

DIALOGIX

HackaTUM Winner 2023



Cross-Institutional Academic Partnership



Jonas Matthaei



Philip Jünemann

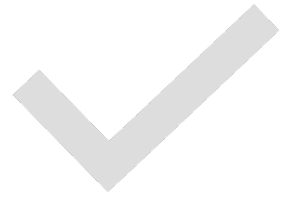


Laurens Houtekamer



Noud Bonke





The objectives

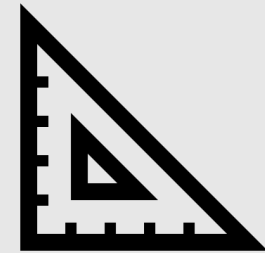




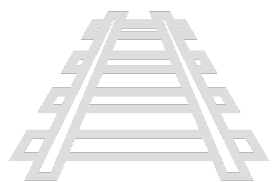
CONCISE COMPLETENESS



INTERACTIVITY



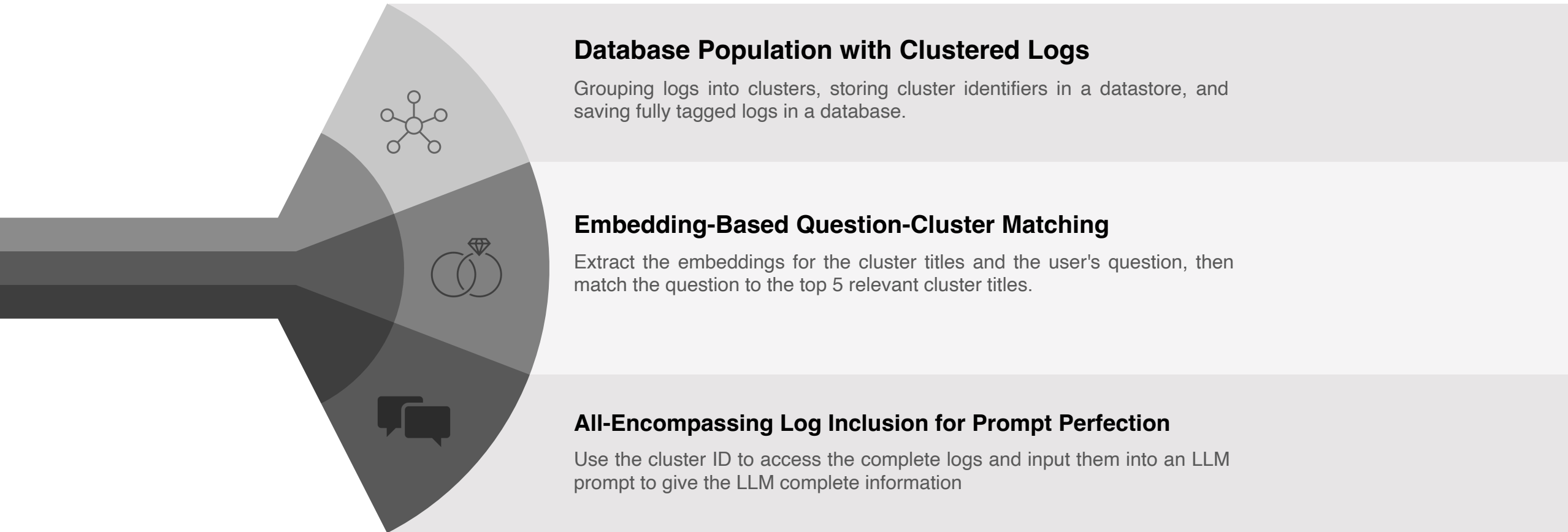
MEASURABLE SUCCESS



The approach



Our Product: A Bird's Eye View



Log Parsing With Bidirectional Parallel Trees

S. Yu, P. He, N. Chen and Y. Wu, "Brain: Log Parsing With Bidirectional Parallel Tree"

- ① Cutting edge method published in 2023.
- ② Faster and more efficient than neural networks, able to match the pace of log generation.
- ③ Enhanced parsing accuracy over alternatives, proven by test on 16 benchmark datasets.
- ④ Able to process approximately **one million** lines of logs in just **46 seconds**.

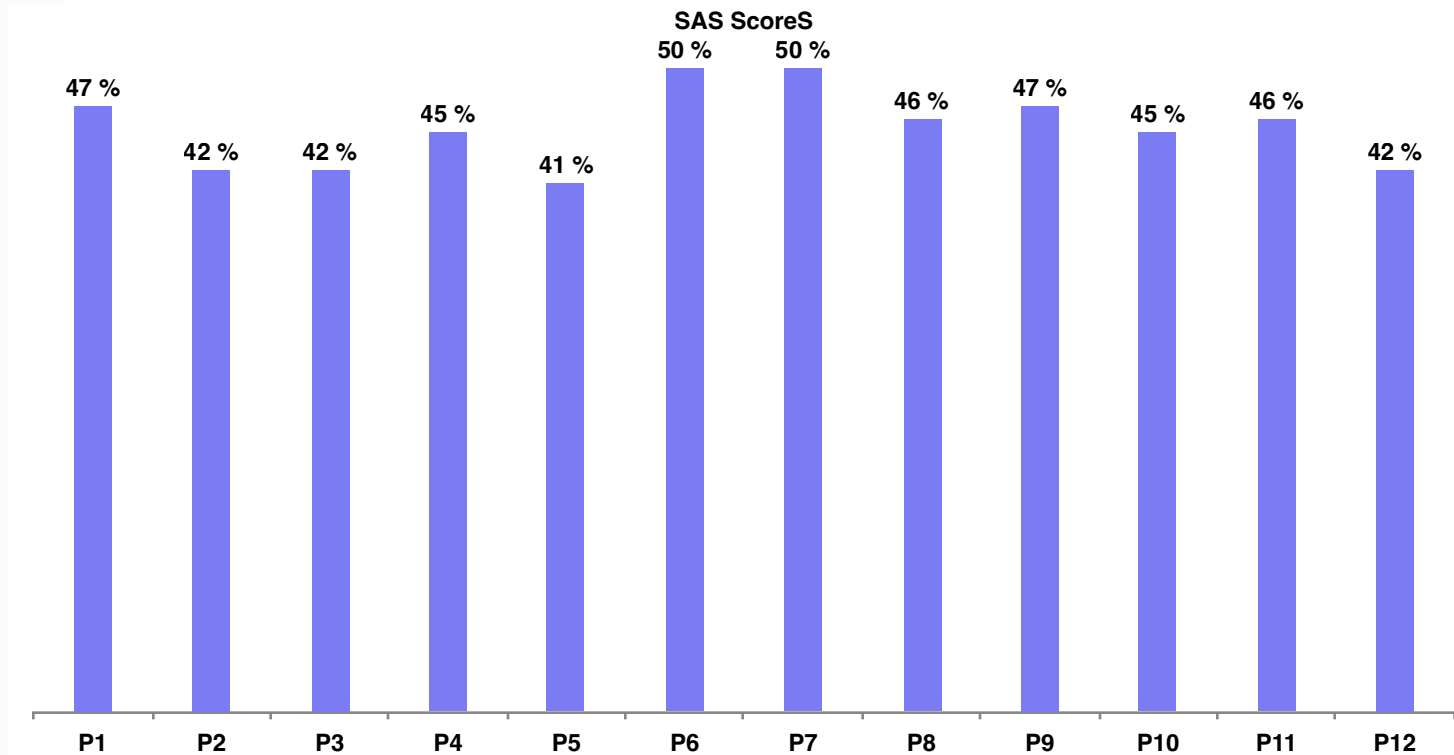
Optimizing through PERFORMANCE MEASUREMENT

Rating outcomes using semantic answer similarity and MLflow

- ① Developed golden standard dataset based on wide array of potentially interesting logs.
- ② SAS to measure semantics instead of lexical overlap.
- ③ SAS shown to correlate highly with human judgement on **three** different datasets.
- ④ Created script to experiment with parameters in an attempt to achieve the optimal pipeline.

COMPARING PARAMETER COMBINATIONS

- ① Retriever model
- ② Reader model
- ③ Similarity threshold
- ④ Prompt engineering





The results






File Upload

Upload a file

Drag and drop file here
Limit 200MB per file • TXT, OUT

Browse files

 final_log.out
21.1MB




Conversation History

Start New Conversation


23-11-19 05:22:42

23-11-19 05:22:42 - Did any processes
receive a SI




 Thank you for uploading the file, let's start exploring.

 Did any processes receive a SIGTERM signal?

 On November 10th 05:49:52 and 05:50:39, CMX50070-101776 xu_launcher processes 1978, 1977, 1979, and 1980 all received signal 17, which is a SIGTERM signal.

Use prompt 'full logs' to see the complete log files corresponding to the requested events.

 full logs

 Nov 10 05:49:52 CMX50070-101776 xu_launcher 1978 Received signal: 17, Nov 10 05:49:52 CMX50070-101776 xu_launcher 1977 Received signal: 17, Nov 10 05:49:52 CMX50070-101776 xu_launcher 1979 Received signal: 17, Nov 10 05:49:53 CMX50070-101776 xu_launcher 1980 Received signal: 17. Nov 10 05:50:39 CMX50070-101776 xu_launcher 1978 Received signal: 17. Nov

Enter your message: 






File Upload

Upload a file

Drag and drop file here
Limit 200MB per file • TXT, OUT

Browse files

 final_log.out
21.1MB


×


Conversation History

Start New Conversation

23-11-19 05:22:42


23-11-19 05:22:42 - Did any processes receive a SI

 Did anyone change file permissions using chmod?

 On Nov 10 at 05:49:38, systemd reported that three configuration files were marked executable, suggesting that someone changed the file permissions using chmod.

Use prompt 'full logs' to see the complete log files corresponding to the requested events.

 What files were marked executable?

 On Nov 10 05:49:38, three files were marked executable:
/lib/systemd/system/mrt.positioning.catrp3dr.service,
/lib/systemd/system/mrt.positioning.catrp3d1.service, and
/lib/systemd/system/mrt.cmsequencer.service.

Use prompt 'full logs' to see the complete log files corresponding to the requested events.

Enter your message: >






File Upload

Upload a file

Drag and drop file here

Limit 200MB per file • TXT, OUT

Browse files

 final_log.out
21.1MB



Conversation History

Start New Conversation

23-11-19 05:22:42

23-11-19 05:22:42 - Did any processes receive a SI



CMX50070-101776 xu_launcher 1978 Waiting for any signal to shut down..., Nov 10 05:49:52
CMX50070-101776 xu_launcher 1977 Waiting for any signal to shut down..., Nov 10 05:49:52
CMX50070-101776 xu_launcher 1979 Waiting for any signal to shut down..., Nov 10 05:49:53
CMX50070-101776 xu_launcher 1980 Waiting for any signal to shut down..., Nov 10 05:50:41
CMX50070-101776 xu_launcher 1981 Waiting for any signal to shut down... Nov 10 05:49:37
localhost kernel pcieport 0000:00:01.1: PME: Signaling with IRQ 25, Nov 10 05:49:37 localhost
kernel pcieport 0000:00:01.3: PME: Signaling with IRQ 26, Nov 10 05:49:37 localhost kernel
pcieport 0000:00:01.5: PME: Signaling with IRQ 27, Nov 10 05:49:37 localhost kernel pcieport
0000:00:08.1: PME: Signaling with IRQ 28, Nov 10 05:49:37 localhost kernel pcieport 0000:00:08.2:
PME: Signaling with IRQ 29 Nov 10 05:49:54 CMX50070-101776 sh 3390 cmseq | CMsequencer
starter processes IDs:



I want to know about ssh attempts. Were there any failed ssh login attempts?



From Nov 10 06:09:41 to Nov 13 17:14:04, there were 14 failed authentication attempts from rhost 10.0.2.217. Additionally, there were 8 successful publickey authentication attempts from various rhosts for root.

Use prompt 'full logs' to see the complete log files corresponding to the requested events.

Enter your message: >





The VISION

OUR FUTURE VISION

- ① Intelligent agents selecting optimal tools.
- ② Creating a SQuAD format dataset specialized on logs for further pipeline optimization.
- ③ The optimal user interface, communicating inside the logs.
- ④ Transforming the logs into a story.