log/netstat/sy g

>grep name=tcpout_ metrics.log



```
04-25-2019 15:46:57.800 -0400 INFO  Metrics - group=queue, name=tcpout_default-autolb-group, max_size=512000, curre  size=511590, largest_size=511999, smallest_size=0
04-25-2019 15:47:28.804 -0400 INFO  Metrics - group=queue, name=tcpout_default-autolb-group, max_size=512000, current_size=511784, largest_size=511999, smallest_size=0
04-25-2019 15:47:59.803 -0400 INFO  Metrics - group=queue, name=tcpout_default-autolb-group, max_size=512000, current_size=5112[illegible]0, larg  t_size=511999, sm llest_size=0
04-25-2019 15:48:31.805 -0400 INFO  Metrics - group=queue, name=tcpout_default-autolb-group, max_size=512000, current_size=5115[illegible]6, largest_size=511999, smallest_size=0
04-25-2019 15:49:02.802 -0400 INFO  Metrics - group=queue, name=tcpout_default-autolb-group, max_size=512000, current_size=26646 , largest_size=511999, smallest_size=0
04-25-2019 15:49:33.802 -0400 INFO  Metrics - group=queue, name=tcpout_default-autolb-group, max_size=512000, current_size=51171 , largest_size=51199 , smallest_size=0
04-25-2019 15:50:04.803 -0400 INFO  Metrics - group=queue, name=tcpout_default-autolb-group, max_size=512000, current_size=511305, largest_size=511999, smallest_size=0
04-25-2019 15:50:35.802 -0400 INFO  Metrics - group=queue, name=tcpout_default-autolb-group, max_size=512000, current_size=511317, largest_size=511999, smallest_size=0
04-25-2019 15:51:06.802 -0400 INFO  Metrics - group=queue, name=tcpout_default-autolb-group, max_size=512000, current_size=511231, largest_size=511999, smallest_size=0
04-25                                    ueue, name=tcpout_default-autolb-group, max_size=512000, current_size=511927, largest_size=511999, smallest_size=0
04-25                                    ueue, name=tcpout_default-autolb-group, max_size=512000, current_size=511974, largest_size=511999, smallest_size=0
04-25                                    ueue, name=tcpout_default-autolb-group, max_size=512000, current_size=511814, largest_size=511999, smallest_size=0
04-25                                    ueue, name=tcpout_default-autolb-group, max_size=512000, current_size=511733, largest_size=511999, smallest_size=0
04-25-2019 15       0400 INFO  Metrics - group=queue, name=tcpout_default-autolb-group, max_size=512000, current_size=511187, largest_size=511999, smallest_size=0
```

netstat –an |grep ":9997"



```
bash-4.2$ nets     a |grep ":9997"
tcp        0          147.107.156.15:47558    169.122.212.55:9997     TIME_WAIT
tcp        0    13                            169.122.220.28:9997     ESTABLISHED
tcp        0          147.107.156.15:48094    169.122.212.55:9997     TIME_WAIT
bash-4.2$ netstat -na |grep ":9997"
tcp        0        0 147.107.156.15:47558                            TIME_WAIT
tcp        0                                  169.122.220.28:9997     ESTABLISHED
tcp        0        0 147.107.156.15:48094    169.122.212.55:9997     TIME_WAIT
```

```
                                              ime=19.4 ms
                                              ime=19.4 ms
                                              ime=19.4 ms
                                                    .4 ms
                              seq=4 ttl=58 time=19.5 ms
```

```
net.core.wmem_
net.core.wmem_         = 124928
net.ipv4.tcp_wmem = 4096         16384    4194304
```

Tcp send-Q growing

tcp 0 1304

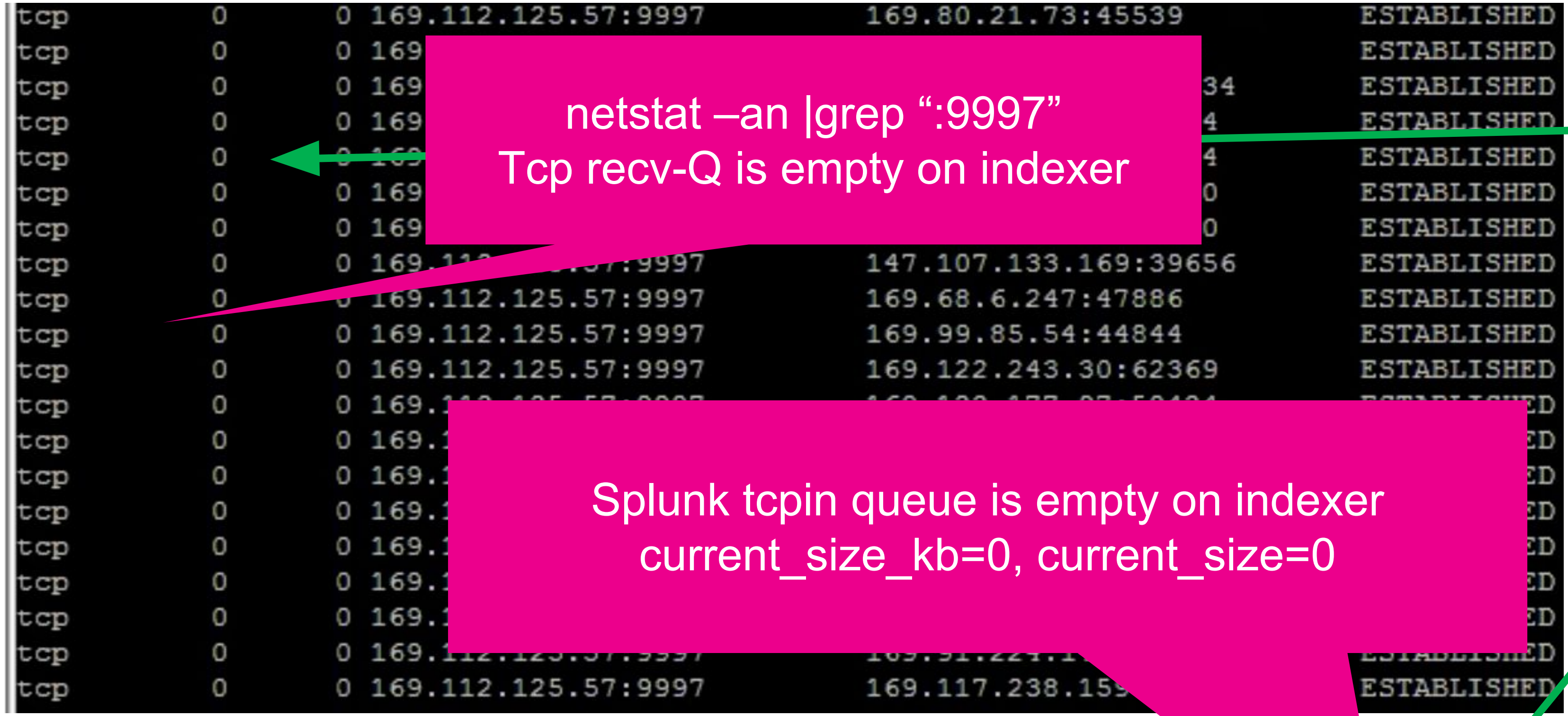
tcp 0 418827

Low tcp buffer settings

- tcpout queue fluctuating.
- tcp send buffer is growing.
- tcp layer buffers are low and might be an issue.
- >sysctl –an |grep wmem
- Investigate TcpinQ concurrently.

Live troubleshooting Tcpin queue

With metrics.log/netstat



```
tcp        0      0 169.112.125.57:9997         169.80.21.73:45539          ESTABLISHED
tcp        0      0 169                                                     ESTABLISHED
tcp        0      0 169                                               34    ESTABLISHED
tcp        0      0 169                                               4     ESTABLISHED
tcp        0                                                          4     ESTABLISHED
tcp        0      0 169                                               0     ESTABLISHED
tcp        0      0 169                                               0     ESTABLISHED
tcp        0      0 169.                  :9997         147.107.133.169:39656       ESTABLISHED
tcp        0        169.112.125.57:9997         169.68.6.247:47886          ESTABLISHED
tcp        0      0 169.112.125.57:9997         169.99.85.54:44844          ESTABLISHED
tcp        0      0 169.112.125.57:9997         169.122.243.30:62369        ESTABLISHED
tcp        0      0 169.                                                        ED
tcp        0      0 169.                                                        ED
tcp        0      0 169.                                                        ED
tcp        0      0 169.                                                        ED
tcp        0      0 169.                                                        ED
tcp        0      0 169.                                                        ED
tcp        0      0 169.                                                        ED
tcp        0      0 169.                                                        ED
tcp        0      0 169.112.125.57:9997         169.117.238.15              ESTABLISHED
```

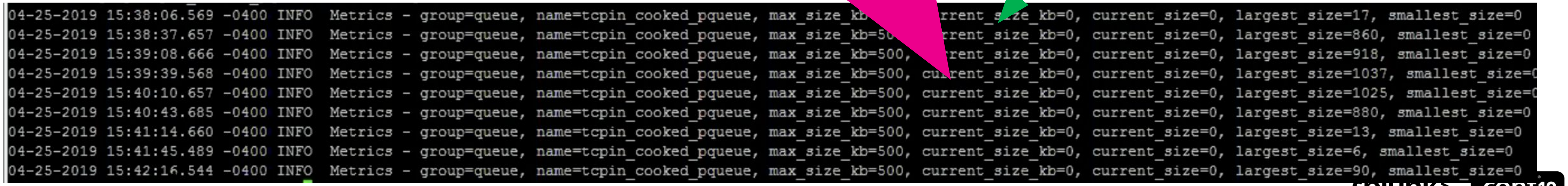
netstat –an |grep ":9997"
Tcp recv-Q is empty on indexer

Splunk tcpin queue is empty on indexer
current_size_kb=0, current_size=0

- tcp recv buffer is empty.
- Splunk tcpin queue is fine as well.

- Tune net.core.wmem_max setting on forwarder. (see previous slide)

>grep name=tcpin_ metrics.log



```
04-25-2019 15:38:06.569 -0400 INFO  Metrics - group=queue, name=tcpin_cooked_pqueue, max_size_kb         rrent_size_kb=0, current_size=0, largest_size=17, smallest_size=0
04-25-2019 15:38:37.657 -0400 INFO  Metrics - group=queue, name=tcpin_cooked_pqueue, max_size_kb=50      rrent_size_kb=0, current_size=0, largest_size=860, smallest_size=0
04-25-2019 15:39:08.666 -0400 INFO  Metrics - group=queue, name=tcpin_cooked_pqueue, max_size_kb=500,    rrent_size_kb=0, current_size=0, largest_size=918, smallest_size=0
04-25-2019 15:39:39.568 -0400 INFO  Metrics - group=queue, name=tcpin_cooked_pqueue, max_size_kb=500, cu rent_size_kb=0, current_size=0, largest_size=1037, smallest_size=0
04-25-2019 15:40:10.657 -0400 INFO  Metrics - group=queue, name=tcpin_cooked_pqueue, max_size_kb=500, current_size_kb=0, current_size=0, largest_size=1025, smallest_size=0
04-25-2019 15:40:43.685 -0400 INFO  Metrics - group=queue, name=tcpin_cooked_pqueue, max_size_kb=500, current_size_kb=0, current_size=0, largest_size=880, smallest_size=0
04-25-2019 15:41:14.660 -0400 INFO  Metrics - group=queue, name=tcpin_cooked_pqueue, max_size_kb=500, current_size_kb=0, current_size=0, largest_size=13, smallest_size=0
04-25-2019 15:41:45.489 -0400 INFO  Metrics - group=queue, name=tcpin_cooked_pqueue, max_size_kb=500, current_size_kb=0, current_size=0, largest_size=6, smallest_size=0
04-25-2019 15:42:16.544 -0400 INFO  Metrics - group=queue, name=tcpin_cooked_pqueue, max_size_kb=500, current_size_kb=0, current_size=0, largest_size=90, smallest_size=0
```

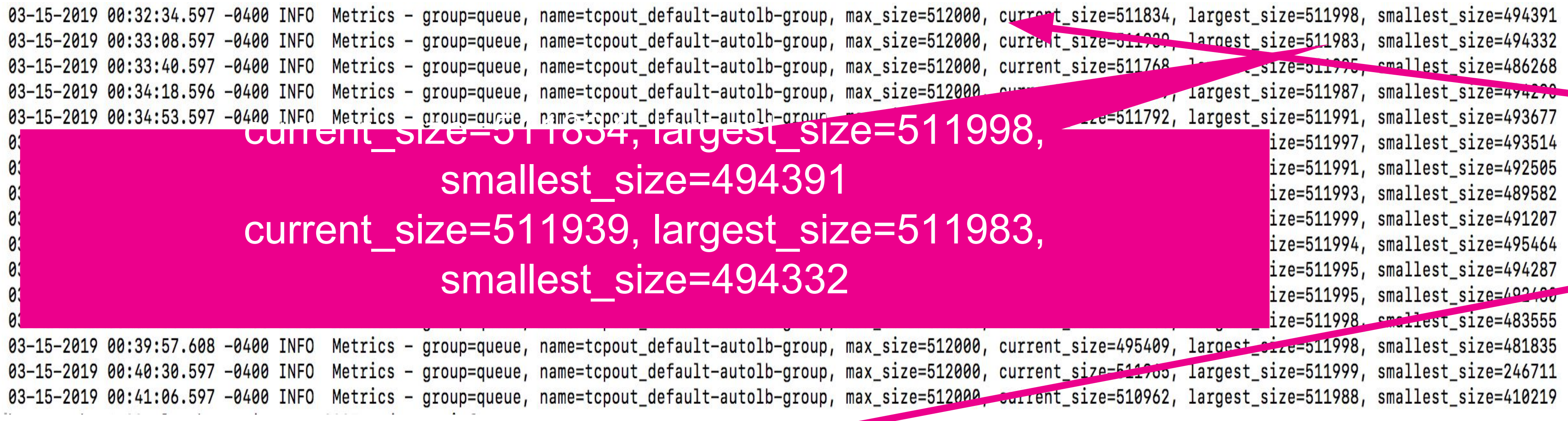
Debugging blocked tcpout queue

Troubleshoot blocked ingestion pipeline queues

Live troubleshooting Tcpout queue

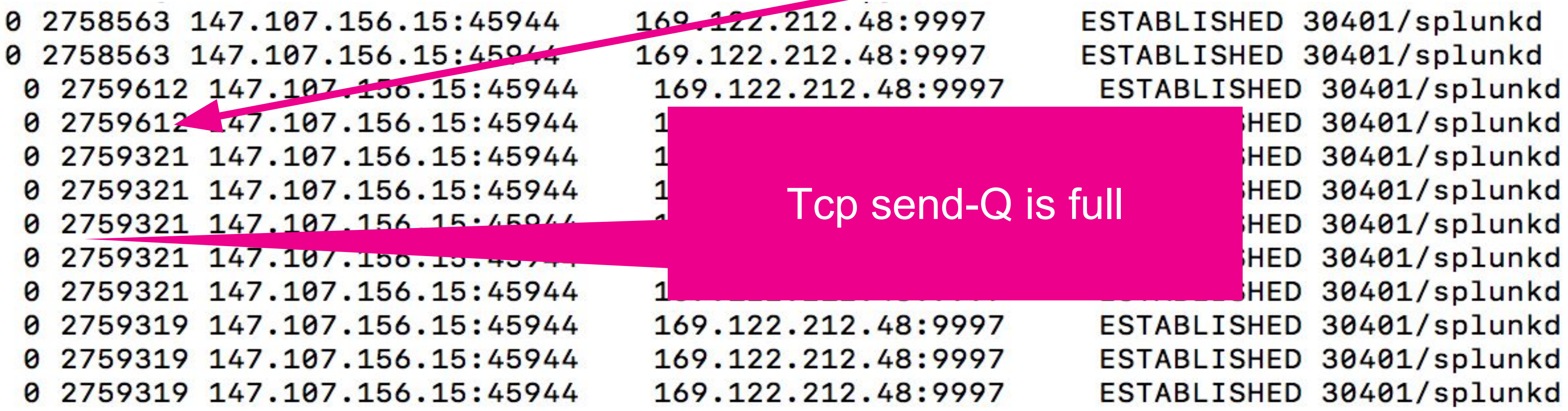
Troubleshooting Blocked Tcpout queue

>grep name=tcpout_ metrics.log



```
03-15-2019 00:32:34.597 -0400 INFO  Metrics - group=queue, name=tcpout_default-autolb-group, max_size=512000, current_size=511834, largest_size=511998, smallest_size=494391
03-15-2019 00:33:08.597 -0400 INFO  Metrics - group=queue, name=tcpout_default-autolb-group, max_size=512000, current_size=511939, largest_size=511983, smallest_size=494332
03-15-2019 00:33:40.597 -0400 INFO  Metrics - group=queue, name=tcpout_default-autolb-group, max_size=512000, current_size=511768,                                smallest_size=486268
03-15-2019 00:34:18.596 -0400 INFO  Metrics - group=queue, name=tcpout_default-autolb-group, max_size=512000,                      largest_size=511987, smallest_size=494290
03-15-2019 00:34:53.597 -0400 INFO  Metrics - group=queue, name=tcpout_default-autolb-group,                   ize=511792, largest_size=511991, smallest_size=493677
03                                                                                                                          ize=511997, smallest_size=493514
03                                                                                                                          ize=511991, smallest_size=492505
03                                                                                                                          ize=511993, smallest_size=489582
03                                                                                                                          ize=511999, smallest_size=491207
03                                                                                                                          ize=511994, smallest_size=495464
03                                                                                                                          ize=511995, smallest_size=494287
03                                                                                                                          ize=511995, smallest_size=49
03                                                                                                                          ize=511998, smallest_size=483555
03-15-2019 00:39:57.608 -0400 INFO  Metrics - group=queue, name=tcpout_default-autolb-group, max_size=512000, current_size=495409, largest_size=511998, smallest_size=481835
03-15-2019 00:40:30.597 -0400 INFO  Metrics - group=queue, name=tcpout_default-autolb-group, max_size=512000, current_size=511, largest_size=511999, smallest_size=246711
03-15-2019 00:41:06.597 -0400 INFO  Metrics - group=queue, name=tcpout_default-autolb-group, max_size=512000, current_size=510962, largest_size=511988, smallest_size=410219
```

current_size=511834, largest_size=511998,
smallest_size=494391
current_size=511939, largest_size=511983,
smallest_size=494332



```
 0 2758563 147.107.156.15:45944    169.122.212.48:9997     ESTABLISHED 30401/splunkd
 0 2758563 147.107.156.15:45944    169.122.212.48:9997     ESTABLISHED 30401/splunkd
  0 2759612 147.107.156.15:45944    169.122.212.48:9997     ESTABLISHED 30401/splunkd
  0 2759612 147.107.156.15:45944    1                            HED 30401/splunkd
  0 2759321 147.107.156.15:45944    1                            HED 30401/splunkd
  0 2759321 147.107.156.15:45944    1                            HED 30401/splunkd
  0 2759321 147.107.156.15:45944    1                            HED 30401/splunkd
  0 2759321 147.107.156.15:45944    1                            HED 30401/splunkd
  0 2759321 147.107.156.15:45944    1                            HED 30401/splunkd
  0 2759319 147.107.156.15:45944    169.122.212.48:9997     ESTABLISHED 30401/splunkd
  0 2759319 147.107.156.15:45944    169.122.212.48:9997     ESTABLISHED 30401/splunkd
  0 2759319 147.107.156.15:45944    169.122.212.48:9997     ESTABLISHED 30401/splunkd
```

Tcp send-Q is full

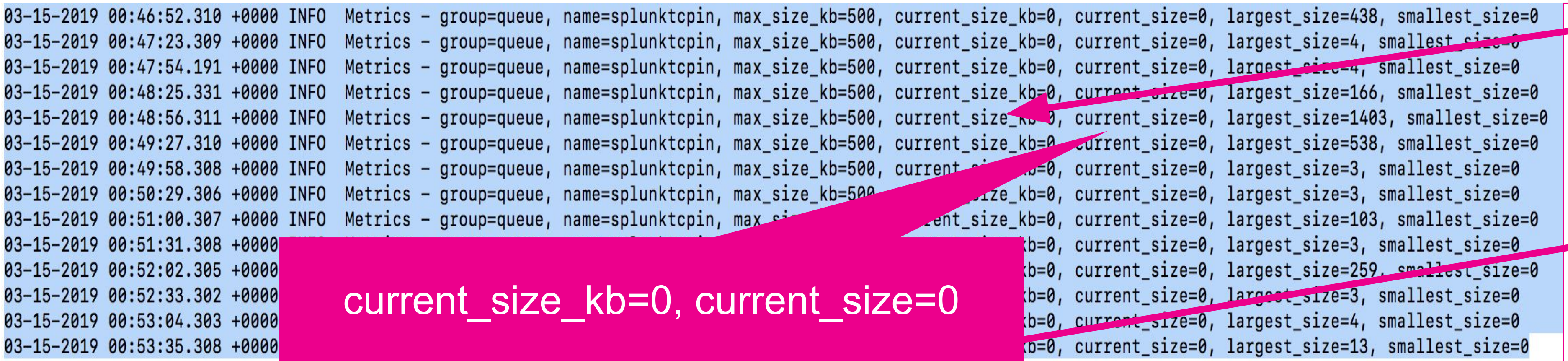
- tcpout queue is full.
- netstat –an |grep :9997
- tcp layer send buffer is also full.

- If TcpoutputQ is blocked. It’s very likely tcp send-Q is also full(netstat output)

Live troubleshooting Tcpin queue

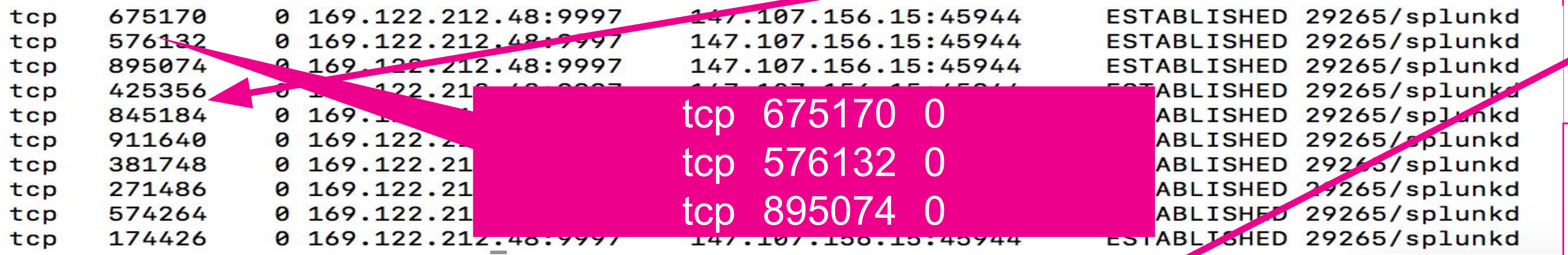
Troubleshooting Blocked Tcpout queue

grep tcpin metrics.log | grep group=queue



```
03-15-2019 00:46:52.310 +0000 INFO  Metrics - group=queue, name=splunktcpin, max_size_kb=500, current_size_kb=0, current_size=0, largest_size=438, smallest_size=0
03-15-2019 00:47:23.309 +0000 INFO  Metrics - group=queue, name=splunktcpin, max_size_kb=500, current_size_kb=0, current_size=0, largest_size=4, smallest_size=0
03-15-2019 00:47:54.191 +0000 INFO  Metrics - group=queue, name=splunktcpin, max_size_kb=500, current_size_kb=0, current_size=0, largest_size=4, smallest_size=0
03-15-2019 00:48:25.331 +0000 INFO  Metrics - group=queue, name=splunktcpin, max_size_kb=500, current_size_kb=0, current_size=0, largest_size=166, smallest_size=0
03-15-2019 00:48:56.311 +0000 INFO  Metrics - group=queue, name=splunktcpin, max_size_kb=500, current_size_kb=0, current_size=0, largest_size=1403, smallest_size=0
03-15-2019 00:49:27.310 +0000 INFO  Metrics - group=queue, name=splunktcpin, max_size_kb=500, current_size_kb=0, current_size=0, largest_size=538, smallest_size=0
03-15-2019 00:49:58.308 +0000 INFO  Metrics - group=queue, name=splunktcpin, max_size_kb=500, current_     _kb=0, current_size=0, largest_size=3, smallest_size=0
03-15-2019 00:50:29.306 +0000 INFO  Metrics - group=queue, name=splunktcpin, max_size_kb=500        ize_kb=0, current_size=0, largest_size=3, smallest_size=0
03-15-2019 00:51:00.307 +0000 INFO  Metrics - group=queue, name=splunktcpin, max_si           ent_size_kb=0, current_size=0, largest_size=103, smallest_size=0
03-15-2019 00:51:31.308 +0000                                                                  kb=0, current_size=0, largest_size=3, smallest_size=0
03-15-2019 00:52:02.305 +0000                                                                  kb=0, current_size=0, largest_size=259, smallest_size=0
03-15-2019 00:52:33.302 +0000                                                                  kb=0, current_size=0, largest_size=3, smallest_size=0
03-15-2019 00:53:04.303 +0000                                                                  kb=0, current_size=0, largest_size=4, smallest_size=0
03-15-2019 00:53:35.308 +0000                                                                  kb=0, current_size=0, largest_size=13, smallest_size=0
```

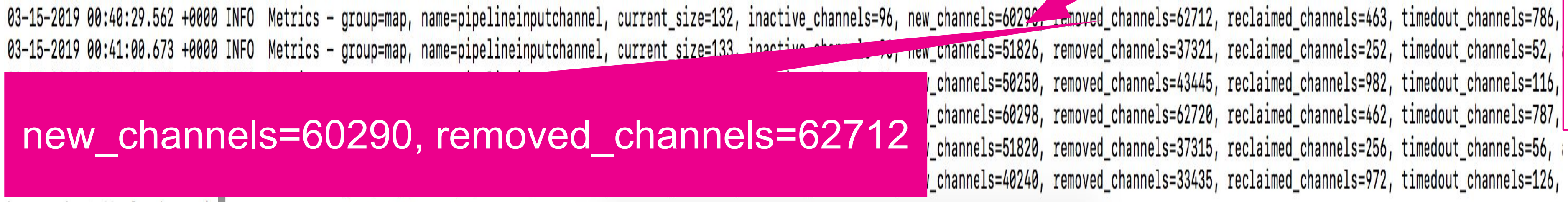
current_size_kb=0, current_size=0



```
tcp    675170    0 169.122.212.48:9997    147.107.156.15:45944    ESTABLISHED 29265/splunkd
tcp    576132    0 169.122.212.48:9997    147.107.156.15:45944    ESTABLISHED 29265/splunkd
tcp    895074    0 169.122.212.48:9997    147.107.156.15:45944    ESTABLISHED 29265/splunkd
tcp    425356    0 169.122.21                                         ABLISHED 29265/splunkd
tcp    845184    0 169.1                                              ABLISHED 29265/splunkd
tcp    911640    0 169.122.2                                          ABLISHED 29265/splunkd
tcp    381748    0 169.122.21                                         ABLISHED 29265/splunkd
tcp    271486    0 169.122.21                                         ABLISHED 29265/splunkd
tcp    574264    0 169.122.21                                         ABLISHED 29265/splunkd
tcp    174426    0 169.122.212.48:9997    147.107.156.15:45944    ESTABLISHED 29265/splunkd
```

tcp 675170 0
tcp 576132 0
tcp 895074 0

grep name=pipelineinputchannel metrics.log



```
03-15-2019 00:40:29.562 +0000 INFO  Metrics - group=map, name=pipelineinputchannel, current_size=132, inactive_channels=96, new_channels=60290, removed_channels=62712, reclaimed_channels=463, timedout_channels=786,
03-15-2019 00:41:00.673 +0000 INFO  Metrics - group=map, name=pipelineinputchannel, current_size=133,                new_channels=51826, removed_channels=37321, reclaimed_channels=252, timedout_channels=52,
                                                                                                              _channels=50250, removed_channels=43445, reclaimed_channels=982, timedout_channels=116,
                                                                                                              _channels=60298, removed_channels=62720, reclaimed_channels=462, timedout_channels=787,
                                                                                                              _channels=51820, removed_channels=37315, reclaimed_channels=256, timedout_channels=56,
                                                                                                              _channels=40240, removed_channels=33435, reclaimed_channels=972, timedout_channels=126,
```

new_channels=60290, removed_channels=62712

- tcpin queue is empty.
- tcp layer receive buffer is full.
- TcpInputProcessor is busy.

- Tune autoLBFrequency on forwarder to reduce channels.

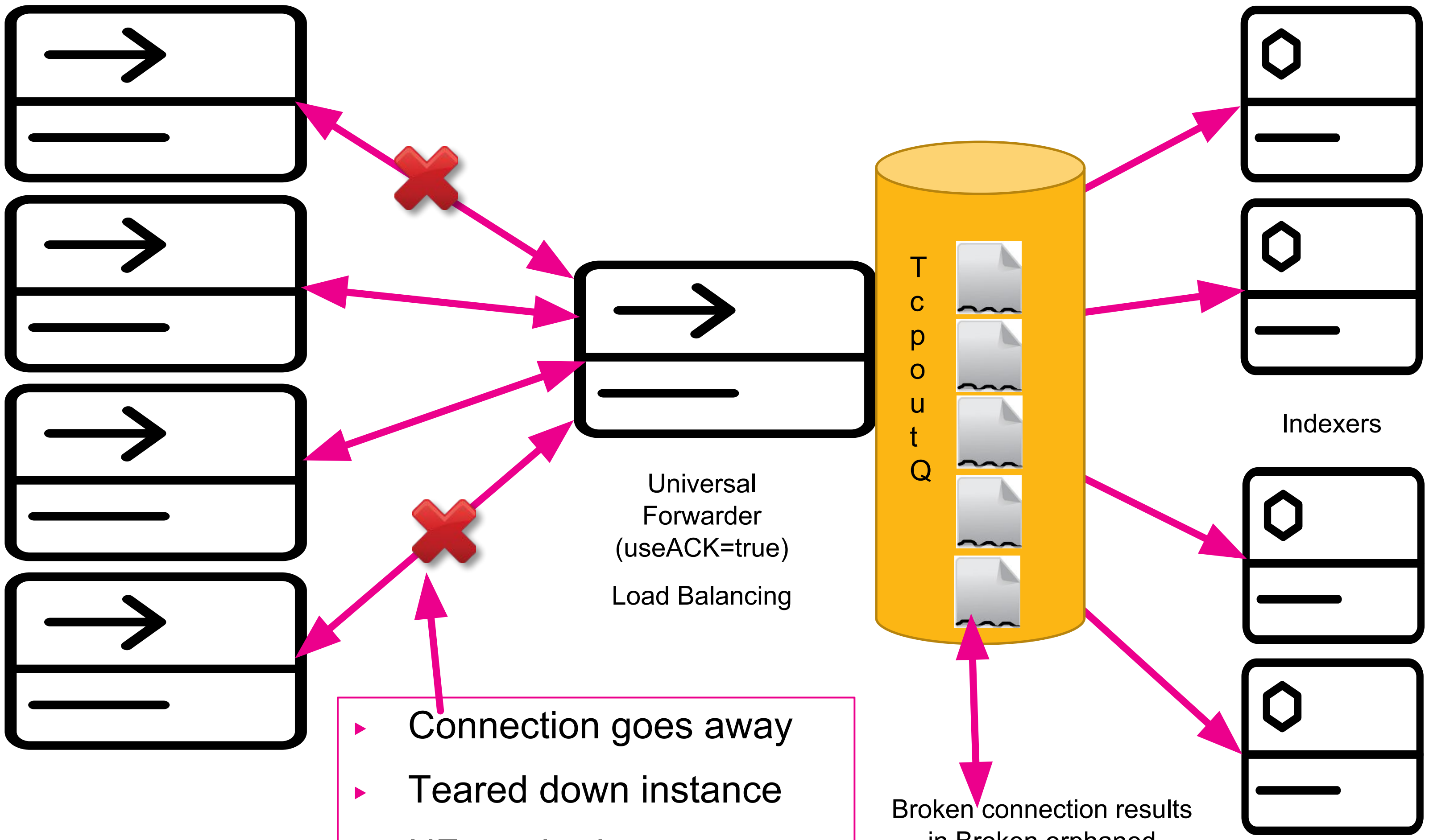
splunk> .conf19

Debugging blocked queue/missing broken events

Troubleshoot blocked ingestion pipeline queues

Debugging blocked queue

Troubleshooting Blocked Tcpout queue/Orphaned Broken events



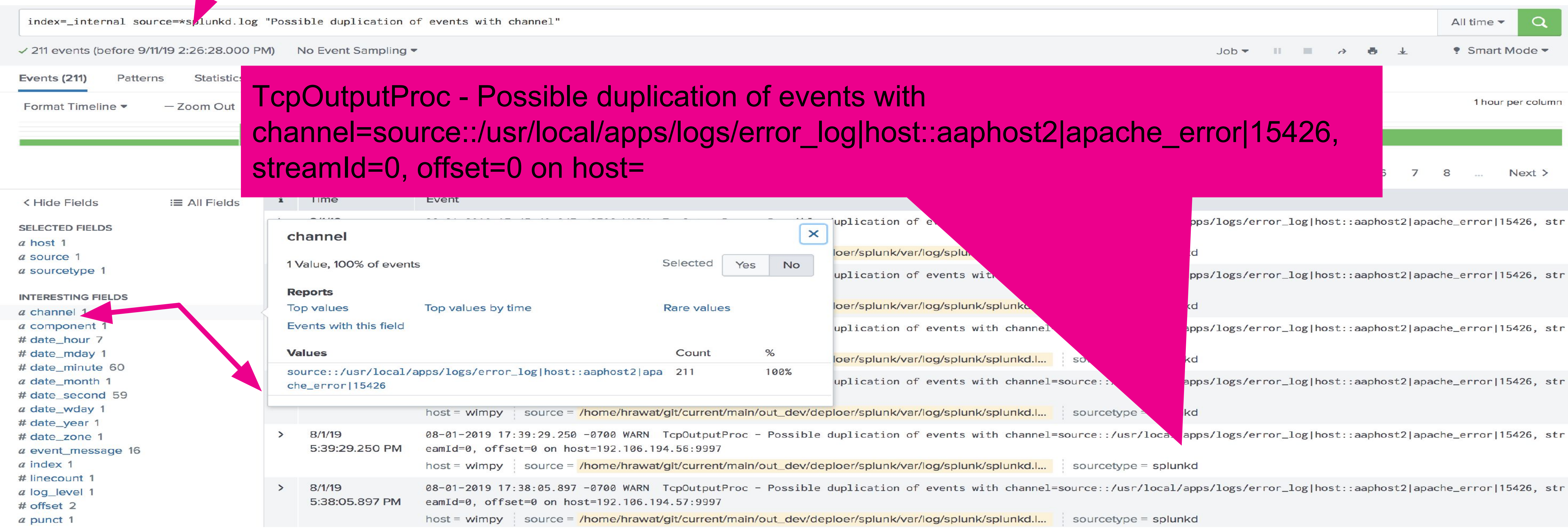
- Connection goes away
- Teared down instance
- UF crashed

Broken connection results in Broken orphaned missing pData stuck in TcpoutQ.

Detect broken missing events

Troubleshooting Blocked Tcpout queue/Orphaned Broken events

Query to detect broken events stuck in tcpoutQ



```
index=_internal source=*splunkd.log "Possible duplication of events with channel"
```

✓ 211 events (before 9/11/19 2:26:28.000 PM)   No Event Sampling ▾

TcpOutputProc - Possible duplication of events with channel=source::/usr/local/apps/logs/error_log|host::aaphost2|apache_error|15426, streamId=0, offset=0 on host=

SELECTED FIELDS
- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS
- a channel 1
- a component 1
- # date_hour 7
- # date_mday 1
- # date_minute 60
- a date_month 1
- # date_second 59
- a date_wday 1
- # date_year 1
- # date_zone 16
- a event_message 16
- a index 1
- # linecount 1
- a log_level 1
- # offset 2
- a punct 1

channel

1 Value, 100% of events   Selected Yes No

Reports
Top values   Top values by time   Rare values
Events with this field

Values	Count	%
source::/usr/local/apps/logs/error_log|host::aaphost2|apache_error|15426	211	100%

```
8/1/19       08-01-2019 17:39:29.250 -0700 WARN  TcpOutputProc - Possible duplication of events with channel=source::/usr/loca  apps/logs/error_log|host::aaphost2|apache_error|15426, str
5:39:29.250 PM  eamId=0, offset=0 on host=192.106.194.56:9997
             host = wimpy   source = /home/hrawat/git/current/main/out_dev/deploer/splunk/var/log/splunk/splunkd.l...   sourcetype = splunkd
8/1/19       08-01-2019 17:38:05.897 -0700 WARN  TcpOutputProc - Possible duplication of events with channel=source::/usr/local/apps/logs/error_log|host::aaphost2|apache_error|15426, str
5:38:05.897 PM  eamId=0, offset=0 on host=192.106.194.57:9997
             host = wimpy   source = /home/hrawat/git/current/main/out_dev/deploer/splunk/var/log/splunk/splunkd.l...   sourcetype = splunkd
```

Solution - use Heavy Forwarder (useACK=true) as intermediate forwarder(Load Balancing)

.conf19

splunk>

Thank You!

Go to the .conf19 mobile app to

RATE THIS SESSION