



How splunkd works

splunkd: Pipelines, Processors, Queues

Inputs: File, Network, Script, HEC, S2S, ...

Debugging: Metrics, Monitoring Console

by Amrit Bath, Abhinav Nekkanti

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance 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 could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. 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 functionality described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Listen to Your Data, 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. © 2017 Splunk Inc. All rights reserved.

About Us

► Amrit Bath (2005) – Engineer

- CLI, Deployment Server, Tailing, REST API, Universal Forwarder, Indexed Extractions, Cloud, SHC, Metrics, ...
- Previously: College
- Hates working on cars
- Owns Bud Light pants

► Abhinav Nekkanti (2013) – Engineer

- Tailing, Pipeline Parallelization, Alerts improvements, Preview improvements, Cloud
- Previously: Citrix (Goto products)
- Size 14 shoe
- Overly enthusiastic about Bud Light tallboys

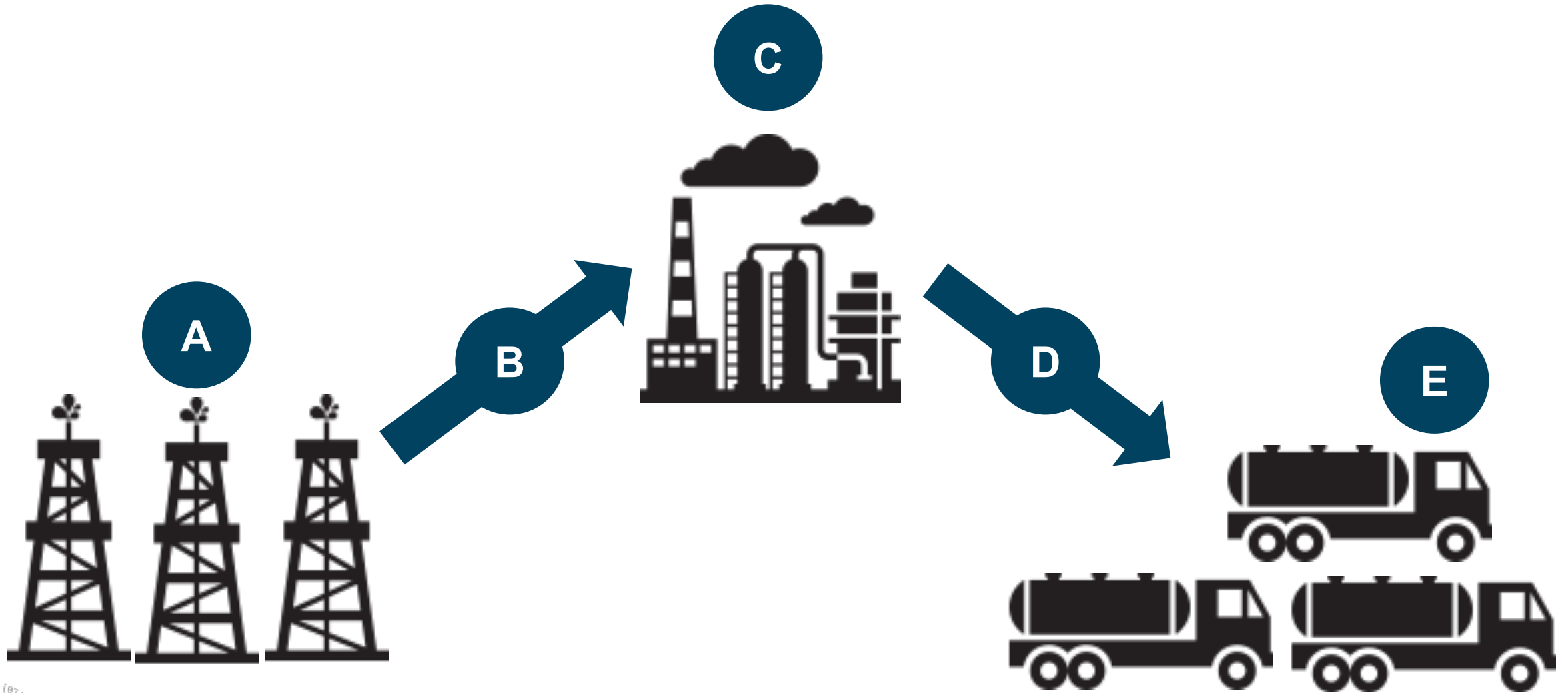


```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L9FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-5W-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CB-01"
ows NT 5.1; SV1: .NET CLR 1.1.4322" 468 125.17 14. - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3"
itemId=EST-16&product_id=RP-LI-02" 468 125.17 14. - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-18&product_id=AV-CB-01"
action=purchase&itemId=EST-18&product_id=AV-CB-01" 468 125.17 14. - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product_id=AV-CB-01"

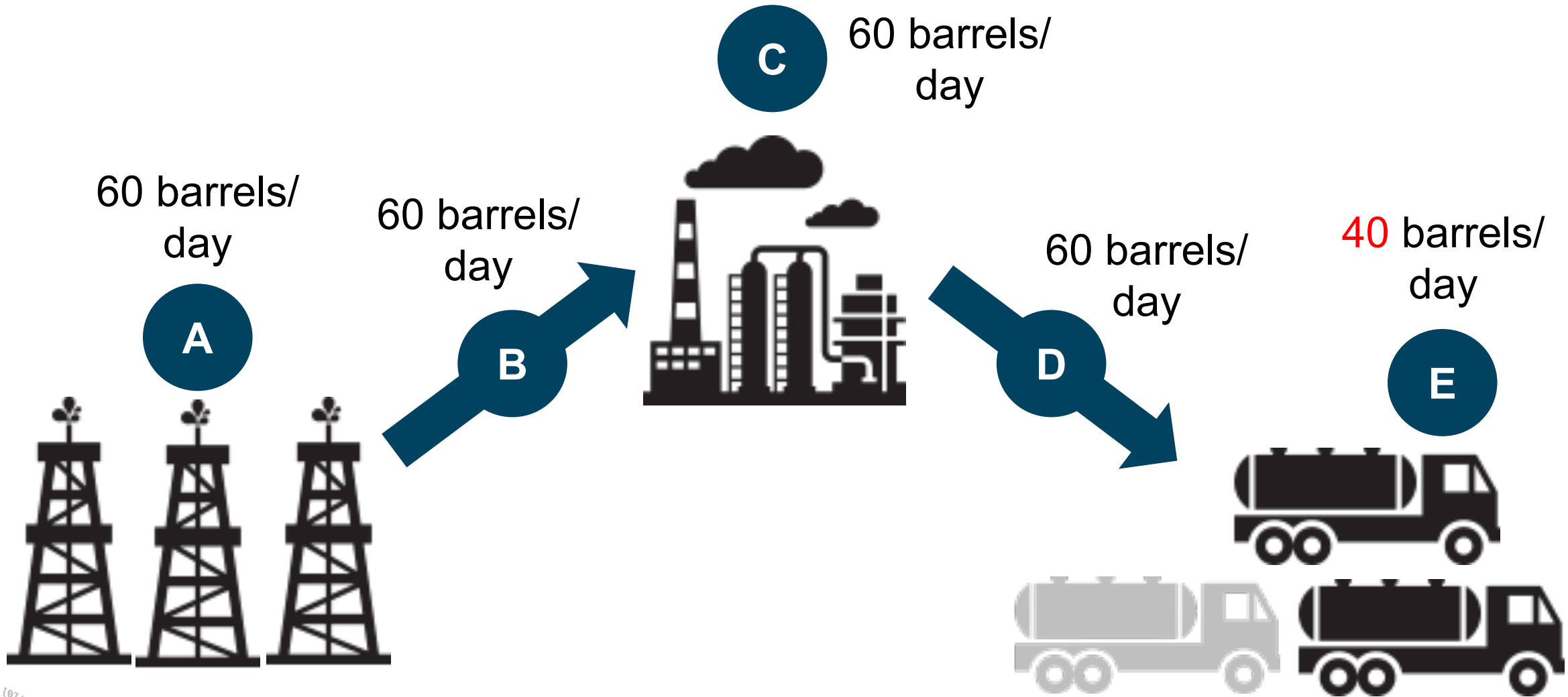
```


It's all a pipeline



```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.10.10.10  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FFGADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.10.10.10  
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.10.10.10  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FFGADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.10.10.10  
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.10.10.10  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FFGADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.10.10.10
```


It's all a pipeline



```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_2; rv:53.0) Gecko/20100801 Firefox/53.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD3SL7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CB-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_2; rv:53.0) Gecko/20100801 Firefox/53.0"
317.27.160.0 - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD3SL7FF6ADFF0 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SL9FF1ADFF3" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_2; rv:53.0) Gecko/20100801 Firefox/53.0"
10.0.0.0 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product_id=AV-CB-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_2; rv:53.0) Gecko/20100801 Firefox/53.0"
10.0.0.0 - - [07/Jan 18:10:55:189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product_id=AV-CB-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_2; rv:53.0) Gecko/20100801 Firefox/53.0"
```


Data structures & Routing

Pipeline Data

_conf	www2, access_log, /var/log/httpd/access_log		
Host	www2		
Index	prod_servers		
...	...		
_raw	10.3.1.92 - - [21/Jul/2011:20:34:44 -0700] "GET /results/bonnie-solns_vm_nick.html HTTP/1.1" 200 2938		
UTF-8 finished?	Line Breaker finished?

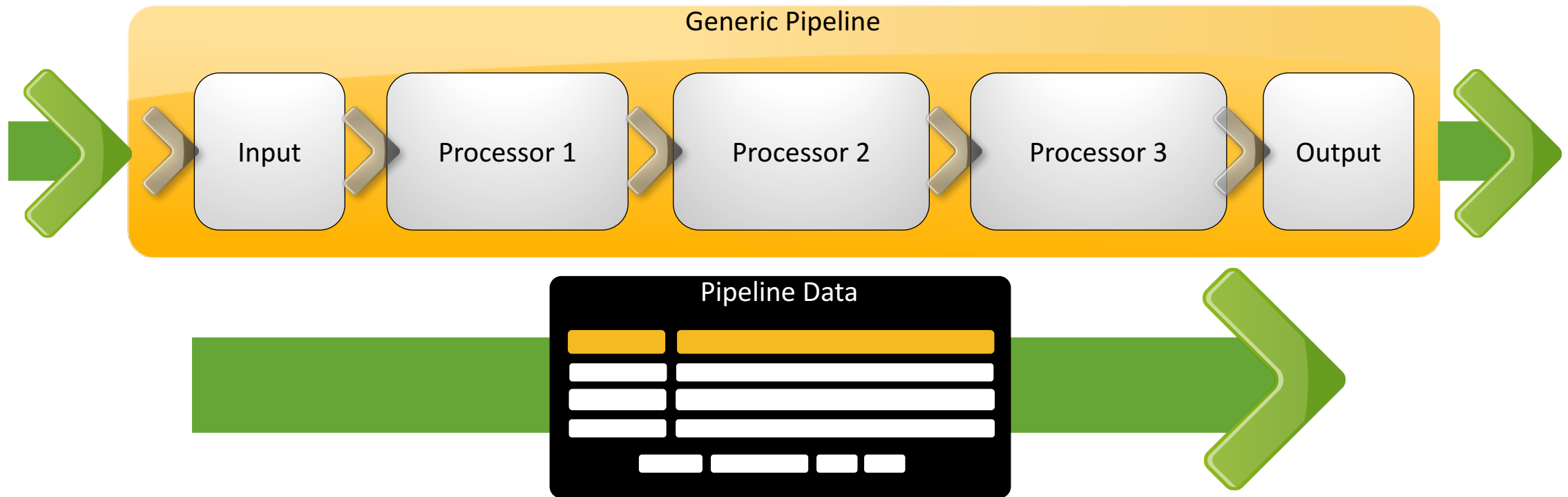
Processor



- Processor: Performs small but logical unit of work
- Contained within a Pipeline
- Examples: LineBreaker, Aggregator, TcpInput, Index

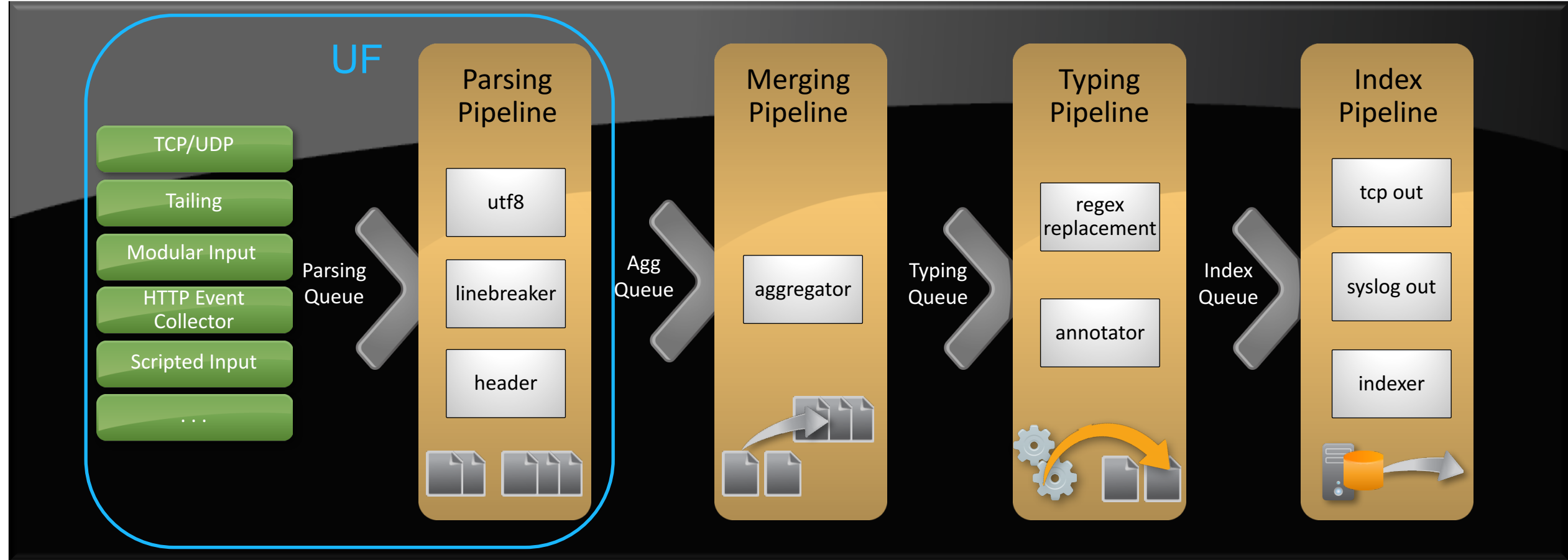
```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L9FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-5W-03" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.2.0) Gecko/20100101 Firefox/3.6"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CU-01" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.2.0) Gecko/20100101 Firefox/3.6"
317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CU-01&JSESSIONID=5D55L9FF1ADFF3" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.2.0) Gecko/20100101 Firefox/3.6"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D15L9FF10ADFF10 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.2.0) Gecko/20100101 Firefox/3.6"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CU-01&JSESSIONID=5D55L9FF1ADFF3" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.2.0) Gecko/20100101 Firefox/3.6"
317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CU-01&JSESSIONID=5D55L9FF1ADFF3" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.2.0) Gecko/20100101 Firefox/3.6"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D15L9FF10ADFF10 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.2.0) Gecko/20100101 Firefox/3.6"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CU-01&JSESSIONID=5D55L9FF1ADFF3" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.2.0) Gecko/20100101 Firefox/3.6"
317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CU-01&JSESSIONID=5D55L9FF1ADFF3" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.2.0) Gecko/20100101 Firefox/3.6"
```


Pipelines



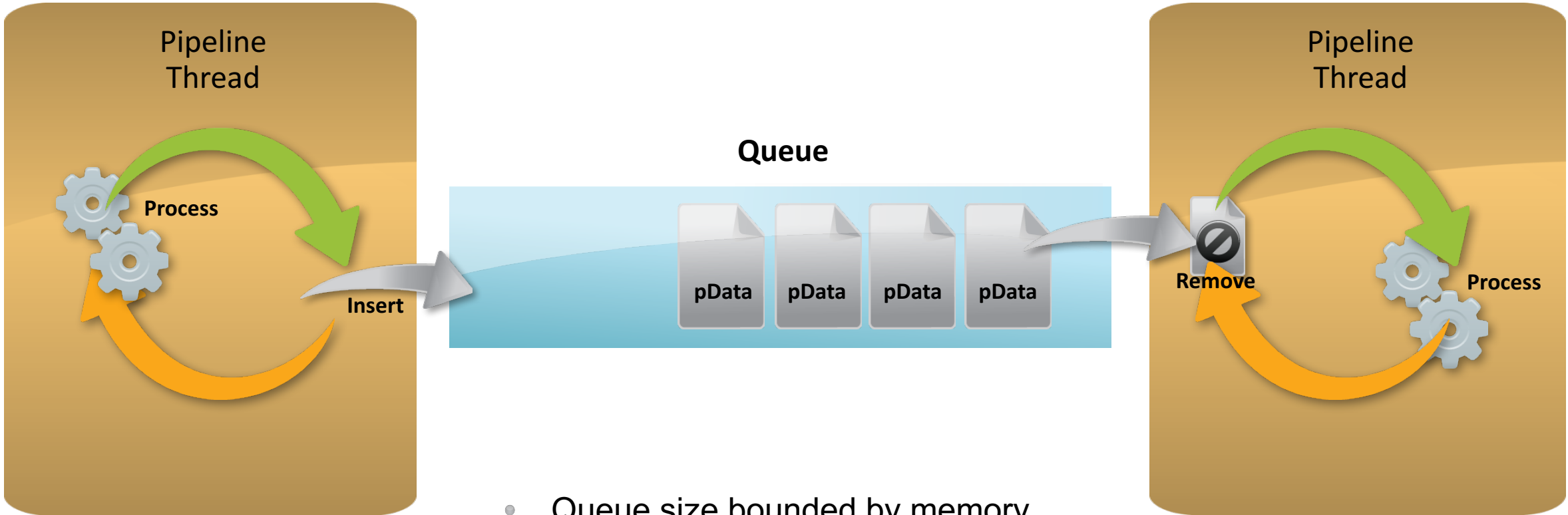
- Each pipeline runs in separate thread
- Naturally parallelized and modular
- Data flows linearly
- Configured in: `$SPLUNK_HOME/etc/modules/`
- Rendered to: `$SPLUNK_HOME/var/run/splunk/composite.xml`

Complete Ingestion Pipeline Set



```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-5W-03" "Mozilla/5.0 (Macintosh; Intel Mac OS X 11_0_0; rv:53.0) Gecko/20100801 Firefox/35.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&JSESSIONID=5D55L9FF1ADFF3" "Mozilla/5.0 (Macintosh; Intel Mac OS X 11_0_0; rv:53.0) Gecko/20100801 Firefox/35.0"
317.27.160.0.0 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&JSESSIONID=5D55L9FF1ADFF3" "Mozilla/5.0 (Macintosh; Intel Mac OS X 11_0_0; rv:53.0) Gecko/20100801 Firefox/35.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&JSESSIONID=5D55L9FF1ADFF3" "Mozilla/5.0 (Macintosh; Intel Mac OS X 11_0_0; rv:53.0) Gecko/20100801 Firefox/35.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&JSESSIONID=5D55L9FF1ADFF3" "Mozilla/5.0 (Macintosh; Intel Mac OS X 11_0_0; rv:53.0) Gecko/20100801 Firefox/35.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&JSESSIONID=5D55L9FF1ADFF3" "Mozilla/5.0 (Macintosh; Intel Mac OS X 11_0_0; rv:53.0) Gecko/20100801 Firefox/35.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&JSESSIONID=5D55L9FF1ADFF3" "Mozilla/5.0 (Macintosh; Intel Mac OS X 11_0_0; rv:53.0) Gecko/20100801 Firefox/35.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&JSESSIONID=5D55L9FF1ADFF3" "Mozilla/5.0 (Macintosh; Intel Mac OS X 11_0_0; rv:53.0) Gecko/20100801 Firefox/35.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&JSESSIONID=5D55L9FF1ADFF3" "Mozilla/5.0 (Macintosh; Intel Mac OS X 11_0_0; rv:53.0) Gecko/20100801 Firefox/35.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&JSESSIONID=5D55L9FF1ADFF3" "Mozilla/5.0 (Macintosh; Intel Mac OS X 11_0_0; rv:53.0) Gecko/20100801 Firefox/35.0"
```

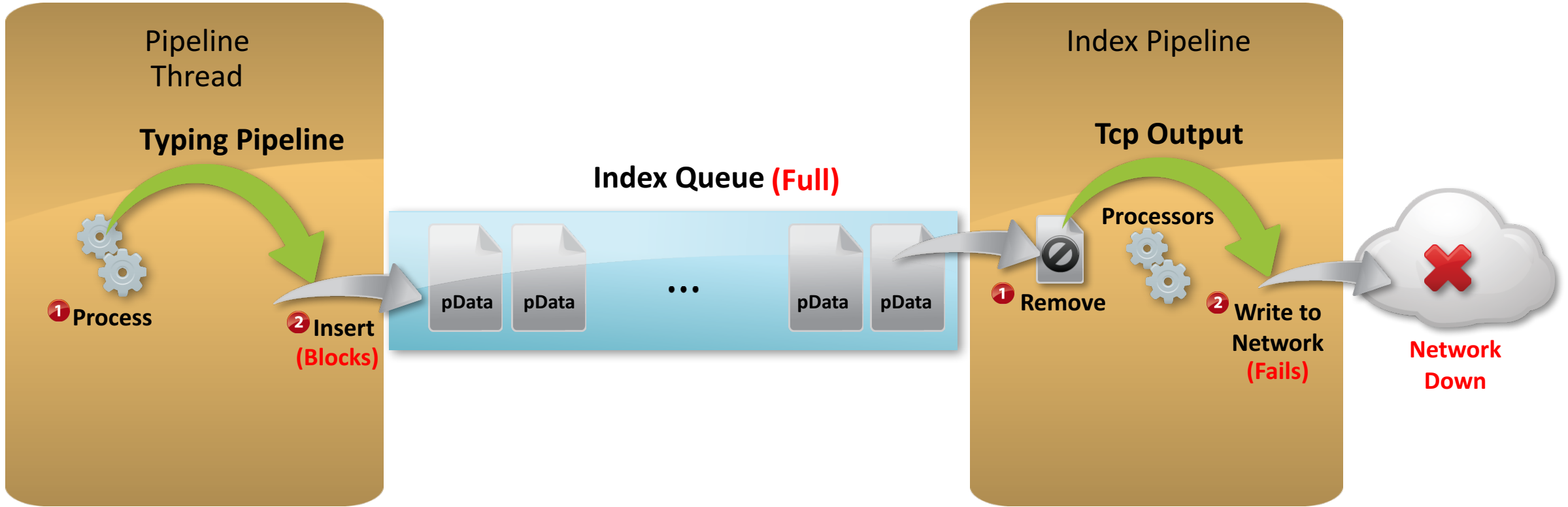
Queue



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

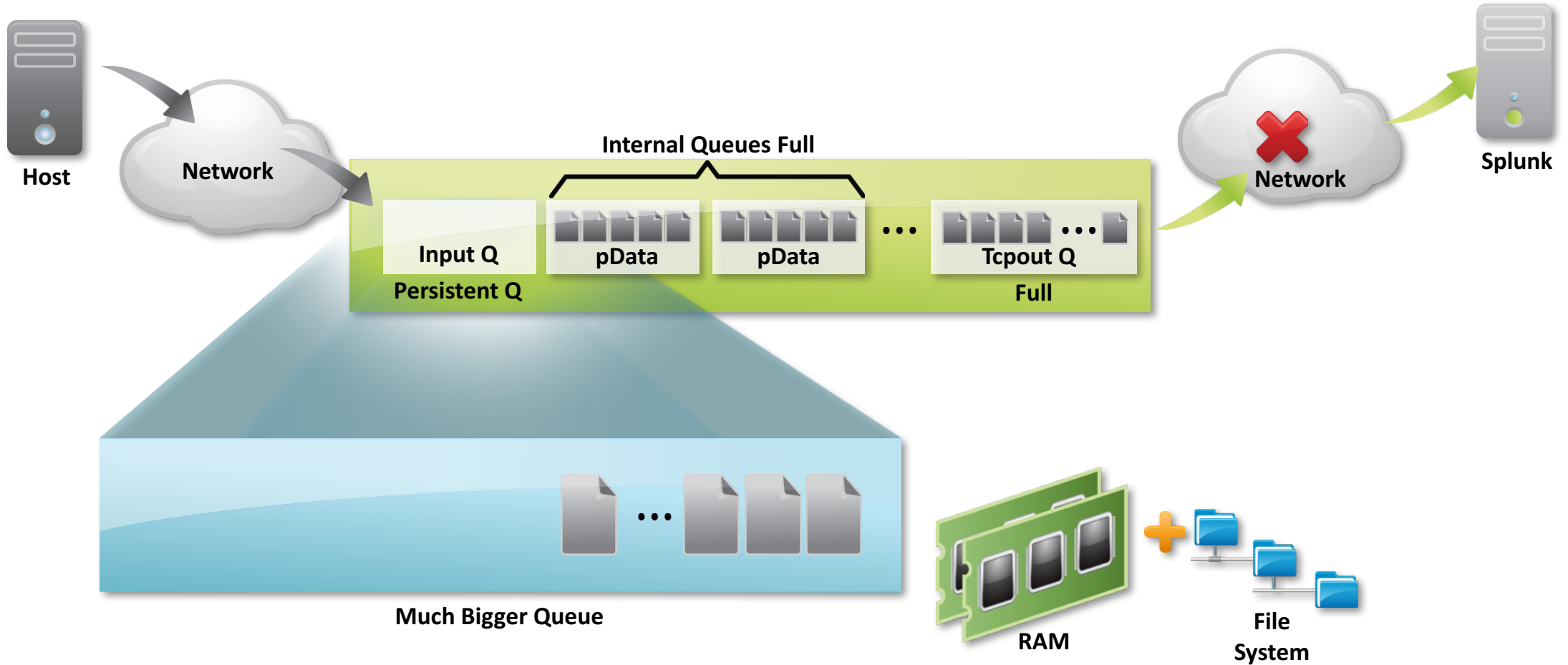
```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.2.0) Gecko/20100101 Firefox/3.6"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD35L7FFGADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K0-CB-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322) 468 125.17 14.1.0.0"
317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5L9FFIADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5L9FFIADFF3" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.2.0) Gecko/20100101 Firefox/3.6"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.2.0) Gecko/20100101 Firefox/3.6"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD35L7FFGADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K0-CB-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322) 468 125.17 14.1.0.0"
317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5L9FFIADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5L9FFIADFF3" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.2.0) Gecko/20100101 Firefox/3.6"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.2.0) Gecko/20100101 Firefox/3.6"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD35L7FFGADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K0-CB-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322) 468 125.17 14.1.0.0"
317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5L9FFIADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5L9FFIADFF3" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.2.0) Gecko/20100101 Firefox/3.6"
```

Queue



```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-5W-03" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.2.0) Gecko/20100101 Firefox/3.6"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=K0-CW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.1.1.1
317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.2.0) Gecko/20100101 Firefox/3.6"
10.0.0.1 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=K0-CW-01" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.2.0) Gecko/20100101 Firefox/3.6"
10.0.0.1 - - [07/Jan 18:10:55:189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product_id=AV-CB-01" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.2.0) Gecko/20100101 Firefox/3.6"
```

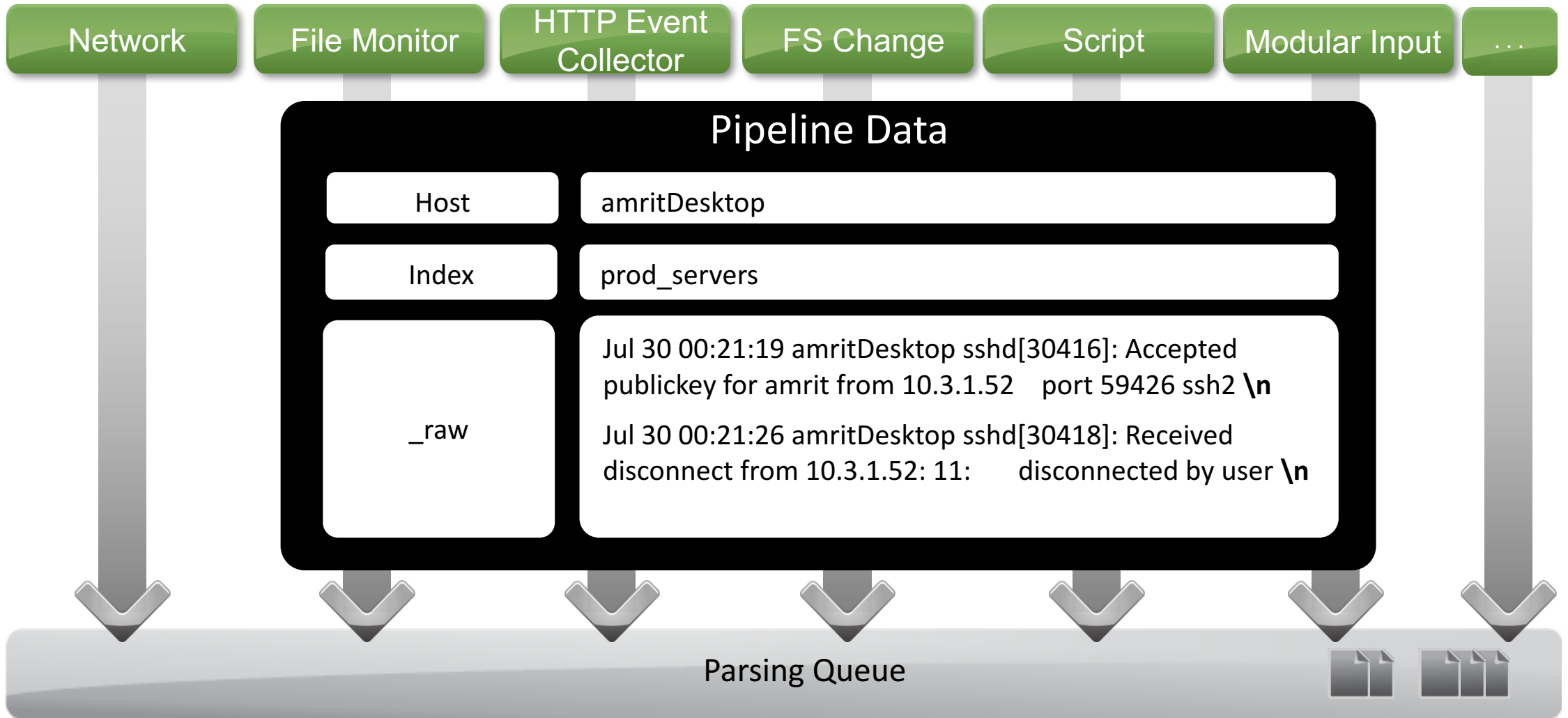
Persistent Queue



```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-5W-03" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_2; rv:53.0) Gecko/20100801 Firefox/53.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_2; rv:53.0) Gecko/20100801 Firefox/53.0"
317.27.160.0 - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L7FF6ADFF0 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L7FF6ADFF0" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_2; rv:53.0) Gecko/20100801 Firefox/53.0"
125.17.14.1 - - [07/Jan 18:10:55:187] "GET /cart.do?action=remove&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L7FF6ADFF0 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L7FF6ADFF0" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_2; rv:53.0) Gecko/20100801 Firefox/53.0"
125.17.14.1 - - [07/Jan 18:10:55:189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L7FF6ADFF0 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L7FF6ADFF0" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_2; rv:53.0) Gecko/20100801 Firefox/53.0"
```

Input Processors

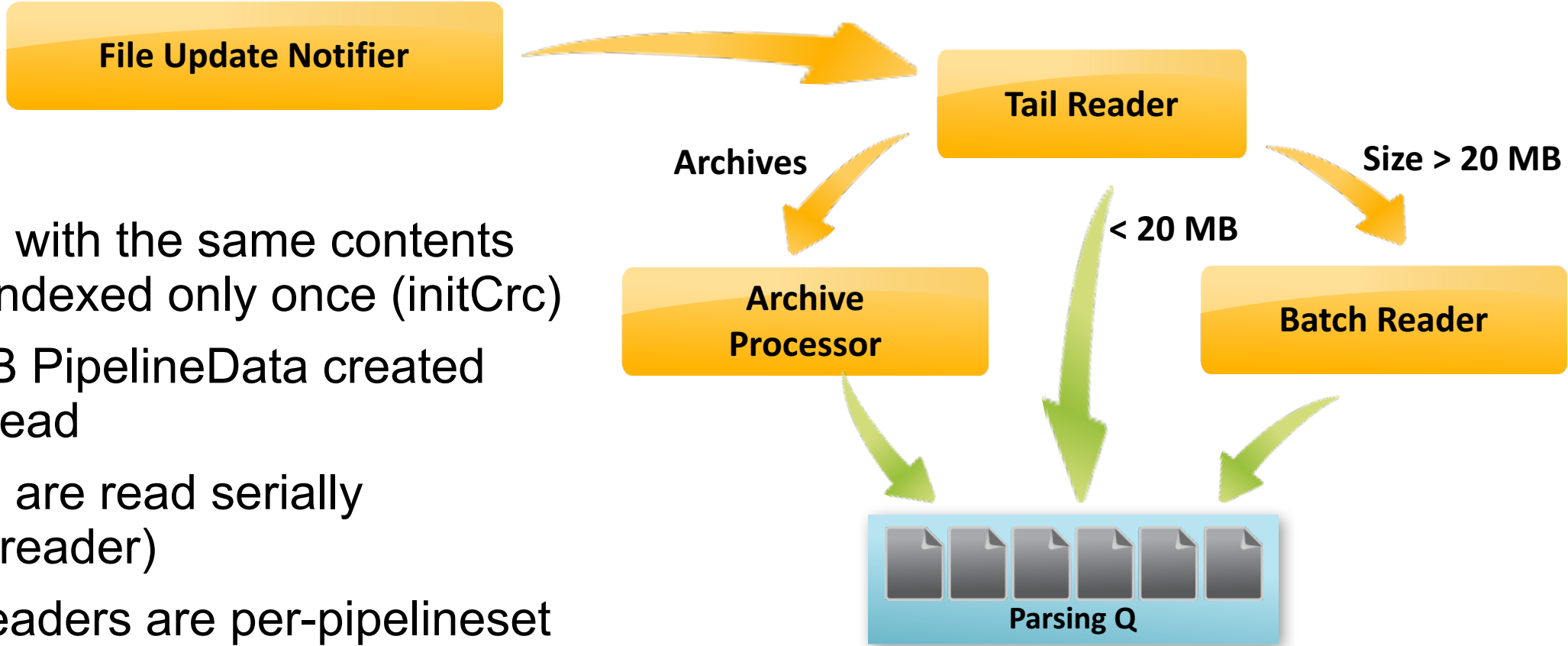
Input Pipelines



```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5SL9FFIADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.category_id=FI-SW-03 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=FI-SW-03"
317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FFGADFF0 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SL7FFGADFF0"
10.55.187 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FFIADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1189"
10.55.187 - - [07/Jan 18:10:56:156] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FFIADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1189"
10.55.187 - - [07/Jan 18:10:56:156] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FFIADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1189"
10.55.187 - - [07/Jan 18:10:56:156] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FFIADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1189"
10.55.187 - - [07/Jan 18:10:56:156] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FFIADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1189"
10.55.187 - - [07/Jan 18:10:56:156] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FFIADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1189"
10.55.187 - - [07/Jan 18:10:56:156] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FFIADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1189"
10.55.187 - - [07/Jan 18:10:56:156] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FFIADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1189"
  
```

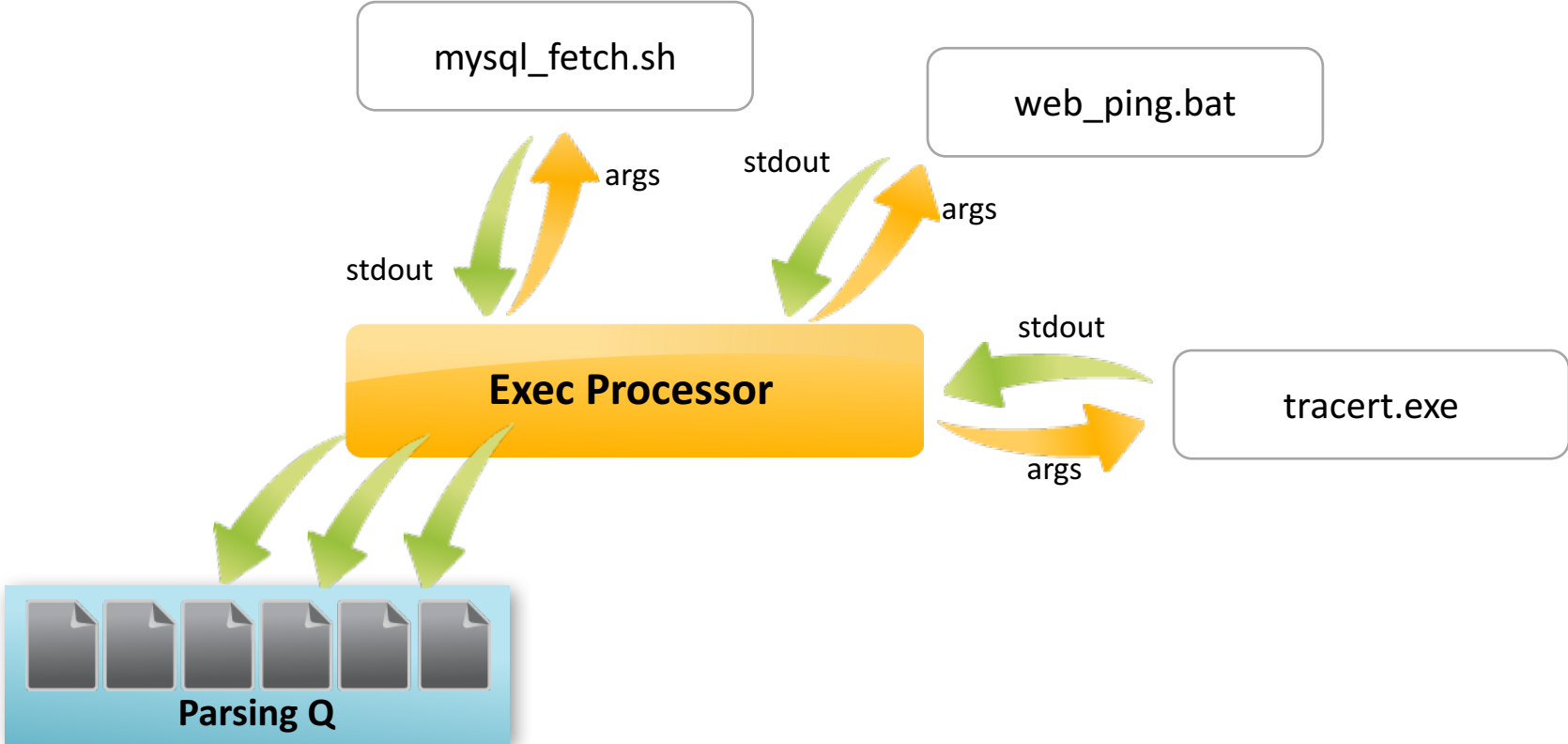
Tailing Processor (monitor input)



- Files with the same contents are indexed only once (initCrc)
- 64KB PipelineData created per read
- Files are read serially (per reader)
- All readers are per-pipelineset

```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-5W-03" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6; rv:53.0) Gecko/20100801 Firefox/53.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6; rv:53.0) Gecko/20100801 Firefox/53.0"
317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6; rv:53.0) Gecko/20100801 Firefox/53.0"
125.17.14 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6; rv:53.0) Gecko/20100801 Firefox/53.0"
125.17.14 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6; rv:53.0) Gecko/20100801 Firefox/53.0"
125.17.14 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6; rv:53.0) Gecko/20100801 Firefox/53.0"
125.17.14 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6; rv:53.0) Gecko/20100801 Firefox/53.0"
125.17.14 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6; rv:53.0) Gecko/20100801 Firefox/53.0"
125.17.14 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6; rv:53.0) Gecko/20100801 Firefox/53.0"
125.17.14 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6; rv:53.0) Gecko/20100801 Firefox/53.0"
```

Scripted Input



```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS"
317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&is.com/oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3"
125.17.14.1 - - [07/Jan 18:10:56:189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3"
10.0.55.187 - - [07/Jan 18:10:55:108] "GET /category.action=remove&itemId=EST-14&product_id=AV-CB-01&JSESSIONID=SD1B5L8FF2ADFF9 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/category.action=remove&itemId=EST-14&product_id=AV-CB-01&JSESSIONID=SD1B5L8FF2ADFF9"
```

Modular Input

```

<scheme>
  <title>S3 Input</title>
  <description>
    Index log files from AWS
    S3.
    ....
  </scheme>

```

aws_s3.py

aws_s3.py

data

args

Modular Input Processor

--scheme

Modular Input Processor



```

<stream>
  <event>
    <data> File 1 contents </data>
    <source> s3:/svc/Foo.gz
  </source>
    <time> 1474483334 </time>
  </event>
  ....
</stream>

```

1) Retrieve a configuration scheme

2) Generate data



HTTP Event Collector

https://splk-idx:8088/services/collector/event



Internet of Things



Servers



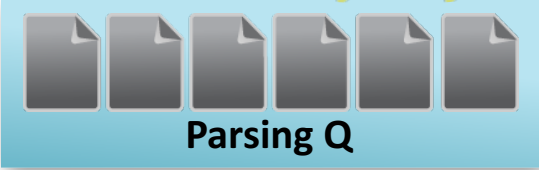
cloud



Network



HEC Processor



Parsing Q

```
{  
  "time": 1426279439, // epoch time  
  "host": "rasp_pi_270b",  
  "source": "temp_kegerator_4",  
  "sourcetype": "temp_sensor",  
  "index": "beer",  
  "event": { "keg_f=38 ambient_f=70" }  
}
```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-5W-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF9 HTTP 1.1" 404 3322 "http://shopping.com/cart.do?action=purchase&itemId=EST-268product_id=KQ-CW-01"
317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3"
10 - - [07/Jan 18:10:56:156] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://shopping.com/cart.do?action=purchase&itemId=EST-268product_id=KQ-CW-01"
10 - - [07/Jan 18:10:56:156] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://shopping.com/cart.do?action=purchase&itemId=EST-268product_id=KQ-CW-01"

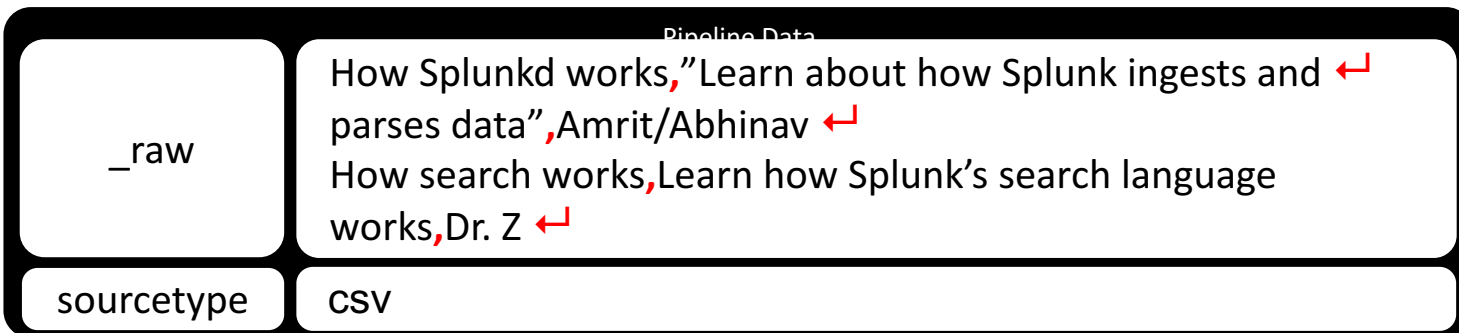
Mining Processors

We're getting there

OR Parsing: CSV/JSON Line Breaker (6.0+)

PRESENTATIONS.CSV

Subject ,	Description ,	Presenter ↵
How Splunkd works ,	"Learn about how Splunk ingests and parses data" ,	Amrit/Abhinav ↵
How search works ,	Learn how Splunk's search language works ,	Dr. Z ↵



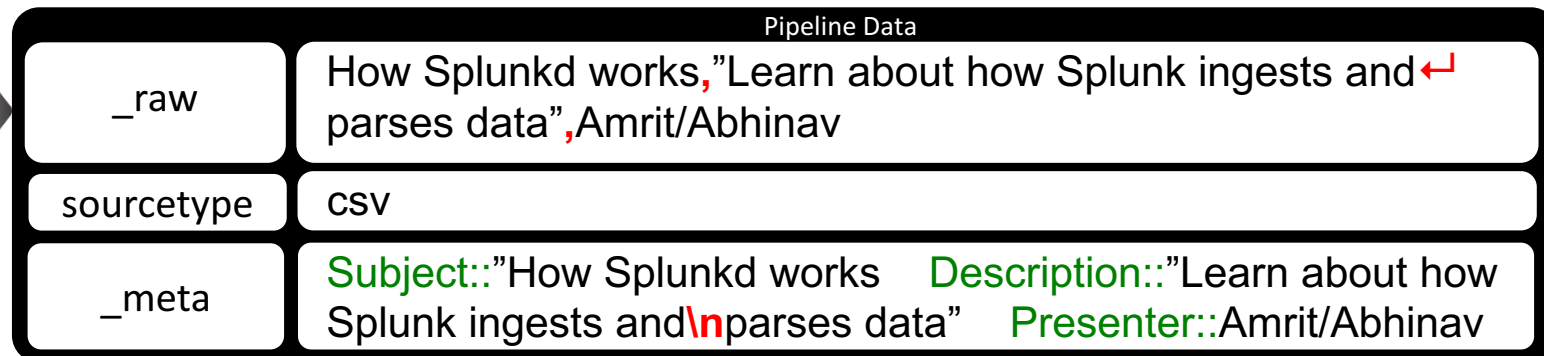
inputs.conf:

sourcetype = _json

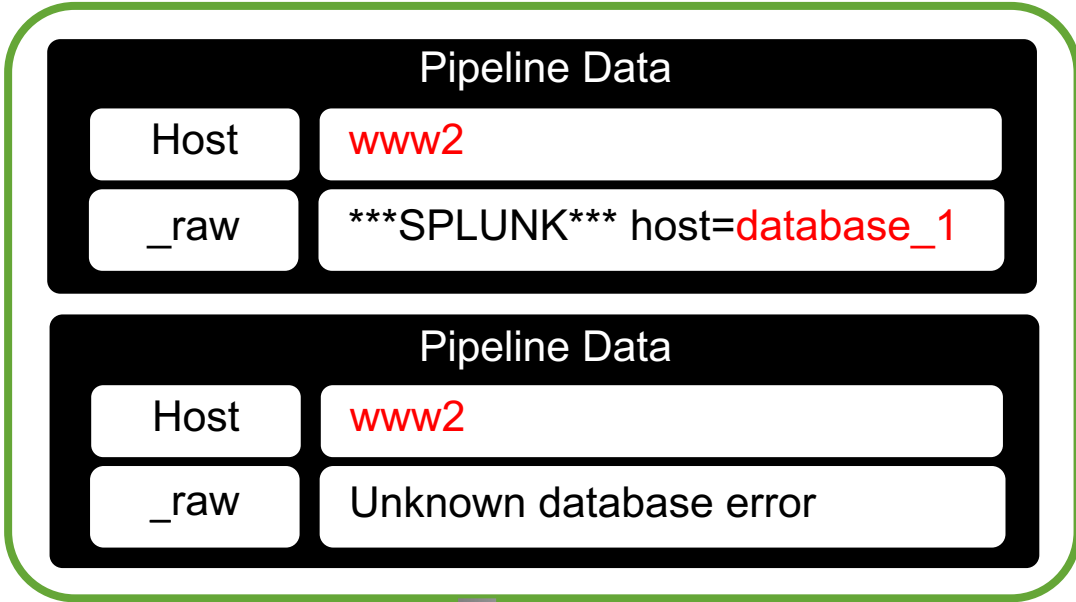
props.conf:

INDEXED_EXTRactions = (csv | json | ...)

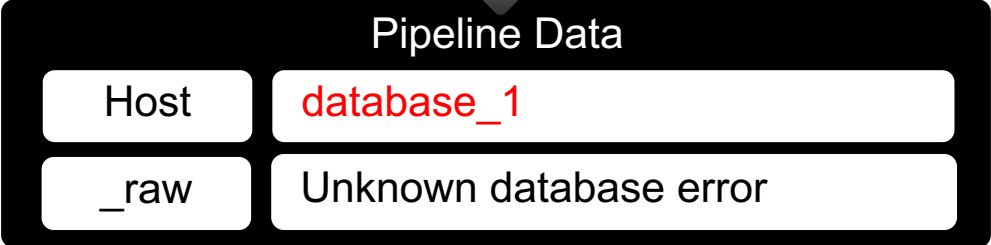
CSV/JSON Line
Breaker



Parsing: Header Processor



props.conf:
HEADER_MODE = (none | firstline | always)



130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L9FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.1.0.0
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=KQ-CW-0" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.1.0.0
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L9FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.1.0.0
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=KQ-CW-0" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.1.0.0
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L9FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.1.0.0
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=KQ-CW-0" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.1.0.0

Merging: Line Merge (aka Aggregator)

Pipeline Data

`_raw``Sep 12 06:11:58 abath-mba13.no.cox.net storeagent[49597] <Critical>: Starting update scan`

Pipeline Data

`_raw``Sep 12 06:11:58 abath-mba13.no.cox.net storeagent[49597] <Critical>: UpdateController: Message tracing {`

Pipeline Data

`_raw``"power_source" = ac;`

Pipeline Data

`_raw``"start_date" = "2014-08-21 20:10:39 +0000";`

⋮

Line Merge

Pipeline Data

`_raw``Sep 12 06:11:58 abath-mba13.no.cox.net storeagent[49597] <Critical>: Starting update scan`

Pipeline Data

`_raw``Sep 12 06:11:58 abath-mba13.no.cox.net storeagent[49597] <Critical>: UpdateController: Message tracing {``"power_source" = ac;``"start_date" = "2014-08-21 20:10:39 +0000";``}`

Pipeline Data

`_raw``Sep 12 06:11:58 abath-mba13.no.cox.net storeagent[49597] <Critical>: Asserted BackgroundTask power`

Typing: Regex Replacement

Pipeline Data

Host	logbox
Sourcetype	syslog
_raw	Sep 12 06:11:58 abath-mba13.no.cox.net storeagent[49597] <Critical>: Starting update scan

props.conf:

[syslog]

TRANSFORMS = syslog-host

transforms.conf:

[syslog-host]

DEST_KEY = MetaData:Host

FORMAT = host::\$1

REGEX = ... (...) ...

Regex Replacement

Pipeline Data

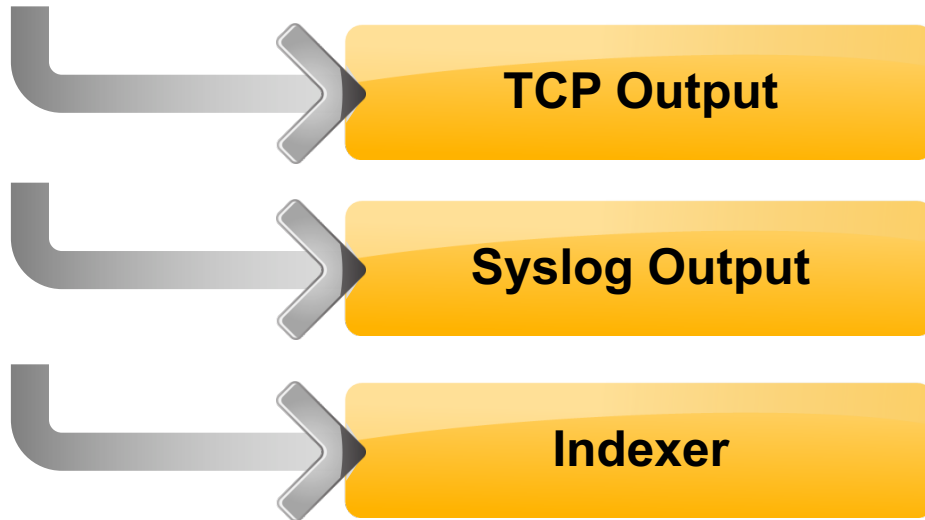
Host	abath-mba13.no.cox.net
Sourcetype	syslog
_raw	Sep 12 06:11:58 abath-mba13.no.cox.net storeagent[49597] <Critical>: Starting update scan

Index & Output Processors

We're still here...

Indexer Pipeline: Fwding, Indexing

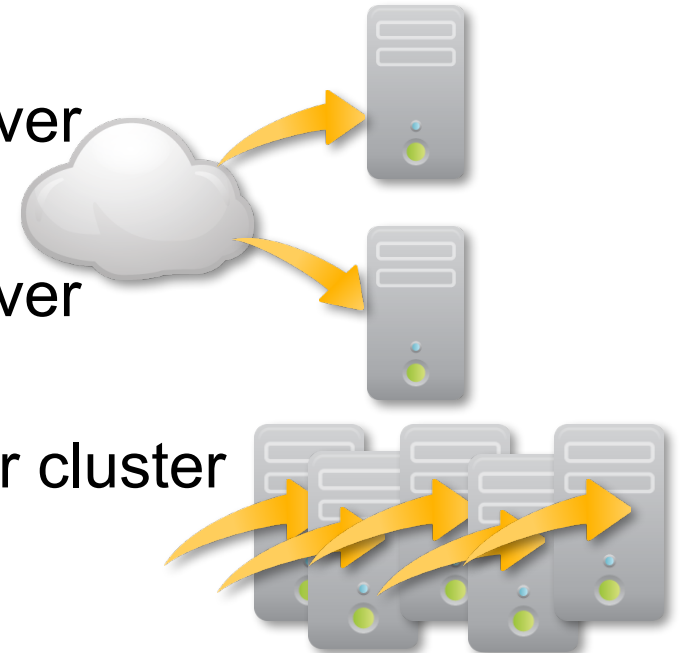
Pipeline Data	
Host	abath-mba13.no.cox.net
Index	main
_raw	Sep 12 06:11:58 abath-mba13.no.cox.net storeagent[49597] <Critical>: Starting update scan



To remote server

To remote server

To disk or cluster

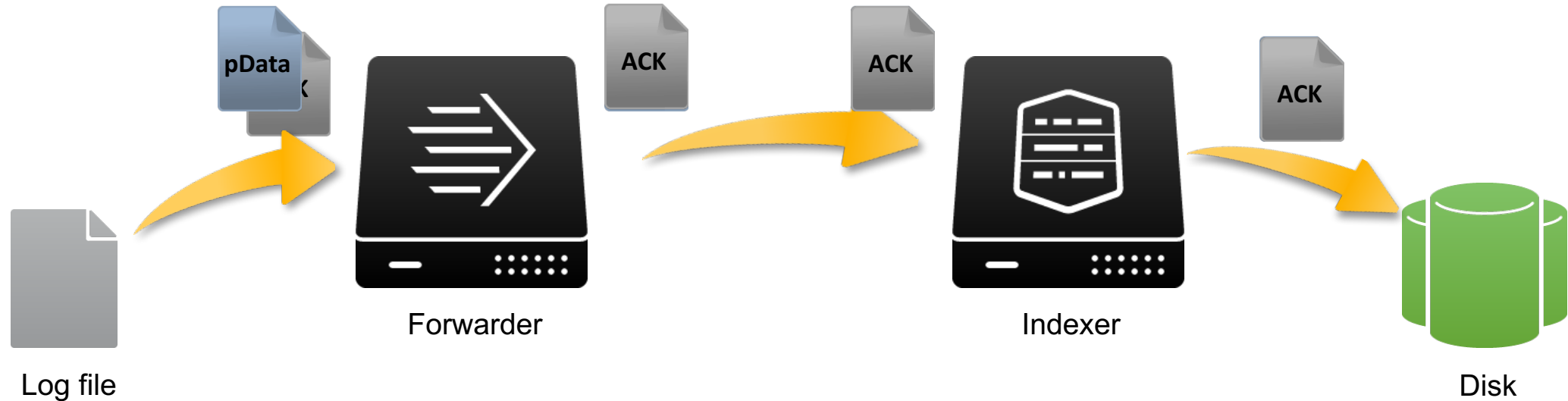


```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L9FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-5W-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=KQ-CU-01"
317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3"
10.0.0.0 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=RP-LI-02"
10.0.0.0 - - [07/Jan 18:10:55:189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://shopping.com/cart.do?action=remove&itemId=EST-26&product_id=RP-LI-02"
10.0.0.0 - - [07/Jan 18:10:55:198] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://shopping.com/cart.do?action=remove&itemId=EST-26&product_id=RP-LI-02"
```


Forwarding and Receiving

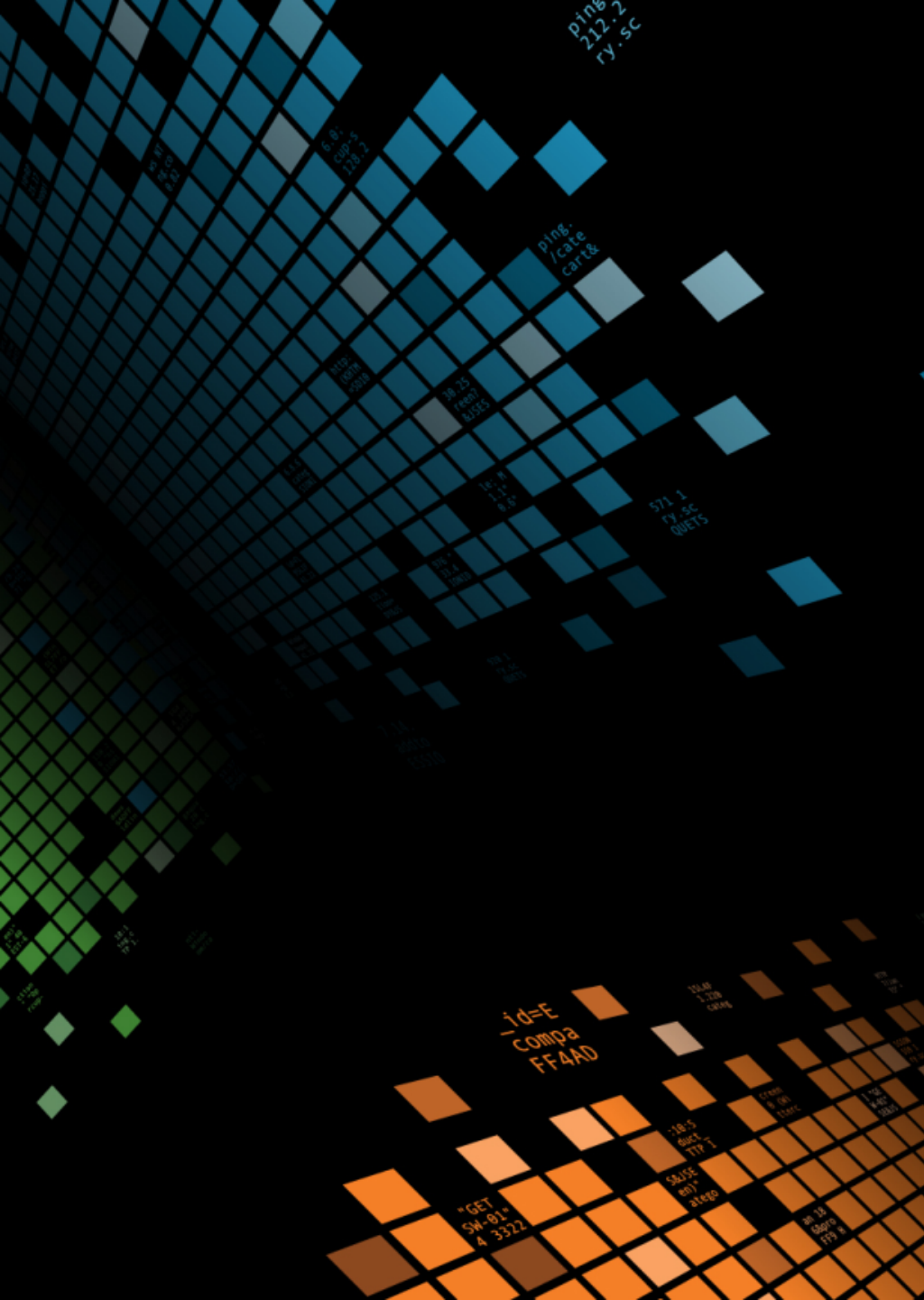
Hi

Forwarding with ACK



```
outputs.conf:  
[tcpout:foobar]  
useACK = true
```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D5L9FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-5W-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D5L9FF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=KQ-CW-01"
317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D5L9FF10ADFF10 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D5L9FF10ADFF10"
10.0.55.187 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D5L9FF10ADFF10 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=KQ-CW-01"
10.0.55.187 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D5L9FF10ADFF10 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=KQ-CW-01"
10.0.55.187 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D5L9FF10ADFF10 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=KQ-CW-01"



Multiple Pipeline Sets

More faster, sometimes

Pipeline Sets: CPU Utilization

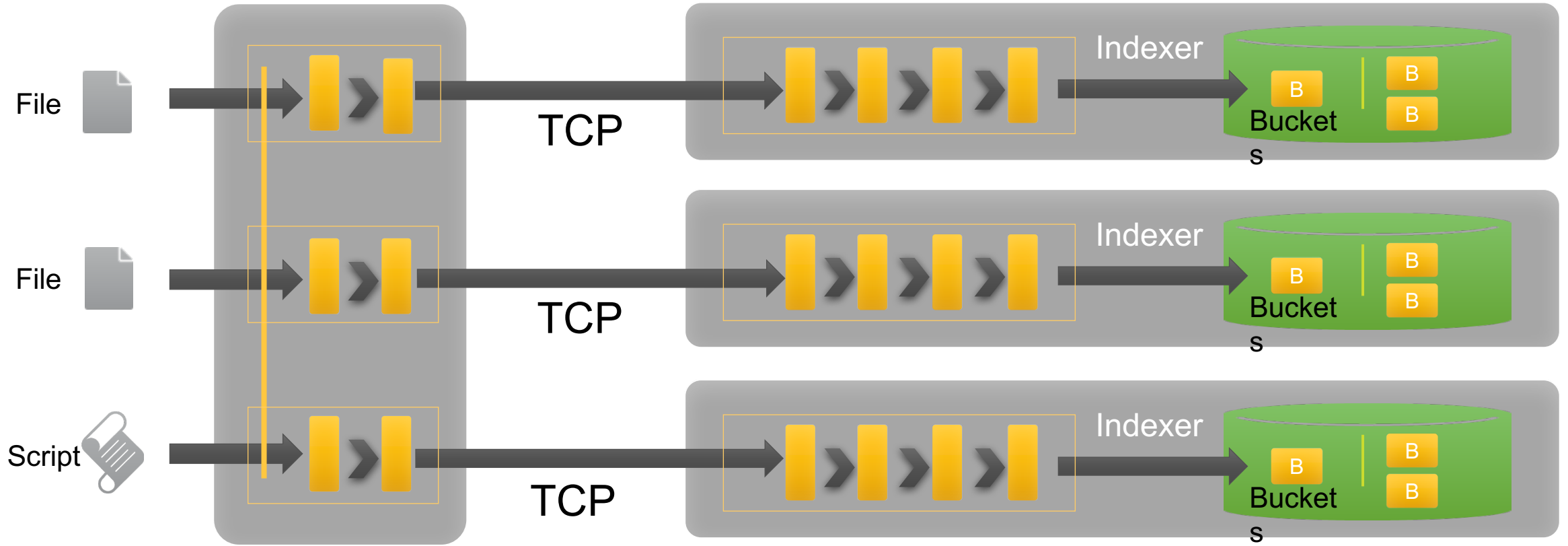
- Rule of Thumb:
 - 4-6 cores per set
 - 1 core per search (unless `batch_search_max_pipeline > 1...`)
- Example: Indexer host with **2** Pipeline Sets:
 - **2** x 6 = **12** cores for splunkd daemon
 - **10** searches running
 - Other cores: “splunk-optimize”, etc, periodically.
 - Total: Roughly **10** + **12** = 22 cores in use.
- Parallel pipeline sets for underutilized hosts:

```
server.conf:
[general]
parallelIngestionPipelines = 2
```

Pipeline Sets: Not an easy decision!

- Can increase forwarding or indexing rate:
 - Total rate = $base_rate \times num_pipeline_sets$
 - **Good idea** on edge Forwarders (see next slide...)
 - **Bad idea** on already-overwhelmed indexers!
- **Does not reduce search time!**
 - Search time = $base_search_time / number_machines$
- Assume: indexing N GB/day
 - On **4** indexers, pipeline sets = **1**.
 - Dense search, 24 hours: Each indexer searches ($N / 4$) GB.
 - Increase to pipeline sets = **2**, downsize to **2** indexers.
 - Dense search, 24 hours: Each indexer searches ($N / 2$) GB.
 - Same indexing rate with fewer machines, but **searches take twice as long!**
 - Except with "batch mode" searches...

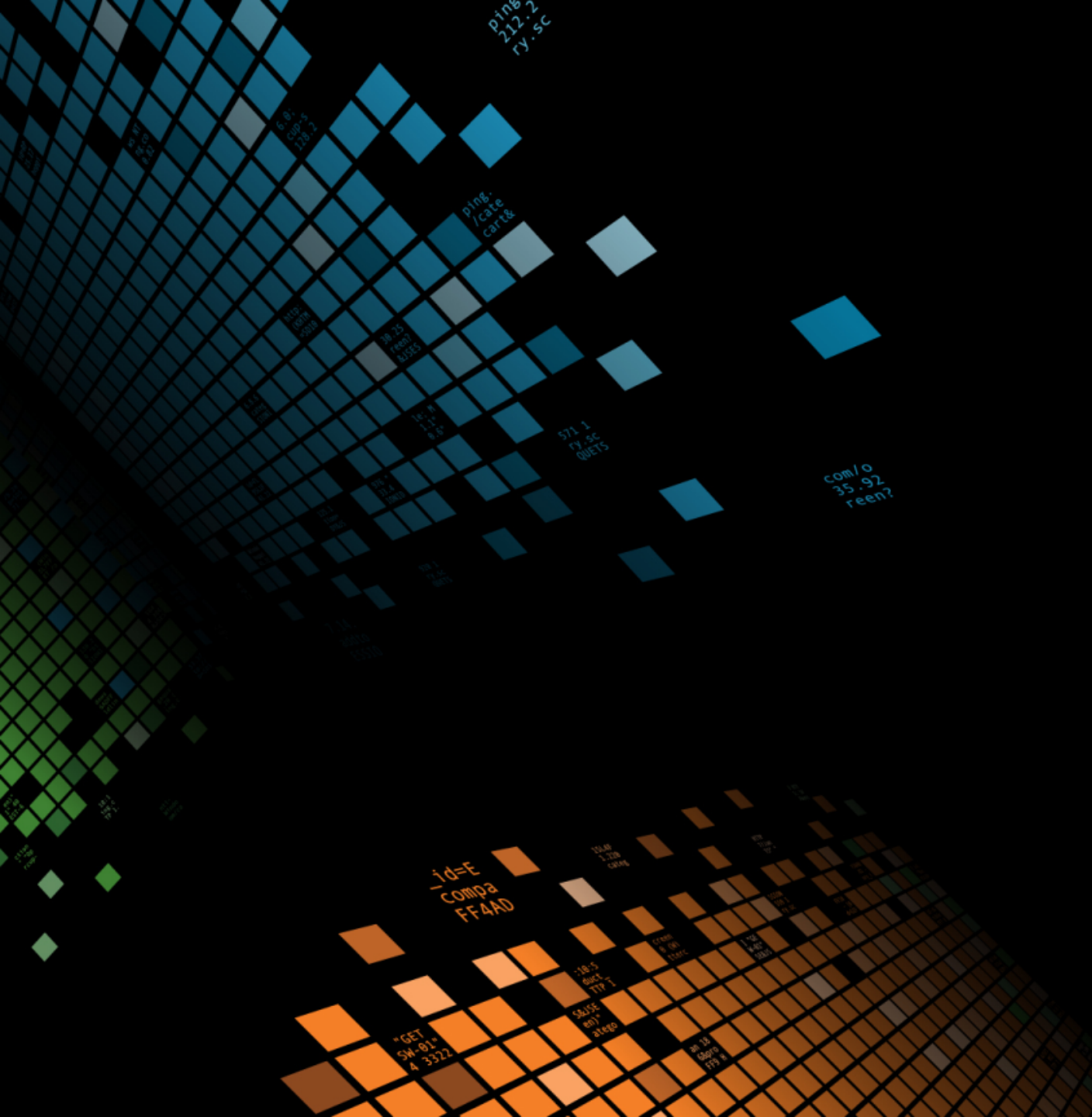
Multiple Ingestion Pipeline Sets over Network



Forwarder: 3 Pipeline Sets

3 Indexers: 1 Pipeline Set each

```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L9FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-5W-03" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.10.10.10  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=KQ-CB-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.10.10.10  
128.241.220.82 - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L7FF6ADFF0 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L7FF6ADFF0" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.10.10.10  
128.241.220.82 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&product_id=KQ-CB-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.10.10.10
```



Nerdier Stuff

8-^)

Resource Management

Pipeline Data Raw Storage

```
2007-01-23 21:15:46,674 DEBUG [com.splunk.doom] com.sun.ebank.ejb.customer... \n  
java.lang.NumberFormatException: For input string: "fish!" \n  
    at java.lang.NumberFormatException.forInputString(NumberFormatException.java:48) \n  
    at java.lang.Integer.parseInt(Integer.java:447) \n  
...
```

Pipeline Data 1

offset

@0 + 100

_raw

2007-01-23 21:15:46,674 DEBUG [com.splu...

Pipeline Data 3

offset

@150 + 80

_raw

at java.lang.NumberFormatException.f...

Pipeline Data 2

offset

@100 + 50

_raw

java.lang.NumberFormatException: For in...

Pipeline Data 4

offset

@230 + 40

_raw

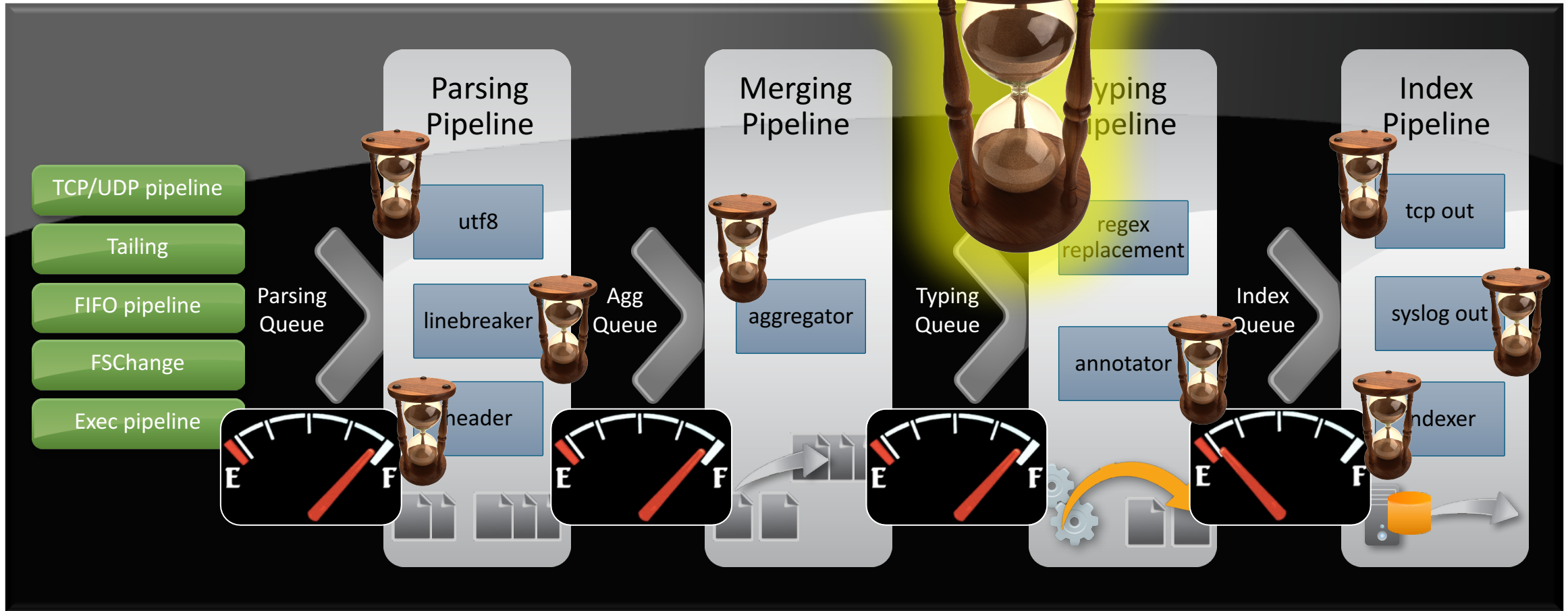
at java.lang.Integer.parseInt(Integer.jav...

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L9FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-5W-03" "00000000-0000-0000-0000-000000000000"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-01" "COMPAQ1101CHN"
317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D15L9FF1ADFF9 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02" "00000000-0000-0000-0000-000000000000"
125.17.14.189 - - [07/Jan 18:10:57:187] "GET /cart.do?action=remove&itemId=EST-16&product_id=RP-LI-02" "00000000-0000-0000-0000-000000000000"
125.17.14.189 - - [07/Jan 18:10:57:189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-16&product_id=RP-LI-02" "00000000-0000-0000-0000-000000000000"

Debugging! Monitoring Console! (aka DMC!)

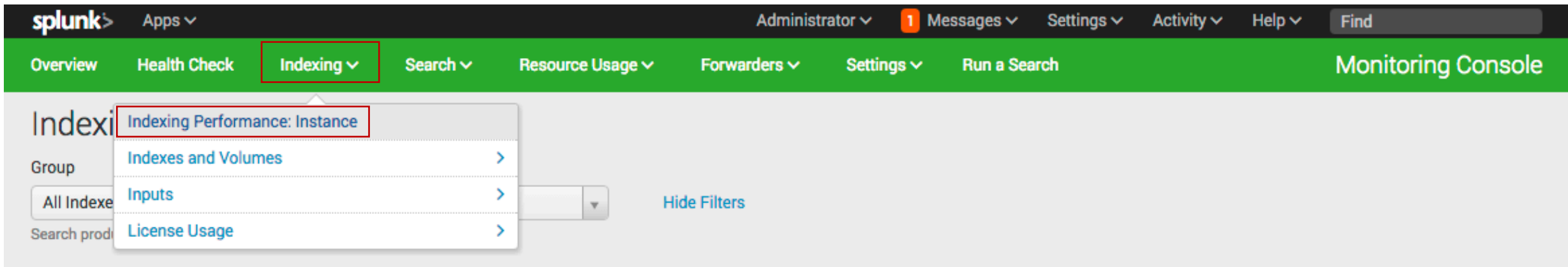


Pipelines/Processors (Debugging)

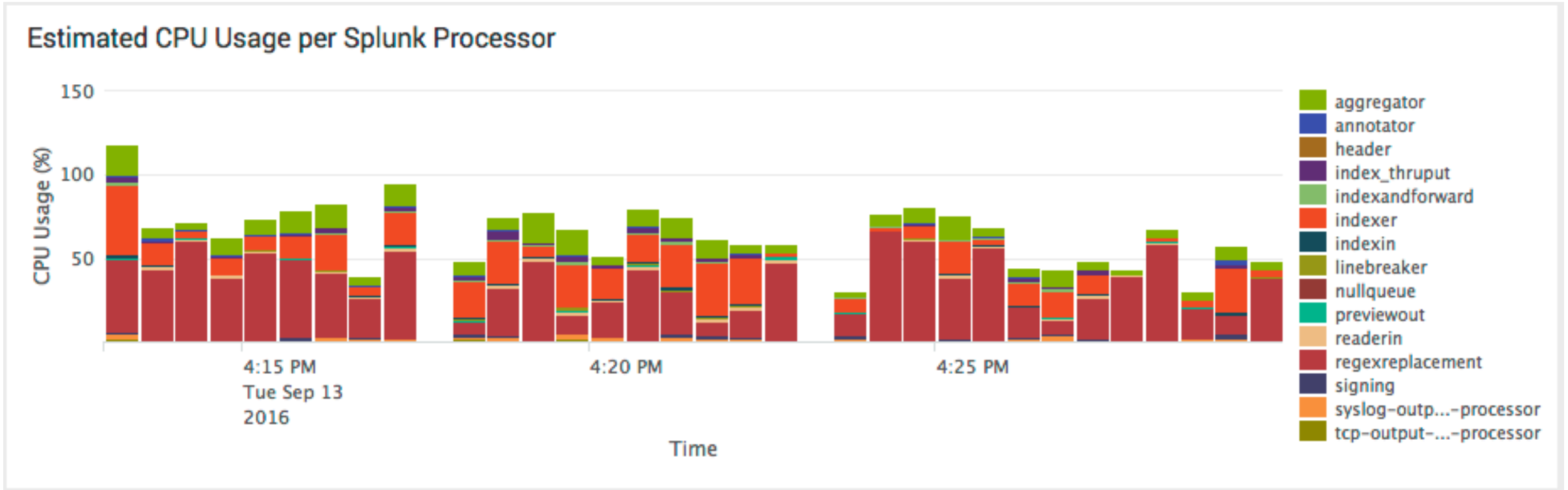


```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-5W-03" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.0.0.0  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=RP-LI-02" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.0.0.0  
128.241.220.82 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.0.0.0  
128.241.220.82 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.0.0.0  
128.241.220.82 - - [07/Jan 18:10:55:189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.0.0.0
```


DMC/Monitoring Console – Indexing Performance



DMC/MC – CPU per Processor (Unhealthy)



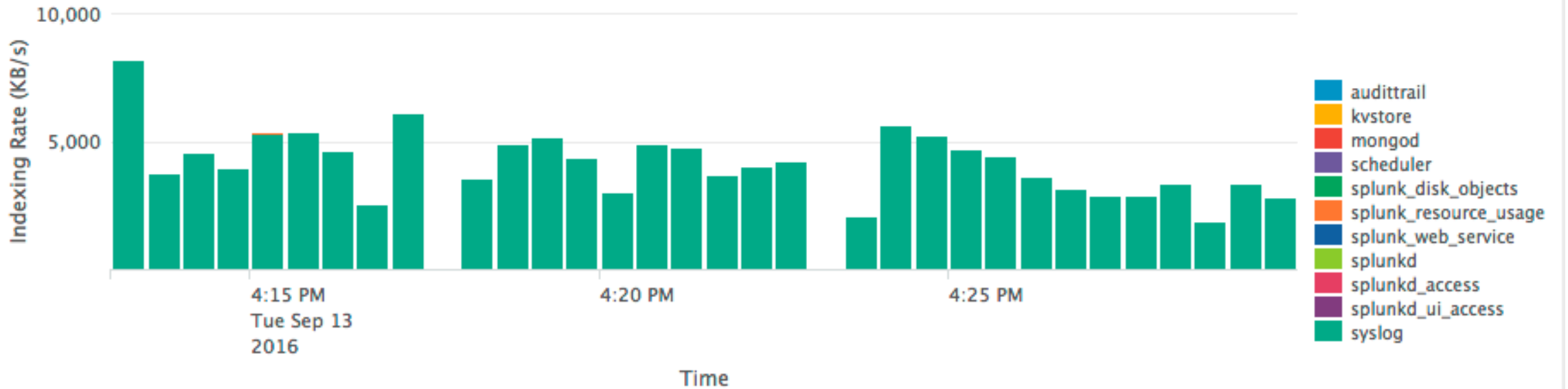
```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-5W-03" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.0.1) Gecko/20100101 Firefox/3.5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14...
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L7FF6ADFF0 HTTP 1.1" 404 322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=RP-LI-02" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.0.1) Gecko/20100101 Firefox/3.5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14...
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-5W-03" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.0.1) Gecko/20100101 Firefox/3.5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14...
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L7FF6ADFF0 HTTP 1.1" 404 322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=RP-LI-02" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.0.1) Gecko/20100101 Firefox/3.5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14...
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-5W-03" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.0.1) Gecko/20100101 Firefox/3.5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14...
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L7FF6ADFF0 HTTP 1.1" 404 322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=RP-LI-02" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.0.1) Gecko/20100101 Firefox/3.5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14...
```

DMC/MC – Indexing Rate

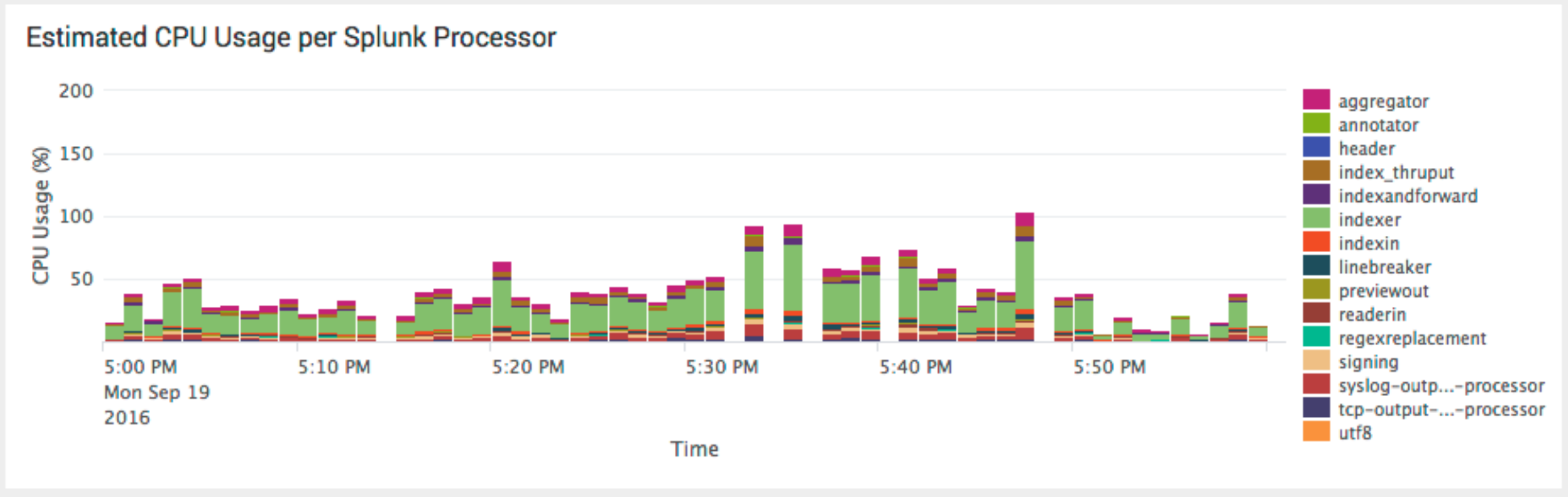
Estimated Indexing Rate Per Sourcetype

Split by

Sourcetype



DMC/MC - CPU per Processor (Healthy)



```
130.60.4 -- [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_0; rv:53.0) Gecko/20100801 Firefox/53.0"
128.241.220.82 -- [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=K9-CU-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_0; rv:53.0) Gecko/20100801 Firefox/53.0"
317.27.160.0 -- [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D19SL9FF2ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_0; rv:53.0) Gecko/20100801 Firefox/53.0"
125.17.14.14 -- [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D5SL9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_0; rv:53.0) Gecko/20100801 Firefox/53.0"
100.100.100.100 -- [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D5SL9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_0; rv:53.0) Gecko/20100801 Firefox/53.0"
100.100.100.100 -- [07/Jan 18:10:55:189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D5SL9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_0; rv:53.0) Gecko/20100801 Firefox/53.0"
```

metrics.log

► Search:

```
index=_internal
source=*metrics.log*
```

► Groups

- pipeline
- queue
- thruput
- per_source_thruput
- per_sourcetype_thruput
- per_index_thruput
- per_host_thruput
- tcpin_connections
- tcpout_connections
- search_concurrency
- clusterout_connections
- deploy-server
- tailingprocessor

The screenshot shows the Splunk Search & Reporting interface. The search query is `index=_internal source=*metrics.log*` with 10,000 events. A group analysis for the field `group` is displayed, showing 21 values representing 99.99% of events. The top 10 values are:

Value	Count	%
pipeline	3,048	30.483%
queue	1,963	19.632%
deploy-server	600	6.001%
per_source_thruput	580	5.8%
per_sourcetype_thruput	579	5.79%
thruput	461	4.61%
per_index_thruput	329	3.29%
search_concurrency	304	3.04%
tailingprocessor	302	3.02%
pool	300	3%

The interface also shows a list of fields on the left, including `component`, `cpu_seconds`, `date_hour`, `date_mday`, `date_minute`, `date_month`, `date_second`, `date_wday`, `date_year`, `date_zone`, `group`, `host`, `instantaneous_eps`, `instantaneous_kbps`, `kb`, `kbps`, `source`, `sourcetype`, `cumulative_hits`, and `current_size`.

metrics.log: Scenarios

- Indexing instance: Index Queue at 100%
 - Forwarding disabled:
 - Indexing rate: **High? Lots of data.** **Low? Check cpu_seconds, iowait, etc.** **Zero? Disk full!**
 - Forwarding enabled: See above, on downstream indexers.
 - Forwarding enabled, and downstream indexers are fine?
 - TCPOut rate: **High? Lots of data.** **Low? See outputs.conf maxKBps, check bandwidth & latency...**
Zero? Check SSL, ports, splunkd.log...
 - Also indexing locally? See “Forwarding disabled” above...
- Universal Forwarder
 - Similar, but: Parsing Queue instead of Index Queue.
- Start from end (healthiest node), work backwards...

metrics.log: Universal Forwarder

- No indexing/searching capability
- Can't forward logs to indexers if forwarding is busted
- Fallback to raw file (grep!)

1) `$ grep group=queue metrics.log | grep --color 'max_size.*current_size_kb[^\,]*,'`

Metrics - group=queue, name=typingqueue, blocked=true, **max_size_kb=500**,
current_size_kb=499, current_size=1821, largest_size=1821, smallest_size=0

2) `$ grep group=tcpout_connections metrics.log`

... destIp=10.159.4.67, destPort=9997 ... **_tcp_KBps=27674.87** ...

_tcp_Kprocessed=802571

3) `$ grep -E '(ERROR|WARN|FATAL|CRIT)' splunkd.log`

4) `$ splunk help list inputstatus`

Older forwarders: <http://blogs.splunk.com/2011/01/02/did-i-miss-christmas-2/>

Questions?

.conf2016