CLP: Efficient and Scalable Search on Compressed Text Logs

Kirk Rodrigues, Yu Luo, Ding Yuan
Compressed Log Processor

**Lossless log compression**
...better than general-purpose compressors

**Can search compressed logs**
...without decompression
...with good performance

<table>
<thead>
<tr>
<th></th>
<th>Uncompressed</th>
<th>Gzip</th>
<th>CLP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Space Utilization (%)</td>
<td>100%</td>
<td>4.72%</td>
<td>2.35%</td>
</tr>
</tbody>
</table>

Diagram: Space Utilization Comparison
- Uncompressed: 100%
- Gzip: 4.72%
- CLP: 2.35%
The Log Management Pipeline

Example log message | Timestamp | Variables | Static text
--- | --- | --- | ---
2020-01-02T03:04:05.006 INFO Task task_12 assigned to container: [NodeAddress:172.128.0.41, ContainerID:container_15], operation took 0.335 seconds
The Log Management Pipeline

Logs

- Provide crucial runtime information
- Widely used for many purposes
The Log Management Pipeline

- Logs
  - Provide crucial runtime information
  - Widely used for many purposes

Ingest

Search Tools

- splunk>Enterprise
  - $2.787B annual revenue
  - Consume lots of resources
The Log Management Pipeline

- **Logs**
  - Provide crucial runtime information
  - Widely used for many purposes
  - Companies generate petabytes of logs

- **Ingest**

- **Search Tools**
  - Consume lots of resources

eBay generated **1.2 PB of logs per day** in 2018

**HDD storage cost**

\[
\text{2c/GB/month}
\]

**1.2 PB/day annual storage cost** $56,031,707
The Log Management Pipeline

Logs

- Provide crucial runtime information
- Widely used for many purposes
- Companies generate **petabytes** of logs

Ingest

Search Tools

- Consume lots of resources
- Build indexes ➔ adds storage overhead

Log Management Tools

- **Splunk Enterprise**
- **Elasticsearch**

Logs ➔ Index
The Log Management Pipeline

- Logs
  - Provide crucial runtime information
  - Widely used for many purposes
  - Companies generate petabytes of logs

- Ingest

- Search Tools
  - Consume lots of resources
  - Build indexes ➔ adds storage overhead
  - Can only retain indexed logs for weeks

- Uncompressed
- Index + compressed log

Space Utilization (%)

- 40.98%
The Log Management Pipeline

Search Tools
• Consume lots of resources
• Build indexes ➔ adds storage overhead
• Can only retain indexed logs for weeks

Archival Tools
• Unsearchable once compressed

Uncompressed: a b c a b x y a b c
Compressed: a b c (3,2)

Space Utilization (%)
- Uncompressed: 40.98%
- Index + compressed log: 0%

- splunk Enterprise
- Elasticsearch
- Compress
- gzip
The Log Management Pipeline

**Search Tools**
- Consume lots of resources
- Build indexes → adds storage overhead
- Can only retain indexed logs for weeks

**Splunk Enterprise**

**Archival Tools**
- Unsearchable once compressed

**Compress**

**Gzip**

Space Utilization (%)

<table>
<thead>
<tr>
<th></th>
<th>0%</th>
<th>50%</th>
<th>100%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uncompressed</td>
<td></td>
<td></td>
<td>40.98%</td>
</tr>
<tr>
<td>Index + compressed log</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Uncompressed: a b c a b x y a b c
Compressed: a b c (3,2) x y (4,2) c
The Log Management Pipeline

**Search Tools**
- Consume lots of resources
- Build indexes ➔ adds storage overhead
- Can only retain indexed logs for weeks

**Archival Tools**
- Unsearchable once compressed

**Space Utilization (%)**
- Uncompressed: 100%
- Compressed: 40.98%

**Uncompressed**
- a b c a b x y a b c

**Compressed**
- a b c (3,2) x y (4,2) c

Mutually Exclusive
Demo
Compression

2020-01-02T03:04:05.006 INFO Task task_12 assigned to container: [NodeAddress:172.128.0.41, ContainerID:container_15], operation took 0.335 seconds
Compression

2020-01-02T03:04:05.006 INFO Task task_12 assigned to container: [NodeAddress:172.128.0.41, ContainerID:container_15], operation took 0.335 seconds

2020-01-02T03:04:06.006 INFO Task task_13 assigned to container: [NodeAddress:172.128.0.42, ContainerID:container_16], operation took 1.221 seconds

2020-01-02T03:04:09.006 INFO Task task_14 assigned to container: [NodeAddress:172.128.0.41, ContainerID:container_15], operation took 0.115 seconds
Compression

2020-01-02T03:04:05.006 INFO Task task_12 assigned to container: [NodeAddress:172.128.0.41, ContainerID:container_15], operation took 0.335 seconds

| ID | Log Type
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Log Type</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ID</th>
<th>Variable Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Variable Value</td>
</tr>
</tbody>
</table>
## Compression

2020-01-02T03:04:05.006 INFO Task task_12 assigned to container: [NodeAddress:172.128.0.41, ContainerID:container_15], operation took 0.335 seconds

<table>
<thead>
<tr>
<th>Log Type Dictionary</th>
<th>ID</th>
<th>Log Type</th>
<th>Dictionary</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td></td>
<td>INFO Task</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Variable Dictionary</th>
<th>ID</th>
<th>Variable Value</th>
</tr>
</thead>
</table>
Compression

2020-01-02T03:04:05.006 INFO Task `task_12` assigned to container: [NodeAddress: `172.128.0.41`, ContainerID: `container_15`], operation took 0.335 seconds

<table>
<thead>
<tr>
<th>Log Type Dictionary</th>
<th>ID</th>
<th>Log Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>4</td>
<td>INFO Task assigned to container: [NodeAddress: , ContainerID: ], operation took seconds</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Variable Dictionary</th>
<th>ID</th>
<th>Variable Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>8</td>
<td>task_12</td>
</tr>
<tr>
<td></td>
<td>9</td>
<td>172.128.0.41</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>container_15</td>
</tr>
</tbody>
</table>
# Compression

2020-01-02T03:04:05.006 INFO Task task_12 assigned to container: [NodeAddress:172.128.0.41, ContainerID:container_15], operation took 0.335 seconds

<table>
<thead>
<tr>
<th>Log Type Dictionary</th>
<th>ID</th>
<th>Log Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>4</td>
<td>INFO Task assigned to container: [NodeAddress:, ContainerID:], operation took seconds</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Variable Dictionary</th>
<th>ID</th>
<th>Variable Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>8</td>
<td>task_12</td>
</tr>
<tr>
<td></td>
<td>9</td>
<td>172.128.0.41</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>container_15</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Encoded Message</th>
<th>Timestamp</th>
<th>Log Type ID</th>
<th>Variable Values</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1577934245006</td>
<td>4</td>
<td>8 9 10 0x3FD570A3D70A3D71</td>
</tr>
</tbody>
</table>
Compression

2020-01-02T03:04:05.006 INFO Task task_12 assigned to container: [NodeAddress:172.128.0.41, ContainerID:container_15], operation took 0.335 seconds

<table>
<thead>
<tr>
<th>Log Type ID</th>
<th>Log Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>INFO Task assigned to container: [NodeAddress:, ContainerID:]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Variable ID</th>
<th>Variable Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>task_12</td>
</tr>
<tr>
<td>9</td>
<td>172.128.0.41</td>
</tr>
<tr>
<td>10</td>
<td>container_15</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Log Type ID</th>
<th>Variable Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>1577934245006</td>
<td>4</td>
<td>8 9 10 0x3FD570A3D70A3D71</td>
</tr>
</tbody>
</table>
Compression

2020-01-02T03:04:05.006 INFO Task task_12 assigned to container: [NodeAddress:172.128.0.41, ContainerID:container_15], operation took 0.335 seconds

<table>
<thead>
<tr>
<th>Log Type Dictionary</th>
<th>ID</th>
<th>Log Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>4</td>
<td>INFO Task</td>
</tr>
</tbody>
</table>

| Shared between messages |

<table>
<thead>
<tr>
<th>Variable Dictionary</th>
<th>ID</th>
<th>Variable Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>8</td>
<td>task_12</td>
</tr>
<tr>
<td></td>
<td>9</td>
<td>172.128.0.41</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>container_15</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Encoded Message</th>
<th>Timestamp</th>
<th>Log Type ID</th>
<th>Variable Values</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1577934245006</td>
<td>4</td>
<td>8 9 10 0x3FD570A3D70A3D71</td>
</tr>
</tbody>
</table>
Search

Uncompressed Message
Search

Log Type Dictionary

Variable Dictionary

Encoded Message
2020-01-02T03:04:05.006 INFO Task task_12 assigned to container: [NodeAddress:172.128.0.41, ContainerID:container_15], operation took 0.335 seconds

Task * assigned to container*:172.128*
Task * assigned to container*:172.128*

2020-01-02T03:04:05.006 INFO Task task_12 assigned to container: [NodeAddress:172.128.0.41, ContainerID:container_15], operation took 0.335 seconds

Task * assigned to container*:172.128*
2020-01-02T03:04:05.006 INFO Task task_12 assigned to container: [NodeAddress:172.128.0.41, ContainerID:container_15], operation took 0.335 seconds

Task * assigned to container*:172.128*

Dictionary variable?

Log type?
Search

2020-01-02T03:04:05.006 INFO Task task_12 assigned to container: [NodeAddress:172.128.0.41, ContainerID:container_15], operation took 0.335 seconds

Task * assigned to container*:172.128*
Search

2020-01-02T03:04:05.006 INFO Task task_12 assigned to container: [NodeAddress:172.128.0.41, ContainerID:container_15], operation took 0.335 seconds

Task * assigned to container*:172.128*

Dictionary variable?
Encoded variable?
Log type?
## Search

Task * assigned to container*:*:172.128*

<table>
<thead>
<tr>
<th>#</th>
<th>Log type</th>
<th>Variables</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Task * assigned to container*:<em>:172.128</em></td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>Task * assigned to container*:</td>
<td>172.128* (IP address)</td>
</tr>
<tr>
<td>3</td>
<td>Task * assigned to container*:</td>
<td>172.128* (float)</td>
</tr>
<tr>
<td>4</td>
<td>Task * assigned to <em>:172.128</em></td>
<td>container*</td>
</tr>
<tr>
<td>5</td>
<td>Task * assigned to <em>:</em></td>
<td>container*, 172.128* (IP address)</td>
</tr>
<tr>
<td>6</td>
<td>Task * assigned to <em>:</em></td>
<td>container*, 172.128* (floating point)</td>
</tr>
</tbody>
</table>
Evaluation

- CLP’s compression ratio & speed
- CLP’s search performance

Lots more detail in the paper!
Tested Tools

**Search Tools**
- ripgrep
- Elasticsearch

**Archival Tools**
- gzip
- lzma
- PPMd
- Izma
- Zstandard
Compression Ratio

<table>
<thead>
<tr>
<th>Tool</th>
<th>Average Compression Ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLP</td>
<td>32.20</td>
</tr>
<tr>
<td>Gzip</td>
<td>16.38</td>
</tr>
<tr>
<td>Splunk Enterprise</td>
<td>2.86</td>
</tr>
<tr>
<td>Elasticsearch</td>
<td>1.75</td>
</tr>
</tbody>
</table>

Diagram showing compression ratio for different tools and datasets.
Compression vs Ingestion Speed

- CLP: 549 MB/s
- Elasticsearch: 38 MB/s
- Splunk: 35 MB/s
Search Performance

Query Benchmark

Designed to exercise all of CLP’s execution paths
Log type queries, variable queries, etc.

Queries which return few and many results
Search Performance

CLP:
- 4.2x faster than Splunk Enterprise
- 1.3x faster than Elasticsearch
- 7.8x faster than ripgrep
Search Performance

- CLP + Persistent-Cache
- CLP
- Elasticsearch
- Splunk Enterprise
- 7z-lzma + ripgrep
- Zstd + ripgrep
- Gzip + ripgrep

Queries that return few results

**CLP:**
- 4.2x faster than Splunk Enterprise
- 1.3x faster than Elasticsearch
- 7.8x faster than ripgrep
Queries that return few results

CLP + cache:
- 40x faster than Splunk Enterprise
- 17.8x faster than Elasticsearch
Related Work

• Singh and Shivanna [US patent 9,619,478] also aims to deduplicate static text from variable values
  • Does not propose a search algorithm
  • Relies on application source
  • Not entirely lossless
• Tools like Splunk Enterprise and Elasticsearch build text indexes to search logs
• Succinct [Agarwal et al. NSDI ’15] proposed a method for compressing indexes
  • But any index still carries overhead whereas CLP deduplicates the original data
• Scalyr uses optimizations to search uncompressed logs at 1.25 GB/s
  • CLP works on compressed data with up to 420 GB/s throughput
• Grafana Loki only indexes labels
  • Index still adds overhead
  • Reduced index size but search limited to labels
Conclusion

• Achieves unparalleled log compression
• Allows search without decompression
• Combines archiving & log search
• Open-sourced!
• Try it out at yscope.com!
• CLP is just the beginning...
  • e.g., Stitch [Zhao et al. OSDI ’16],
  Log20 [Zhao et al. SOSP ’17]

Want to get in touch?
kirk.rodrigues@yscope.com
info@yscope.com